European Investigations Guide

2020

With contributions from:

A&L Goodbody
Babić & Partners
Borenius Attorneys
Camilleri Preziosi
Cerrahoğlu
Chrysses Demetriades
COBALT
Ellex Klavins
Gasser Partner
HAVEL & PARTNERS
Hjort
Hogan Lovells
Kalo & Associates
Kambourov & Partners
Kinstellar
KNOETZL
Kromann Reumert
Lutgen + Associés
Mareş & Mareş
Miro Senica and attorneys
Nordia Law
Ovvadias S. Namias
Sayenko Kharenko
taormina
Uría Menéndez

European Investigations Guide 2020

Published by

Hogan Lovells International LLP

Karl-Scharnagl-Ring 5

80539 Munich

Germany

Second Edition
Published 2020

Contributing editors

Dr. Sebastian Lach, Hogan Lovells

Salomé Lemasson, Hogan Lovells

Inga Ludewig, Hogan Lovells

Désirée Maier, Hogan Lovells

Victoria Parr, Hogan Lovells

Editorial assistants

Stephanie Küppers, Hogan Lovells

Tomas Schurmann, Hogan Lovells

Contents

Preface 1

Cross-Border Investigations 2

Data Privacy in Investigations 6

Legal Framework for Money Laundering in Europe 11

Cartel Investigations 16

Export / Sanctions 21

Overview 26

Albania – Kalo & Associates 27

Austria – KNOETZL HAUGENEDER NETAL 35

Belgium – Hogan Lovells 43

Bulgaria – Kambourov & Partners 53

Croatia – Babić & Partners 60

Cyprus – Chrysses Demetriades & Co 67

Czech Republic – Kinstellar 74

Denmark – Kromann Reumert 80

Estonia – COBALT 87

Finland – Borenius Attorneys 95

France – Hogan Lovells 102

Germany – Hogan Lovells 110

Greece – Ovvadias S. Namias 118

Hungary – Hogan Lovells 126

Ireland – A&L Goodbody 133

Italy – Hogan Lovells 142

Latvia – Ellex Klavins 150

Liechtenstein – Gasser Partner 157

Lithuania – COBALT 164

Luxembourg – Lutgen + Associés **171**

Malta – Camilleri Preziosi Advocates **178**

The Netherlands – Hogan Lovells **186**

Norway – Hjort **196**

Poland – Hogan Lovells **203**

Portugal – Uría Menéndez Abogados **210**

Romania – Mareş & Mareş **218**

Russia – Hogan Lovells **226**

Slovakia – HAVEL & PARTNERS **233**

Slovenia – Miro Senica and attorneys **241**

Spain – Hogan Lovells **250**

Sweden – Nordia **258**

Switzerland – taormina **266**

Turkey – Cerrahoğlu **273**

Ukraine – Sayenko Kharenko **281**

United Kingdom – Hogan Lovells **289**

Preface

Dear Reader,

On behalf of all colleagues and experts involved, we are proud to publish the second and updated edition of the European Investigations Guide. This guide continues to be designed to provide you with a quick reference to some of the most pressing questions and trends relating to internal investigations in European countries.

Although it is important to note that this guide cannot, and is not intended to, replace any kind of legal advice in individual cases, it will help the compliance expert to identify the risks arising and the right questions to ask to address those risks. To that end, a group of leading practitioners from various European countries have provided their expert input on such issues in their jurisdiction. As this guide presents the view of experts on legal issues, we can of course not exclude that courts, authorities and other third parties might hold or take different views.

We hope that you will find the European Investigations Guide helpful and would like to thank you for your interest in this publication.

Dr. Sebastian Lach

Partner
Hogan Lovells

Cross-Border Investigations

INTRODUCTION

The more countries and jurisdictions are involved in a matter, the harder it becomes to run and complete an investigation quickly, efficiently, and comprehensively. Various issues arise like language barriers, different cultural perceptions, local laws, data privacy provisions, and blocking statutes. All of those have to be coordinated at the same time. Such investigations are therefore, not only difficult to complete, but also bear the risk that the investigation itself may lead to cases on non-compliance. As a consequence, those in charge of such investigations have to be mindful to avoid generating such risks – also for themselves personally.

While it is no substitute for individually tailored legal advice, this Guide aims to reduce those very risks. It provides a general overview of investigations on the European continent to help orient those leading or involved with such investigations. The following article provides an overview of the most important questions and considerations that arise during the various stages of an investigation – from the beginning to the end.

START OF A CROSS-BORDER INVESTIGATION

Various issues have to be considered after an initial assessment of which countries are implicated in the investigation.

The first question is often whether local support is needed. The answer will often be yes. Mostly, local in-house legal capabilities will be sufficient. However, outside counsel or other external resources will sometimes have to be consulted. In this regard, it has to be noted that it may prove difficult to find the right experts in certain countries. In many locations there is seldom an abundance of white collar crime or compliance experts. It is therefore advisable to build and maintain a network of experts in the most important countries, even before an investigation starts. In crisis situations (like dawn raids or cyber-attacks) there may not be time to search for local support. Even if there is time, if competitors or other companies are faced with the same problem, the best counsel may already have been taken or may already be conflicted once they are approached. Working with non-expert counsel, especially in smaller legal markets, can bear risks and create inefficiencies.

Once the team has been assembled, the next question is whether one is even allowed to investigate in the respective country. This question must be answered with the help of dedicated local counsel. In this regard, one has to differentiate between blocking statutes and data privacy considerations. A blocking statute will often mean that all or certain investigative measures may not be allowed or may only be allowed with special permission. Data privacy concerns relate to the treatment of data containing personal information, but rarely present an absolute obstacle to any investigative step. To provide a simple example, a blocking statute may prevent an interview, while data privacy laws may simply limit the use of information gathered from an interview or call for special measures for the collection and treatment of that data.

Once the question of blocking statutes has been addressed, one may have to clarify whether specific bodies like trade unions, works councils, corporate supervisory boards, financial stakeholders and shareholders have to be informed of the start of the investigation or the information that led to the investigation. Some local laws have very rigid and detailed disclosure requirements. The violation of any such requirements might hinder the investigation or even lead to civil or criminal liability of the company or the individual actors.

In addition, it must be carefully assessed whether early disclosures to local law enforcement agencies are necessary or would be helpful from a strategic standpoint. In some countries, certain situations call for such disclosure under the applicable local laws. In other countries it is culturally necessary to involve the authorities to maintain a cooperative atmosphere. In other countries, however, such disclosures are uncommon and may create more problems than they solve. In cross-border cases, where many authorities may be involved, there may be a strategic advantage to disclosing information in a certain order or having one authority take the lead. Especially at this stage, local expertise – legally and culturally – is very helpful to avoid making the wrong decisions.

THE INVESTIGATIVE PHASE

Once all obstacles that may hinder the start of an investigation have been cleared, the company can start the investigation.

An investigation often begins with so-called immediate measures. Normally, the first task is to ensure that any potentially ongoing criminal or unlawful conduct is stopped. This frequently means monitoring certain payment streams or putting certain individuals at least under close monitoring to make sure that all their actions are appropriate going forward. It may also mean checking whether certain products can still be sold on the market.

Another early step is to ensure that all data potentially relevant to the investigation is preserved. This may entail a wide range of measures, from issuing a data hold to suspending auto-delete functions to immediately imaging data carriers. These measures play an important role in dissuading local prosecutors from performing dawn raids. If one can demonstrate that all relevant data has been stored securely, it may even be disproportionate for prosecutors to raid companies.

The investigation team then has to decide who will formally lead the investigation. The question often comes down to whether this is done by in-house counsel or external lawyers. In this regard, the sensitivity of the matter and privilege protection will often be decisive factors. The rule of thumb is that countries in Continental Europe often award very little privilege protection to in-house counsel. This can even mean that work product of outside counsel in the custody of in-house counsel of the company could be confiscated and reviewed by the authorities in some jurisdictions. Therefore, the decision is not only who runs the investigation, but also where to generate and store sensitive work product.

When collecting and reviewing information, data privacy laws have to be considered. The good news is that a uniform European Data Privacy Regulation came into force in 2018. This reduced the impact of local law specifics. On the other hand, local law specifics are not completely abolished as for example certain labor laws or criminal laws may contain stricter provisions on data handling. In addition, potential penalties substantially increased and rules became more stringent. Given the potential legal exposure and the complexity of the issue, it is strongly recommended that expert data privacy counsel be part of any cross-border investigation team in all phases. Another specific issue in cross-border cases is the "export" of data to other countries. This can be particularly problematic if such countries do not have an equivalent level of data privacy protection compared to the European Union. This may necessitate a case-by-case analysis and may also call for additional protective measures like reducing data amounts or redacting personal information before any data transfer.

The right of participation of works councils and/or trade unions during an investigation may also need to be considered. Local laws will have different views in this regard. A mistake in this area can have serious consequences. It cannot only damage the relationship between the company and its employees, but can also lead to the end or at least to an interruption of the investigation itself. Disregarding the rights of a works council may allow this body to obtain a cease-and-desist order against the investigation.

Interviews often also raise various legal issues, such as the need for data privacy waivers and the need for special instructions on the right to not self-incriminate or the right to legal counsel. Each jurisdiction has its own rules and best practices in this regard. If an interviewee is not properly instructed or the interview is otherwise not done correctly, these issues can lead to evidence being deemed inadmissible down the road.

THE END OF THE INVESTIGATION

Questions arising at the end of an investigation may also vary from one jurisdiction to the other. However, some issues are frequently in focus in many countries.

The first question, which comes up rather frequently, is whether a detailed investigation report should be produced or not. This is, again, linked to the question of privilege. If in-house counsel produces an investigation report, this report may not be privileged in many countries on the European continent. Even if outside counsel produces the report, it may have only limited protection if it enters into the custody of the company. In some countries, authorities may view the waiver of privilege and production of the report as necessary to demonstrate good will and cooperation. There may then be pressure to produce such a report.

Another step at the end of the life cycle of an investigation is remediation. Firstly, this may make an update of internal processes necessary. What is legally possible and state of the art with respect to internal guidelines may differ greatly, especially throughout Europe. For companies operating in multiple jurisdictions, it may be necessary to conform worldwide internal guidelines to the higher legal standard in the home jurisdiction, even though a lower standard may be permissible in local jurisdictions. In the end, it is often in the home jurisdiction where the biggest risks lie. Secondly, personnel measures like warning letters, trainings and terminations will play an important role in any remediation. In this regard, it is important to note that countries may have different deadlines for implementing personnel measures. If the deadlines are missed, personnel measures may not be taken for that reason alone. Furthermore, it may again be necessary to involve works councils or trade unions in such processes. The prerequisites for termination will also differ greatly among countries. For example, it may be much easier to terminate an employee in the United Kingdom than in France or Germany.

Finally, a step that is sometimes missed at the end of an investigation is recovery. In many countries, board members are responsible for compliance in companies. If a major compliance failure arises, board members may be liable to the company if they had knowledge of the conduct or if they had responsibility for the respective compliance topic and failed to implement an appropriate compliance system. The company may then even be under a duty to assess such claims against its own board members and – if there is substance to such claims – pursue them. This may even mean that, if the company or the management of the company fail to assess and pursue such claims, those responsible for the assessment may themselves be liable for the omission. In Germany, for example, this can even lead to the criminal liability of the supervisory board for breach of fiduciary duties.

CONCLUSION

Many steps have to be kept in mind when doing a cross-border investigation in or involving Europe. Issues can arise at every stage in the life cycle of an investigation. It is not necessary to know all the answers from the beginning, but important to ask the right questions. Once a potential issue has been identified, the investigative process can be set up and managed in a way that minimizes risks.

AUTHORS

Dr. Sebastian Lach
Partner
Hogan Lovells Munich
T +49 89 29012 187
sebastian.lach@hoganlovells.com

Sebastian Lach is partner at Hogan Lovells Munich and head of the German IWCF practice. Sebastian Lach handles compliance and investigation issues, as well as complex product safety and liability cases. In the field of compliance and investigations, he has advised various clients on the creation of global compliance systems. Sebastian has successfully advised on criminal matters (e.g. bribery, fraud, embezzlement) and internal investigations relating to more than 50 countries worldwide, including FCPA, SEC/DOJ implications. Throughout his career, he has handled more than 20 multi-jurisdictional investigations, most of them for Fortune 500 and DAX 30 clients.

Désirée Maier
Partner
Hogan Lovells Munich
T +49 89 29012 289
desiree.maier@hoganlovells.com

Désirée Maier focuses on white collar, compliance and internal investigations. She advises national and international clients from various industries, in particular life sciences, on all issues of compliance.

One focus of her work lies in the set-up and management of internal compliance investigations. She has particular experience in advising during dawn raids, conducting cross-border compliance investigations, as well as in communicating with German, U.S., and other authorities.

Désirée also advises clients on the establishment and enforcement of global compliance systems. Moreover, she has expertise in supporting clients in the defense against criminal law charges and providing advice on recovery issues in relation to claims arising from compliance matters.

Désirée also worked in the U.S. legal department of a world's leading U.S. pharmaceutical company (Fortune 500) with a global responsibility for investigations.

Data Privacy in Investigations

*Companies must observe strict data protection law requirements when conducting an internal investigation. The European General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), which became effective on 25 May 2018, provides a uniform set of rules for data processing throughout the European Union, replacing the existing patchwork of national laws governing how personal data is handled. Under the GDPR, new rules impose stricter and more detailed obligations for companies processing personal data, including extensive accountability obligations. Failure to demonstrate compliance with these rules could lead to claims for damages as well as administrative sanctions and high fines from the competent data protection authorities. In addition, despite harmonization on the European level, national differences must be taken into account, such as specific national law provisions in the area of processing of employee data that can have a substantial impact on how internal investigations can effectively be conducted.*

The following sections shall provide a general overview on the requirements and conditions for internal investigations under the GDPR. The text also highlights the relevant case-law and the potential consequences of unlawful processing.

WHAT IS THE LEGAL BASIS FOR PERFORMING INTERNAL INVESTIGATIONS UNDER THE GDPR?

Companies may only perform internal investigations if they can base the respective data processing operations on a valid legal basis. The appropriate legal basis depends on the purpose of the investigation, the categories of data subjects affected, and the nature of the data concerned.

- **Legal obligation to perform investigation:** Under certain conditions, companies may be legally obliged to perform an internal investigation. In this case, the company may base the data processing on Article 6(1) lit. c GDPR. However, such cases will likely to remain an exception in practice.
- **Data processing due to legitimate interests:** Companies may justify the data processing to the extent the processing is necessary for legitimate interests pursued by the company or a third party (Article 6(1) lit. f GDPR), provided that the legitimate interests of the affected data subjects do not supersede. This requires a thorough balancing of interests, taking into account all circumstances of the individual case, including the extent of the investigation, the nature of the data processed, the reasonable expectations of the data subjects and the potential consequences for their rights and freedoms. The envisaged processing activities are not admissible if there are less intrusive measures to achieve the purposes of the investigation. A key aspect of the balancing of interests will be the safeguards implemented to reduce the impact on the data subject and to ensure a proportionate approach in compliance with the data protection principles (see below). The balancing of interests should be thoroughly documented.
- **Consent of data subject:** The GDPR stipulates strict requirements for obtaining valid consent, including, in particular, that consent must be freely given. This means that data subjects must have a real choice to agree to the related processing of their personal data or not, and also to withdraw any consent given at any time. Therefore, consent is not advisable as a general legal basis for permitting an internal investigation. In particular within an employment context, due to the imbalance between the employee and the employer, consent will likely not be considered voluntary. This may potentially be different where the processing implies any legal or economic advantage for the employee or the employer and employee pursue similar interests, such as in limited scenarios for certain types of custodians or whistleblowers who are free to provide their consent or not.
- **Collective agreements:** Collective agreements (in particular works council agreements) may also form a legal basis for internal investigations. However, collective agreements which are intended to legitimize data processing must comply with the specific requirements of Article 88 GDPR and potential national implementations laws (see below).

If the internal investigation also involves special categories of personal data within the meaning of Article 9(1) GDPR (e.g., race, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, health data), additional restrictions apply. Companies may only process sensitive data if they can rely, in addition to a legal basis

under Art. 6(1) GDPR as set out above, on one of the exemptions stated in Article 9(2) GDPR. In particular, companies may process sensitive data to the extent necessary for the establishment, exercise or defense of legal claims (Article 9(2) lit. g GDPR). On the other hand, companies cannot legitimize the processing of sensitive data merely on the basis of their legitimate interests.

WHAT OTHER REQUIREMENTS DO COMPANIES HAVE TO CONSIDER?

Apart from the aforementioned restrictions, the GDPR (and national implementation laws, where applicable) provides for additional requirements and conditions for internal investigations.

- **Compliance with data protection principles:** When performing internal investigations, companies have to comply with the general principles of data processing set out in Article 5 GDPR (i.e., lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation and integrity, and confidentiality). In particular, companies should carefully assess whether the intended processing of personal data is limited to what is necessary and whether all data is in fact adequate and relevant for the investigation. Where possible, companies should only process data which have been anonymized or pseudonymized. Proportionality is a key aspect and may require, among other things, a thorough definition of search terms, a limitation of the group of data subjects concerned, the use of automated filtering, the implementation of pseudonymization, and other safeguards.
- **Considering national implementation laws:** National implementation laws to the GDPR and other legal national particularities may provide for additional requirements for internal investigations. As an example, the German Federal Data Protection Act ("**BDSG**") imposes strict requirements on companies willing to perform internal investigations in the employment context. In addition, German law is interpreted to impose strict limits on the possibilities of an employer to access and review electronic communications of its employees, such as emails, where private use of the employer's IT and communication systems is permitted.
- **Accountability obligations:** The GDPR imposes strict accountability and documentation obligations on companies (Article 5(2), Article 24(1) GDPR). In particular, companies must not only take all measures to ensure compliance with data protection laws but also be able to prove, such as in the case of enquiries from the data protection authorities, that they have performed the internal investigation in accordance with the GDPR. To comply with these obligations, companies should establish a documented data protection concept and investigation plan setting out the legal considerations and all technical and organizational safeguards implemented for conducting the internal investigation and should comprehensively document every step taken.
- **Information of data subjects:** In general, companies must inform affected data subjects about the processing of their personal data in advance (Articles 12 *et seq*. GDPR). This applies, in principle, also in case of internal investigations. However, the success of the investigation might be at risk if the suspect is informed about the envisaged data processing in advance. The GDPR does not provide for explicit exceptions to the notification requirements for such cases. The national implementation laws, however, may include respective provisions. For instance, under German law, companies do not have to inform data subjects in certain scenarios where the information would impair the establishment, exercise or defense of legal claims. However, there is no uniform implementation on national level across Europe. Therefore, companies should carefully assess in each case to what extent national exceptions can be relied upon. Whenever possible, companies should inform affected data subjects prior to the investigation.
- **Data transfer to third parties:** It might be necessary for companies to transfer personal data to third parties outside the company, either to analyze the information with the help of external advisors or to share the results of an investigation with third parties, such as in case of disclosures to courts or law enforcement authorities. Such data transfers, however, must also comply with the requirements of the GDPR. Where external service

providers are involved, acting only as processors on behalf and in accordance with the instructions of the company conducting the investigation, the data can likely be shared provided an appropriate data processing agreement is entered into which reflects the requirements under Art. 28 GDPR. In other data transfer scenarios to controllers, companies will have to thoroughly assess whether and on which legal basis the data can be shared and what safeguards need to be implemented to protect the personal data. To reduce the impact on the rights and freedoms of data subjects, the authorities require companies to take a layered approach, in particular in case of cross-border disclosures of personal data involving the transfer of only anonymized or pseudonymized data. In addition, the transfer of personal data to recipients in third countries outside the European Economic Area is only permitted where the strict requirements for international data transfers according to Articles 44 *et seq*. GDPR are met. Safeguards may need to be implemented to ensure an adequate protection of personal data, such as entering into additional agreements with the recipients outside the European Economic Area.

- **Data protection impact assessment ("DPIA"):** Generally, data controllers must perform a DPIA if the envisaged data processing is likely to result in a high risk to the freedom and rights of data subjects (Article 24 GDPR). In many cases, in particular cases involving the automated processing of large data sets, internal investigations can have such a potential impact on the rights and freedoms of the affected data subjects. To avoid legal risks, companies should perform a DPIA prior to any investigation.
- **General data protection law requirements:** As for any other processing of personal data, the general requirements under the GDPR must be complied with, such as establishing appropriate records of processing activities (Art. 30 GDPR), ensuring compliance with the principles of data protection by design and by default (Art. 25 GDPR), and implementing appropriate technical and organizational security measures appropriate to the risks for the protection of personal data (Article 32 GDPR).
- **Co-determinations rights of works council:** In some countries it may be necessary to involve the local works council in advance. Investigation measures which the works council did not consent to might be invalid. In addition, the works council might seek a preliminary injunction to ban the employer from performing the investigation.

WHAT MAY BE THE CONSEQUENCES OF UNLAWFUL PROCESSING?

Companies which do not consider the aforementioned requirements and conditions may face high legal risks when processing personal data in the course of internal investigations.

- **Administrative fines/criminal liability:** Companies which do not comply with the strict requirements of the GDPR may face administrative fines up to €20 million or four percent of their total global turnover for the previous year, whichever is higher. In case of company groups, there is the risk that data protection authorities will calculate fines on the basis of the consolidated revenue of the group. Additionally, national implementation laws as well as national criminal codes may provide for criminal liability in case of unlawful processing.
- **Exclusion of evidence:** In case of unlawful processing, the company may not be able to use the findings of the internal investigation in court. This aspect is particularly important if the company has imposed sanctions (e.g. a dismissal) against an employee due to the findings of the internal investigation. If the employee challenges the lawfulness of the dismissal in court, the company has to show that it has performed the respective data processing in accordance with the applicable data protection laws. If the court deems the data processing as unlawful, the findings may be excluded as evidence and the dismissal might be invalidated.
- **Claim for damages by affected data subjects:** Data subjects whose personal data have not been processed in accordance with the GDPR may claim damages from the company. Those claims may refer to material and non-material losses due to the infringement.

WHICH CURRENT CASE LAW IS RELEVANT FOR INTERNAL INVESTIGATIONS?

In January 2016, the European Court of Human Rights ("**ECHR**") rendered an important decision regarding the secret monitoring of employee communication (application No. 61496/08). In the so-called "Bărbulescu" case, the ECHR ruled that employers violate the employees' fundamental right to respect for private life and communication (Article 8 European Convention of Human Rights) if they secretly monitor their employees' messenger communication without implementing appropriate safeguards to preserve the employees' legitimate interests.

According to the ECHR, employers are generally allowed to monitor their employees' communication to a certain degree. Such monitoring measures, however, must be accompanied by adequate and sufficient safeguards to preserve the employees right to privacy. In particular, employers must generally inform their employees about the envisaged monitoring in advance. This notification must include detailed information on the nature, the extent of the monitoring and the degree of intrusion.

In addition, employers need to provide for legitimate reasons to justify the monitoring of employee communication. In this context, the ECHR particularly refers to the principle of data minimization. The employers must prove that there is no less intrusive measure to reach the envisaged purposes.

The criteria established for the monitoring of employees were further refined in a recent decision of the ECHR in the Ribalda case (applications Nos. 1874/13 and 8567/13) in October 2019. The court ruled that a covert video surveillance of employees does not violate the employees' fundamental rights for private life and communication (Article 8 European Convention of Human Rights) and the knowledge gained by the employer may be used as justification for the dismissal.

The case revolved about the fact that in a Spanish supermarket over a period of several months merchandise worth between €8,000 and €25,000 per month disappeared – with increasing tendency. The employer used covert video surveillance to identify the guilty parties (a group of cashiers and sales assistants) who were then dismissed. The Grand Chamber decided that – while covert video surveillance is not justified for every slightest suspicion of misappropriation or wrongdoing –the video surveillance in the specific case was lawful despite the fact that employees had not been informed in advance about the monitoring by the employer. The case is different than the Bărbulescu case (where also no prior information was given) because the Bărbulescu case concerned the general monitoring of an employee's activities during working hours, while in the Ribalda case there was concrete suspicion of a crime causing considerable damage. The ECHR weighed the protection of the privacy of employees against the protection of the employer's property and business operations, considering that there was a legitimate aim because of concrete and reasonable suspicion of a serious misconduct causing a substantial extent of losses and endangering the smooth function of the company, the employees' expectation as to the protection of their private life was limited (because employees were monitored not in very private areas (such as toilets or locker rooms or closed working areas) but in areas open to public (such as checkout counters) where their privacy was in any event restricted by the permanent contact with customers, and the activities filmed were not of an intimate or private nature), the duration had not exceeded what was necessary in order to confirm the suspicions of theft, and the measures were appropriate and proportionate as there were no other less intrusive means to achieve the legitimate aim. While the court stressed the importance of appropriate prior information, the lack of information in the specific case was considered just one of the criteria to be taken into account in order to assess the proportionality of the measures taken and other safeguards were sufficient to justify the overall balancing in favor of the employer.

Although the Bărbulescu and Ribalda decisions did not directly refer to the GDPR, the decisions are generally understood to interpret the accepted principles under the European Convention which remain applicable under the GDPR. Therefore, companies are well advised to consider the criteria established by the ECHR when conducting international investigations.

CONCLUSION

The GDPR and the national implementation laws, if applicable, set strict limits for conducting internal investigations. Companies have to deal with a variety of requirements and obligations. To ensure compliance with data protection laws, companies should carefully assess the individual circumstances and legal requirements for each investigation. Companies are well advised to establish a professional data protection concept and investigation plan, including appropriate internal procedures and technical and organizational safeguards, enabling the company to effectively manage the internal investigation in line with legal requirements. The steps taken should be documented in order to be able to demonstrate compliance with the GDPR. Otherwise, companies may face serious sanctions, data subject damage claims, reputational damage and exclusion of evidence due to unlawful processing.

AUTHOR

Dr. Martin Pflüger

Partner
Hogan Lovells Munich
T +49 89 29012 440
martin.pflueger@hoganlovells.com

Since the early days of his career, Martin Pflueger has been focusing his practice on advice in the area of information technology, Internet, e-commerce and data protection law, with a focus on the technology, automotive and life sciences industry. Not only from his various secondments with clients in the technology and pharmaceutical sector, including as European privacy counsel for a worldwide leading cloud computing service provider, Martin brings extensive experience in drafting and negotiating IT agreements, evaluating new technologies and business models as well as advising clients on all aspects of European and German data protection law.

Martin is recognized for having a deep understanding of the expectations and legal challenges clients are facing in connection with complex technology or outsourcing projects, the implementation of business processes in the field of Internet and e-commerce matters, or the handling of personal data. He regularly advises clients on IT/IP related aspects in various commercial and corporate transactions. Martin's privacy practice covers all aspects of European and German data protection law, including the coordination of multi-jurisdictional projects on European and international level – whether you are looking at setting-up your cross-border transfers of personal data (including implementing Binding Corporate Rules), managing your internal investigations or compliance systems, or at dealing with the particularities for the processing of employee or health data, whether you need assistance with the drafting of privacy policies or data transfer agreements, or whether you seek advice on topics such as Artificial Intelligence, Big Data, Connected Cars or the Internet of Things. He regularly assists companies in relation to GDPR compliance audits and implementation projects.

Legal Framework for Money Laundering in Europe

INTRODUCTION

An estimated two to five percent of the Global Gross Domestic Product ("**GDP**") is the result of money laundering. Money launderers prefer countries with solid financial markets and financial services, high GDP, high exports and imports and, of course, with a rather lax anti-money laundering regime and low fines.

According to a study from the European Parliament dated 2017, this issue poses a particular threat to large European countries. The United Kingdom tops the list with an estimated total of €282 billion laundered annually, followed by France, Belgium, Germany, Luxembourg, the Netherlands, and Austria. Compared to their GDP, the Baltic States, Luxembourg and Cyprus have a disproportionate volume of money laundering.

In Europe, a number of steps to combat money laundering have been undertaken, such as five EU Anti-Money Laundering Directives, the latest of which was enacted in May 2018 and entered into force on 9 July 2018 ("**AMLD5**"), only three years after its predecessor ("**AMLD4**") which was enacted in May 2015. The member states were required to bring into force the laws, regulations and administrative provisions necessary to comply with AMLD5 by 10 January 2020 ("**AML laws**"). However, the above-mentioned European Parliament study came to the conclusion that in order to reach a harmonized anti-money laundering policy in Europe, a "one size fits all"-approach is not promising as European countries differ significantly in their administrative and economic (infra)structures to reach the same level of compliance. The study further concluded that the European Union could be subdivided into at least four groups of countries to be targeted differently. The study stressed the important role of advanced member states, in training less advanced countries to create a common understanding of the need for anti-money laundering.

In recent years, the competent local authorities have published general guidelines to inform the obliged entities about the applicable due diligence and organizational requirements. As a further step, several thousand audits have been performed in the member states to evaluate the status quo and pave the way for further action against those who do not comply with the requirements of the AML laws. The most recent reports demonstrate that administrative fines have been levied against traders of goods. The most common reasons have been:

- The official identification document was not fully copied during the customer identification process.
- The obliged entity cannot prove that it has obtained appropriate confirmation whether or not the contracting party is acting on behalf of a beneficial owner.
- The obliged entity cannot prove that it has verified the obtained customer data on the basis of an appropriate official identification document.

OBLIGED ENTITIES UNDER AML LAWS

It is a widespread misconception that only financial institutions and the related industry must undertake appropriate measures in the European Union to comply with AML laws. So-called traders of goods are subject to the same legal requirements. Other affected parties are lawyers, auditors, tax advisors, real estate agents (including when acting as intermediaries in the letting of immovable property), casinos, art traders (i.e. persons storing, trading or acting as intermediaries in the trade of works of art) and operators and brokers of online gambling platforms as well as custodian wallet providers and virtual currency exchange service providers.

CRIMINAL AND ADMINISTRATIVE LIABILITY

The member states must ensure that obliged entities can be held liable for breaches of AML laws. Furthermore, the member states have the right to provide for and impose penalties under criminal law and must lay down rules on administrative measures to ensure that their competent authorities may enforce AML rules and regulations. In addition, member states must ensure that their competent authorities promptly report any identified criminal offenses to their law enforcement authorities.

With regard to criminal liability, some member states previously excluded "self-laundering" from money laundering as a criminal offense. The reason for the previous exclusion was that if, for example, a person stole money and was prosecuted for both theft and money laundering, this was seen as an inadmissible double punishment. However, under strong pressure from the Financial Action Task Force on Money Laundering ("**FATF**"), all countries have meanwhile amended their laws, declaring self-laundering a money laundering crime. Germany was the last country to amend its laws accordingly in November 2015.

Administrative sanctions and measures apply to breaches on the part of obliged entities that are serious, repeated, systematic, or a combination thereof, of the requirements for:

- Customer due diligence;
- Suspicious transaction reporting;
- Record-keeping; and
- Internal control measures.

Member states must ensure that in these cases, the administrative sanctions and measures include at least:

- A public statement which identifies the natural or legal person and the nature of the breach;
- An order requiring the natural or legal person to cease the conduct and to desist from repetition of that conduct;
- Withdrawal or suspension of the authorization where an obliged entity is subject to an authorization;
- A temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person, held responsible for the breach, from exercising managerial functions in obliged entities;
- Maximum administrative fines of at least twice the amount of the benefit derived from the breach where that benefit can be determined, or at least €1 million.

SUPERVISION OF AML LAWS

Member states are required to appoint competent authorities to effectively supervise obliged entities and in particular to monitor the adherence and take the measures necessary to ensure compliance with the AML laws. In this context it is important that member states provide to the competent authorities adequate powers of enforcement, including the power to demand any information that is relevant to monitoring compliance and to perform external audits.

More specifically, the standard under European AML rules requires that the competent authorities have on-site and off-site access to all relevant information on particular domestic and international risks associated with clients, products and services of the obliged entities. Regarding the frequency and intensity of on-site and off-site supervision, competent authorities will consider the individual risk profile of obliged entities and the risks of money laundering and terrorist financing in the respective member state.

OBLIGATIONS UNDER AML LAWS

Compliance with the requirements of the AML laws mainly consists of satisfying two high-level obligations:

- Organizational requirements; and
- Customer due diligence requirements.

RISK ANALYSIS

Obliged entities are required to rate individual business relationships and transactions in light of their respective money laundering risk (risk-based approach). The results of the risk assessment must be documented. It should describe the potential risks associated with the business of the obliged entity which can be divided into the following categories:

- Company risks;
- Customer risks;
- Product risks;
- Transactional risk; and
- Geographic risks.

The relevant risk factors were specified in Appendices I and II to AMLD4. As soon as the potential risks have been determined and described, it is the task of the obliged entity to determine to what extent they may actually materialize. Depending on the risk levels (i.e. risk-based approach), preventive measures and safeguards may be implemented. The risk assessment must also be updated at least once a year in order to ensure the effectiveness of the preventive measures and safeguards.

MONEY LAUNDERING REPORTING OFFICER

The essential element of compliance with AML laws lies in an appropriate internal organization. Even if this is only required for certain entities (where appropriate with regard to the size and nature of the business), the appointment of a money laundering reporting officer ("**MLRO**") is recommendable, to bear responsibility for the development of internal policies, procedures and controls, including risk analysis and risk management measures, customer due diligence, reporting, record keeping, internal control, and employee screening. The MLRO is also entitled to report suspicious events to the central office for financial transaction investigations (Financial Intelligence Unit – "**FIU**"). The position of the MLRO was generally strengthened by the latest amendments of AMLD4, as the fulfillment of his or her duties may not lead to any disadvantages in the employment relationship. The clear organizational responsibility for this task is the foundation for compliance with the AML laws.

AML MANUAL

With the confidential risk assessment in place, the next element of the compliance structure – the AML manual – can be drafted and implemented. The AML manual describes the internal processes and activities to be implemented by the company to ensure compliance with legal requirements. Amongst other matters, the manual includes regulations for client identification, the document or software system to be used, the escalation process for on-boarding politically exposed persons, as well as record keeping and retention requirements and the internal procedure to report suspicious activities to the MLRO and other corporate governance provisions.

AML POLICY

Each obliged entity must implement appropriate processes and train employees on the types and current methods of money laundering and terrorist financing. This requirement can be met through an AML policy where each employee receives general information on money laundering and appropriate obligations. The training should be repeated at regular intervals depending on the respective AML risk of the obliged entity; market standard is every two years. It is also important to document all employees' attendance of the training sessions to ensure compliance with the AML provisions.

INTERNAL CONTROLS

With the AML manual and the AML policy in place, the company and all employees must implement the internal requirements in practice. One of the central tasks is the performance of customer due diligence. More generally, it is important to monitor the business activities and effectiveness of the implemented preventive measures and safeguards.

CENTRAL REGISTER OF BENEFICIAL OWNERS

In order to obtain and store information on beneficial owners, all member states are required to set up a central register of beneficial owners. All legal persons under private law as well as all registered partnerships must collect, hold, and provide beneficial ownership information and communicate this information to the central register. AMLD5 improved public access to beneficial ownership information. There is no longer a need to demonstrate a legitimate interest to access the central register. Public access to beneficial ownership information allows greater scrutiny of information by civil society, including by the press or civil society organizations, and contributes to preserving trust in the integrity of business transactions and of the financial system. However, some restrictions continue to apply as access to beneficial ownership information of trusts and similar legal arrangements should only be granted to any person that can demonstrate a legitimate interest.

CRIMINAL LIABILTY

In order to complement and reinforce the application of AMLD5, a directive on combating money laundering by criminal law was adopted on 23 October 2018 ("**AMLD6**"). It lays down minimum rules on criminal liability for money laundering. Member states are obliged to transpose the requirements into national law by 3 December 2020. In particular, AMLD6 harmonizes the definitions of money laundering and predicate offenses, lays down minimum sanctions, and extends criminal liability to legal persons.

CONCLUSION

To meet AML compliance in practice, it is market standard that obliged entities produce three documents: a risk analysis, an AML manual and an AML policy, all tailored to their respective business model and the entailing AML risks. The risk-based approach allows an individual set of measures depending on the respective level of risk, i.e. fewer measures in case of lower risks. Most importantly, the documentation provides protection against reputational harm and external challenges by supervisory authorities.

AUTHORS

Dr. Richard Reimer
Partner
Hogan Lovells Frankfurt
T +49 69 962 36 414
richard.reimer@hoganlovells.com

Richard Reimer advises German and international banks and financial institutions on all aspects of banking regulation and compliance, with a particular focus on payments and e-money law. Furthermore, Richard advises on regulatory aspects of M&A transactions involving banks and financial institutions (e.g. ownership control proceedings). He has dealt with major portfolio transactions of the firm involving bad banks. He is part of the investment fund team and contributes to all regulatory aspects in structuring investments (UCITS and AIF) in Germany. Richard leads a team which primarily advises on banking license proceedings, own funds requirements and compliance projects including whistleblowing systems, anti-money laundering compliance and financial sanctions.

Sarah Wrage, LL.M.
Senior Associate
Hogan Lovells Frankfurt
T +49 69 962 36 421
sarah.wrage@hoganlovells.com

Sarah Wrage advises German and international banks and financial services institutions as well as other companies on all aspects relating to banking regulatory law, payment services law and investment law. The main focus of her work is to give advice on licensing, capital requirements, duty of care and organizational requirements, compliance, and regulatory implications of transactions. Furthermore, Sarah assists her clients in the implementation of new financial products, particularly in the payment area.

In investment law, Sarah primarily offers advice and support to asset management companies, investment fund managers and investors regarding the structuring and setting up of investment funds as well as the permissibility of investments and the distribution of funds.

Cartel Investigations

CARTEL INVESTIGATIONS STILL ON THE RISE

Competition law has proven to be a high-risk area for companies in many different industries all over the world. Multi-jurisdictional cartel investigations are of increasing importance to businesses around the globe, with legal and compliance departments investing heavily in competition expertise. This is also true for the European Union where both the European Commission ("**Commission**") and National Competition Authorities ("**NCA**") are taking a clear stance on competition law violations. The recent investments by the Commission into digital investigation intelligence, a newly established data analysis unit, and the whistleblower hotline are starting to pay off for the enforcer: According to the Commission, 25 percent of the currently opened cartel investigations are started by the Commission on its own initiative.

In recent years, the Commission has also expanded its enforcement focus to industries which had not been in the spotlight in the past, like financial services or digital markets. Further, the Commission has targeted some atypical cartel cases which are based on rather novel theories of harm. This adds further uncertainty to the cartel proceedings. Big data, algorithms and competition for innovation have become buzzwords for modern competition law enforcement and we expect to see a further rise in antitrust investigations in these industries, both on an EU level as well as on a national level within the EU Member States.

When it comes to cartel investigations, being prepared is key to being able to react appropriately during a dawn raid and master the subsequent proceedings in the best possible way for the company. In the following paragraphs we will provide an overview of the legal framework, the relevant institutions, and the different stages of a typical Commission cartel investigation.

LEGAL FRAMEWORK AND RELEVANT INSTITUTIONS

The Treaty on the Functioning of the European Union ("**TFEU**") provides the rules to implement a system of undistorted competition, substantially unchanged for decades. Investigations into alleged cartels or other forms of anti-competitive agreements between companies (Article 101 TFEU) as well as unilateral measures by market dominant companies (Article 102 TFEU) constitute an important pillar of European competition law enforcement. Both provisions are directly applicable in all EU Member States and can be enforced by the Commission as well as by NCAs.

Council Regulation (EC) No. 1/2003 ("Regulation 1/2003") sets out the Commission's powers during the different stages of an investigation. The Commission has published best practice guidelines as well as an internal manual of procedures which provide useful information on how the Directorate General for Competition ("**DG Competition**") runs investigations.

The Commission acts as the European competition law enforcer. Regulation 1/2003 grants considerable powers to the European Union's executive body to ensure that the Commission can effectively guard the adherence to competition law rules in the Treaty. Within the Commission there are generally two hearing officers responsible for ensuring the rights of accused undertakings, especially impartiality and objectivity of competition proceedings.

The Commission also takes a central role in the European Competition Network ("**ECN**"). The ECN consists of the Commission and the NCAs in the EU Member States. The ECN provides means to ensure an effective and coherent cross-border application and enforcement of competition law within the European Union.

Upon appeal, Commission decisions in cartel cases are subject to examination by the General Court (formerly referred to as Court of First Instance). Ultimately, the European Court of Justice ("**ECJ**") is responsible for appeals on the point of law against General Court decisions.

Considering the complexity of EU level cartel investigations and the authorities involved, it comes as no surprise that cartel cases may last many years starting from the authorities' first investigative steps to a final potential decision by the ECJ.

OVERVIEW OF A TYPICAL EU COMMISSION CARTEL INVESTIGATION

Initiation of Proceedings

The Commission can start proceedings either on its own initiative, on the basis of a third-party complaint, or via a leniency applicant blowing the whistle on a cartel conspiracy. While third-party complaints usually mark the beginning of an abuse of dominance-probe, cartel cases are often triggered by leniency applications which are followed by dawn raids. The Commission stated that it has significantly increased the number of cartel investigations opened at the Commission's own initiative to 25 percent of the currently launched investigations. This mainly results from the Commission's investments into digital investigation intelligence, the whistleblower hotline, and its newly established data analysis unit which uses data-mining and algorithms to scour information for specific patterns indicating collusion.

a) Leniency Applications

Leniency applications mark the typical start of a Commission investigation into an alleged cartel. In order to win the race for leniency, an undertaking can set a "marker" with DG Competition, i.e. file an abridged application for a reduction of fines and submit detailed information within a certain period of time thereafter in order to secure its rank under the Leniency Program. Cooperating with the Commission in the investigation can result in full immunity from fines for being first-in or substantial fine reductions for subsequent applications. The different cooperation scenarios are laid out in the Commission Notice on Immunity from fines and reduction of fines in cartel cases ("**Leniency Notice**").

b) Dawn Raids

DG Competition has extensive powers to conduct unannounced inspections ("**dawn raids**") when there is an early suspicion of competition law infringements. As long as the scope of the inspection is limited to business premises, no judicial search warrant is needed. Commission inspectors – usually supported by national inspectors – make use of their extensive rights. Undertakings are liable for obstructions of these inspections such as destroying or withholding of evidence with potential fines of up to one percent of the undertaking's annual turnover. On site, the Commission is empowered to examine books and business records both in digital and hard copy format, take copies, seal particular objects, and interview employees at all levels (Article 20 Regulation 1/2003).

In recent years the Commission's focus has shifted towards e-dawn raids where the Commission requests large amounts of electronic data which it then reviews on its own mobile servers at the undertaking's premises.

Dawn raids hit companies rather unexpectedly and are often disturbing for the operational business. As mistakes during the dawn raid can be very costly and may jeopardize the companies and employees' defense position, dawn raid preparation is key. It is highly advisable to have a specific process for Commission dawn raids with designated antitrust advisors established to regularly train the in-house dawn raid team, and to have IT system administrators trained and prepared to provide the inspectors with easy access to the IT infrastructure.

A very sensitive and important topic throughout the entire investigation and specifically during a dawn raid is the protection of legally privileged documents. Generally speaking, only communication with or prepared for, external lawyers, which have taken place after the initiation of the administrative proceedings, can be legally privileged under EU law and can therefore be withheld from inspection. Prior communications can only be regarded as privileged where they relate to the subject matter of the procedure. Other documents and data need to be provided upon request as long as they fall within the scope of the investigation.

The duration of such inspections depends – amongst other factors – on the scope of the investigation, the company's size, and the amount of data requested by the Commission. Inspections at the companies' premises

can last several days and may be continued at DG Competition's offices in Brussels if the data volume to be reviewed by the officials is very large.

Additional Investigative Powers

Before the Commission initiates formal proceedings, it gathers information relevant to the specific sectors in order to uncover competition law infringements and to collect evidence of such alleged violations. Commission investigations are driven by the *ex officio* principle. The authority is under a duty to investigate all facts relevant to the case diligently and impartially. In addition to the powerful investigative tool of dawn raids, Regulation 1/2003 equips the Commission with a range of additional powers typically applied by DG Competition in cartel investigations:

- **Requests for information:** In order to carry out its duties under Regulation 1/2003, the Commission may issue a Request for Information (Article 18 Regulation 1/2003). The submission of incorrect or misleading information can be fined with up to one percent of the undertaking's total annual turnover (Article 23(1)(a) Regulation 1/2003).
- **Power to take statements:** Further, the Commission has the power to take statements and may interview any natural or legal person for the purpose of collecting information relating to the subject-matter of the investigation (Article 19 Regulation 1/2003).

Initiation of Formal Proceedings, Statement of Objections and Oral Hearing

The opening of proceedings is a formal act by the Commission which is notified to the parties and usually also to the public. The Commission can formally open the proceedings in different ways. Typically, DG Competition opens formal proceedings by issuing a so-called Statement of Objections ("**SO**") to the companies under investigation. The SO lays out the Commission's position and must contain all facts and evidence necessary for the final decision.

The main purpose of the SO is to inform the undertakings about the concrete competition law charges against them and to enable them to exercise their rights of defense. Informal meetings could be held before the SO is issued, helping the companies to understand the Commission's views on the status of the case. The cover letter to the SO explains the rights of the addressees and sets a deadline for the reply.

The issuing of the SO usually also marks the point in time where the companies under investigation receive access to the Commission's file. Access to the file is part of the companies' right to be heard and constitutes a very important element in the companies' defense strategy: It provides the opportunity to inspect any potential leniency application and consecutive statements of other cooperating parties involved in the investigation. Depending on the scope and complexity of the SO and the size of the Commission's file, companies are usually granted a period of six to 10 weeks to file their reply to the SO (**"Reply"**).

Where documents are submitted as part of the Reply, confidentiality should be claimed for those documents containing business secrets and other confidential information to prevent them from being disclosed to other parties.

In case one of the companies involved requests an Oral Hearing, this will usually take place following the Commission's receipt of the Replies. The Oral Hearing is held by the Hearing Officer and provides the Commission as well as the companies involved with a forum to discuss their case and exchange arguments on the facts and legal analysis.

Decision and Settlement

The procedure generally comes to a close with the Commission adopting its final decision in which it can impose substantial fines. In most cases the publication of the decision is preceded by a State of Play meeting. In this meeting, the Commission presents its conclusions to the company.

Only when the Commission is convinced of a competition law infringement based on meaningful and consistent evidence, it can adopt a decision and impose fines. Fines for infringements of Articles 101 and 102 TFEU can go up to 10 percent of the company's total annual turnover. In setting the fine, the Commission weighs different factors such as

gravity and duration of the infringement as well as the role of the undertaking in the infringement. The details on the fining method are laid out in the Commission's Guidelines on the method of setting fines. After years with very significant fines (€3.7 billion in 2016; €1.9 billion in 2017), the Commission again imposed accumulated fines of €0.8 billion in 2018, €1.5 billion in 2019, and €0.3 billion in 2020. With the cartel investigations currently pending in Brussels, a significant increase in fines is expected for 2021.

In recent years, many cartel cases have been settled between the Commission and the companies under investigation. Such settlements usually take place before the submission of the SO. However, recent cases have also shown that even after the submission of the SO, and even after the companies under investigation have filed their Reply to the SO, a slot for settlement negotiations with the Commission may open up. It is the essence of settlements that the settling companies acknowledge their misconduct and their liability and in return may receive an (additional) reduction of the fine of up to 10 percent based on the Commission Notice on the conduct of settlement procedures in cartel cases ("**Settlement Notice**"). On the part of the participating undertakings, this has the advantage that further money and resources can be saved as the procedure is expedited.

TYPICAL FOLLOW-ON: CARTEL DAMAGES CLAIMS

Since the Commission has no power to award damages to victims of a cartel, civil cartel damages litigation has increased significantly in recent years. Both the European Courts and the Commission have pushed this development and called for effective means to recover cartel damages before national civil courts.

Such "follow-on" litigation can prolong the lifetime of cartel cases significantly. The risks of such claims by companies who may have suffered damages, for instance through the payment of cartel overcharges, must already be carefully considered by the companies under investigation during the Commission proceedings, e.g. when determining leniency or settlement strategies.

CONCLUSION

Cartel investigations are still on the rise and constitute a high-risk area for companies around the globe, bringing along everything companies need to avoid: Cartel cases have a very long lifecycle from dawn raids to follow-on litigation, are costly, bind a lot of resources and can damage the reputation of the companies involved.

The experience shows that preparation is key for companies to master the dawn raid situation as well as the subsequent cartel proceedings in the best possible way.

AUTHORS

Dr. Christoph Wünschmann
Partner
Hogan Lovells Munich
T +49 89 29012 432
christoph.wuenschmann@hoganlovells.com

Christoph Wünschmann advises clients with a focus on German and European antitrust and merger control law.

Christoph deals with all competition aspects of M&A transactions. He handles merger filings with the European Commission and the German Federal Cartel Office and coordinates filings worldwide. He represents companies in cartel investigations and represents his clients in antitrust related court proceedings, including follow-on damages claims. Christoph also advises on all kinds of corporate and commercial agreements (joint ventures, cooperations, distribution, R&D, technology transfer) as well as abuse of dominance issues.

Christoph teaches European competition law at the MLB master class at the Freie Universität Berlin and is a regularly recommended lawyer for competition law in all major legal directories.

Christian Ritz, LL.M. (USYD)
Partner
Hogan Lovells Munich
T +49 89 29012 432
christian.ritz@hoganlovells.com

National and international clients entrust Christian Ritz with their complex German and European competition law issues. Christian can assist you with his extensive experience in cartel authority investigations, cartel damages litigation as well as compliance issues and merger control procedures. You may also seek Christian's advice on state aid law as well as regulatory issues. With a background in policy-making and government relations, Christian can assist you to get your voice heard at national as well as at EU level.

Prior to joining our firm, Christian practiced antitrust and competition law at the Berlin office of Freshfields Bruckhaus Deringer. He also gained valuable experience in the EU public policy arena while working for Alber & Geiger in Berlin and Brussels.

Export / Sanctions

Sanctions and export control issues continue to pose challenges for companies. Political developments such as the U.S. elections, Brexit, conflicts in Belarus or trade tensions demonstrate the need to keep internal compliance programs under review. Key developments in the last year include the following:

In 2020, the EU has adopted new sanctions regimes. Such regimes cover sanctions against Nicaragua, Belarus and Turkey, as well as sanctions to counter cyber-attacks. Although these regimes introduce mainly asset-freezing measures against certain parties, they have extended the spectrum of controls and reiterated the need to observe additional compliance areas. The EU is also working towards introducing a new global human rights regime similar to the Magnitsky Act in the U.S., targeting perpetrators of serious human rights violations.

Further, the EU is currently completing the process for updating the Dual-Use Regulation. The EU institutions concluded negotiations for the compromise text of the new Dual-Use Regulation on 10 November 2020, which must now be approved into law by the European Parliament and the Council of the EU. If adopted in its current form, it will impose additional obligations on EU exporters of dual-use goods and technology. The agreed updates include new catch-all controls on non-listed cyber-surveillance items that can be used for violating human rights, increased due diligence obligations on exporters seeking global export authorizations, new General Export Authorisation ("**GEA**") for intra-company technology transfers and encryption, as well as increased transparency rules. These changes are expected to increase compliance risks in this sector.

While sanctions against Iran were partially lifted by the EU in January 2016, thus creating new opportunities for companies, the Trump Administration has caused uncertainty by withdrawing from the Joint Comprehensive Plan of Action ("**JCPOA**") in May 2018 and reinstating sanctions against Iran, including recently the designation of the Bank of Iran as a Specially Designated Person ("**SDN**"). The EU's response was to boost its Blocking Regulation by including certain U.S. sanctions on Iran in its scope, thus prohibiting EU companies from complying with such U.S. sanctions and requiring an authorisation from the European Commission for doing so. However, the Blocking Regulation and reinstated U.S. sanctions on Iran often pose conflicting obligations on EU companies and consequently entail increased compliance risks. U.S. President Elect, Joe Biden, has demonstrated the willingness to negotiate the U.S.' return to the JCPOA, provided that Iran adheres to strict compliance. It remains to be seen whether the situation in Iran will change, but the country Iran remains of politically high profile.

The United Kingdom ("**UK**") left the EU on 31 January 2020 and a transitional period will apply until 31 December 2020. Both the EU and the UK have adopted contingency measures to address regulations in the areas of sanctions and export controls. In particular, the UK has adopted domestic legislation to implement its own sanctions regimes and to carry over all EU sanctions regimes in a no-deal Brexit scenario, i.e. if the EU and the UK cannot agree on a comprehensive Free Trade Agreement following the transition period. In this context, the UK has already adopted its first independent sanctions regime, the Global Human Rights Sanctions Regulations 2020, targeting persons and entities involved in human rights violations in recent years. At the same time, while the overall framework for export controls will not change, there will be new licensing requirements for trading dual-use items between the EU and the UK. The UK has published a new Open General License (OGEL) for exports to the EU, while the EU has added the UK in the list of countries subject to GEA EU001.

2020 also saw the tightening of U.S. controls on Chinese companies and Chinese-made technology in an effort to counter unfair trading practices and boost the U.S. economy. Moreover, sanctions relating to North Korea, Syria, Russia, Ukraine and Crimea, to name only a few, continue to directly impact companies' business behavior. As the EU and the U.S. play the most important role when it comes to shaping new sanctions policies, this area continues to affect many businesses worldwide.

The broad scope of many sanctions regimes and the deep impact on business relations with customers in targeted countries makes compliance with all applicable laws a permanent challenge for businesses engaging in international trade and investment. Infringements may result in heavy fines, reputational damage or even criminal prosecution. As a result, investigations of infringements – whether those occurred willfully or negligently – are a crucial instrument to

protect the integrity of a company and to ensure that it keeps control of the situation. On the positive side, national authorities in EU Member States are alive to the challenges faced in this area by companies. The possibility for voluntary disclosure covering certain infringements and the publication of detailed guidelines on designing internal compliance policies specific to trade compliance are useful contributions in an ongoing dialog between companies and authorities.

Typically, internal investigations of a potential export control or sanctions infringement are triggered by one of the following situations:

- **Internal suspicions of export control infringements.** Very often, companies themselves realize that they have erred in applying export control provisions, e.g. by relying on an incorrect general license or by not consulting the latest list of designated entities or individuals. Sometimes an initial high-level audit produces evidence that employees have engaged in restricted trade with sanctioned countries. Another example may be the incorrect "deduction" of shipped items from the total number of products for which an export license has been obtained, which might result in goods being shipped without authorisation, despite such authorisation being required under EU rules. This is a particularly difficult issue to track and may be easily caused by human mistake (e.g. due to inadequate training) or by the lack of software tools that facilitate tracking exported goods (e.g. appropriate IT systems).

  In such cases, an internal investigation is required to fully assess the gravity of the infringement, potential liability of the company and the steps required to remedy the concerns, e.g. a voluntary disclosure of the infringement to the authorities or training of the persons in charge of exports. Voluntary disclosures to avoid fines are encouraged in many jurisdictions. However, due to the different scope among EU Member States of the breadth of voluntary disclosure provisions, companies should seek legal advice before proactively making use of this procedure. This is because they may find themselves in a risky situation, including a criminal investigation, if the conduct is not covered by the scope of the applicable voluntary disclosure scheme, or if such a scheme is not provided for under applicable national legislation.

- **Official investigations by authorities.** Internal investigations may also be triggered by an external review such as an audit of the company's books without any concrete suspicion of export control issues. In such a case, a company should mirror the authority's "fishing expedition" to ensure that it has clean records. Where an authority is already investigating an alleged breach of export control or sanctions laws, the company concerned may want to investigate whether any further infringements have occurred and require immediate action.

- **M&A and financing.** Finally, investigations of potential past export control and sanctions issues and more generally of the compliance system in this field may be caused by M&A or financing projects. In the course of preparing documents for a due diligence or for corporate finance projects (issuing bonds, entering into new credit facility agreements etc.), third parties may request a statement on potential legal areas of concern and a risk assessment. In this case, companies need to investigate their compliance internally with the export control and sanctions rules applicable to them.

While an investigation in the area of export control and sanctions has many parallels with investigations in other legal areas, some specifics need to be considered.

First, the applicable legal regime and the competent authorities need to be identified. It follows from the nature of trade activities that a number of jurisdictions may need to be considered in determining which law applies to a specific transaction. Some jurisdictions such as the U.S. have a far-reaching extra-territorial scope. In particular, with regard to investigations in defense sector companies, U.S. International Traffic in Arms Regulations ("**ITAR**") controls the movement of controlled data between the EU and the U.S. This means that investigations should be structured to ensure that potentially ITAR-sensitive material is reviewed in an ITAR-compliant manner. This may limit the ability of non-U.S. citizens to be involved in the review of such data. In an internal investigation, the steering team needs to ensure that such data is identified and kept separate from other information to be reviewed. Appropriate documentation is required to

demonstrate compliance with these export control rules. Another example are U.S. secondary sanctions, which extend controls to non-U.S. companies in non-U.S. transactions that the U.S. deems as presenting risks under certain sanctions regimes. U.S. secondary sanctions increase compliance risks for EU companies and require particular vigilance in export transactions, including appropriate due diligence prior to approving "sensitive" transactions. Further, EU or Member States' law may even prohibit complying with certain sanctions other states impose through anti-boycott laws, such as the Blocking Regulation.

In the EU, export control and sanctions provisions are generally set at the EU level while the enforcement falls into the competence of Member States' authorities. Very often companies need to deal with parallel investigations by several authorities, whether that is authorities in different EU Member States, or even multiple authorities within the same Member State. It is worth noting that in the U.S., a reporting obligation for boycott requests exists regardless of whether the company complied with the request. Again, this may impact the way an investigation is structured between the EU and U.S. For instance, EU subsidiaries receiving a boycott request should make their U.S. parent entity aware of it, so that the U.S. corporation can comply with potential reporting obligations.

Second, scoping an investigation correctly facilitates a thorough review of all aspects that might be relevant both for the company and for the competent national authorities. For the former, an investigation allows identification of the deficiencies in its systems and procedures, and for the latter, it helps to have a complete overview of the remedial measures that the company concerned has taken to remedy the situation and their adequacy. Identifying the root causes of a problem might not be easy, in particular in companies with presences in several countries and complex internal structures. In cases like these, there might be elements in transactions that would not necessarily strike an auditor but which might play a big part in creating a compliance issue. Such elements are, for example, U.S.-nexus such as transactions denominated in U.S. dollars that immediately trigger U.S. sanctions rules. Another example is technology transfer, which might be a particularly sensitive issue from an export control perspective. Therefore, initiating an investigation with a broader scope than would usually be expected might prove useful in dealing with the situation in a holistic manner.

A further issue of particular importance for scoping an investigation is that sanctions rules, by their nature, can rapidly change due to political developments as demonstrated by the situation in Iran. This makes it difficult for companies to keep their compliance system up to date. For instance, from time to time entities or individuals will be added to or removed from the asset freezing and blocking of economic resources lists. In other areas, rapidly introduced sanctions sometimes make provision for the "grandfathering" of existing contracts otherwise covered under the new regime. These grandfathering provisions can differ between EU and U.S. sanctions regimes, between contracts entered into in a variety of different time frames, and sometimes only apply on a temporary basis, in effect stipulating a grace period for winding up existing contracts. Following the relaxation of EU sanctions on Iran in 2016 and the re-instatement of U.S. sanctions on Iran in 2018, the scope for disparities between the two regimes in this area has increased. This also appears to have an impact on financing by EU banks, which often request further information in relation to certain actions of EU clients if they consider that the transaction may lead to exposure under U.S. law. This raises significant difficulties for European companies doing business in Iran. In practice, before starting an investigation, a legal assessment by a sanctions law expert should be sought in order to identify the factual scope of the investigation. This aims at ensuring that the investigation uncovers all relevant material, including both incriminating and exculpatory material.

Third, investigations of export control infringements are particularly complex. Unlike in other investigations, emails often do not contain all the relevant facts required for a risk assessment. Even interviews with the key employees involved, e.g. the export control officer, do not ensure that all facts can be sufficiently established. In companies with complex internal structure and business organization, identifying the person(s) in charge of exports might prove to be a complicated exercise, given that often different employees in different positions across the supply chain are involved in dealing with exports. Many infringements therefore require a broad scope of interviews with the company's personnel

involved in all stages of the export process across the supply chain, from taking and recording an order to the finance department.

Moreover, an in-depth review of the company's electronic accounts is useful in identifying the number of shipments involved, the items shipped and the consignees of the goods. So-called structured data that needs to be reviewed resides in an electronic repository. For instance, this may originate in SAP systems tracking all orders and shipments a company handles in its day-to-day business operations. In order to understand and investigate such data files, it is important to obtain the database schema, which helps to determine the relationships between tables within the database. Accordingly, a thorough legal investigation goes hand-in-hand with the involvement of forensic experts experienced in the e-discovery of structured data.

This is also true for exports of technology items, or exports which take the form of technical assistance. In particular the use of cloud servers can easily expand the impact of export control and sanctions laws to business conduct even within the same group of companies. For instance, sending via email, traveling abroad with a business laptop containing or uploading to a cloud server technical drawings or CAD files of technology that may both be used for civil and military applications ("dual-use technology") can trigger export control questions and may require prior authorisation. This may be the case even where the technology never leaves the business, but physically or virtually crosses a border. For those investigating potential technology transfer infringements, compliance with export control provisions is likewise important, e.g. when sending emails with attachments from Europe to the U.S. in the course of an internal review.

The complexity of export control law and the difficulties in reviewing the vast amount of data is also a challenge for the authorities. Many national export control authorities or customs authorities therefore appreciate the cooperation of companies which investigate potential infringements internally and present the results of their review to officials. Depending on the concrete infringements, companies may qualify for a voluntary disclosure program that in some jurisdictions provides companies with full immunity from fines. But even if full immunity is not available, disclosing information voluntarily is often considered as a mitigating factor in determining a fine, and may even lead to a termination of administrative procedures without a conviction. In this process, it is crucial that national authorities see that the company concerned has taken measures to rectify the situation and correct the root cause of the problem. Steps such as conducting training of its personnel at all stages of the supply chain or introducing appropriate software tools, such as Enterprise Resource Planning (ERP) systems, to help track correctly exports are vital in actively showing that a company takes compliance seriously and invests resources in remediation.

Increased regulator attention in the area of trade compliance is necessarily leading to the maturing of internal compliance policies, often with guidance provided by different authorities on key aspects to consider. These policies should cover the full range of possible export control or sanctions issues, taking into account a company's individual risk profile in this area. For example, as well as covering supply chain issues, a trade compliance policy may also lay down rules on taking business laptops abroad where there is a risk of inadvertently exporting controlled technology stored on the computer. A robust internal compliance policy assists investigations in three main ways. First, such a policy should prevent or at least pick up possible infringements. Second, it provides a structure for investigation of any infringement that does occur: identifying gaps in hierarchy or supply chains which may be susceptible to such infringements, as well as helping to track information flow within a supply process. Finally, these two reasons also mean that such a policy provides reassurance to authorities that a company not only takes this subject seriously but has the means to implement any lessons learned in the case of a genuinely mistaken infringement. This may act as a mitigating factor in determining a fine.

Export control and sanctions problems generally gain high management attention. This is not only due to the risk of fines and reputational damage. Under certain legal systems in the EU, it is mandatory for companies exporting goods to have a board member take legal responsibility for export control compliance. Governmental procedures are often directed against this board member. Accordingly, investigations of export control infringements require professional handling

including experience both of substantive export control laws and of the procedural aspects of handling an investigation in order to fulfill management expectations.

The above considerations have been identified by the EU as being important for designing an effective Internal Compliance Programs ("**ICP**"). In August 2019, the European Commission published guidance on ICPs in the area of export controls, taking into account both international standards from other export control regimes, as well as best practices by national authorities. The guidance identifies seven core elements that an ICP should contain: (i) top-level management commitment to compliance; (ii) organizational structure, responsibilities and resources; (iii) training and awareness-raising; (iv) transaction screening processes; (v) performance reviews, audits, reporting and corrective actions; (vi) record keeping and documentation; and (vii) physical and information security. Although these elements are not an exhaustive list and ICPs should be tailored to the company concerned and its business activities, the guidance provides useful insight into the competent authorities' priorities when reviewing a specific transaction or investigating a company.

CONCLUSION

In times of dynamic international relations, export control and sanctions law gains importance as a political instrument. Infringements carry a high risk of fines, criminal prosecution and reputational damage for companies, members of their management, as well as their personnel. Internal investigations in this area require specialized expertise regarding the substantive legal assessment, the procedural management of the investigation, the forensic review of electronic data and the internal procedures followed at all stages of the supply chain until the export is completed.

AUTHORS

Dr. Falk Schöning
Partner
Hogan Lovells Brussels
T +32 2 505 0911
falk.schoening@hoganlovells.com

Falk Schöning can assist you regarding all questions and problems of EU and German antitrust law, foreign investment control law and export control law. He advises in particular on international cases which require coordination between different legal systems or representation vis-à-vis several regulators. Falk is frequently called on by companies which need advice on EU or German export control law, in particular regarding procedures with the German authorities. He knows the typical pitfalls of trade and sanctions cases and regularly cooperates with European and German regulators BAFA, Bundesbank, the Federal Ministry of Economics and the customs authorities. As part of Hogan Lovells' wider European trade compliance team Falk frequently structures compliance programs according to BAFA's guidance on Internal Compliance Programs.

Eleni Theodoropoulou
Associate
Hogan Lovells Brussels
T +32 2 505 0942
eleni.theodoropoulou@hoganlovells.com

Eleni focuses her practice on EU and international trade and investment law. She advises on EU sanctions and export controls, EU customs matters, as well as international trade and investment policy in the context of free trade agreements. She has also participated in export control investigations and internal audits.

Prior to joining Hogan Lovells, Eleni completed traineeships at the European Commission's Directorate-General for Trade, the International Center for Trade and Sustainable Development in Geneva, the Permanent Representation of Greece to the Council of Europe in Strasbourg and in private practice in Athens. Throughout her experience, she has worked on various issues of WTO law, international and EU investment law and policy, including in preparation for free trade agreement negotiations.

Overview

The following jurisdictions are covered in this guide:

Albania
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Liechtenstein
Lithuania
Luxembourg
Malta
The Netherlands
Norway
Poland
Portugal
Romania
Russia
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
Ukraine
United Kingdom

Albania

Kalo & Associates


Shirli Gorenca


Eni Kalo


Adi Brovina

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X		X
No				X	

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Whistleblowing in Albania is regulated by Law No. 60/2016 ("**Whistleblowing Law**"). The law establishes mechanisms for the protection of whistleblowers and obligations for public and private entities vis-à-vis whistleblowers.

Under the Whistleblowing Law, private companies and public authorities must establish an internal whistleblowing unit ("**WU**"), composed of one or more employees, which is responsible for reviewing whistleblower reports and for the protection of the whistleblowers. Although normally a whistleblower should provide their name and contact information in any report, the Whistleblowing Law permits anonymous reports, where the whistleblower can justify the need for anonymity and the report contains sufficient information to begin an investigation.

During the investigation, the whistleblower's identity may not be disclosed to third parties without their written consent. Information relating to the report is confidential and may not be shared with, or transmitted to, internal or external third parties without the written consent of the whistleblower, unless disclosure is required to fulfill a legal obligation.

Under the Whistleblowing Law, an investigation must be, barring special circumstances, concluded within 60 days of the commencement of the investigation. The whistleblower may request information about the progress and results of the investigation, which must be provided within 30 days of receipt of the written request. In any event, the WU must notify the whistleblower about the status and, if applicable, of the results of the investigation within 30 days from the moment the report was made.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) An employees' council is charged with representing the interests of employees and, to that end, is entitled to supervise the enforcement of laws, collective agreements, and a company's articles of association (Article 20 of Law No. 9901 of 14 April 2008). Councils have a statutory right to information and the right to make suggestions about the general policies at their companies.

However, the information rights of the employees' council likely do not apply to internal investigations. Nevertheless, an obligation to inform the employees' council may stem from an individual employment contract, a collective agreement or another agreement between the employer and the employees' council.

In practice, employees' councils are very rarely formed in Albania and, therefore, no unified practice exists in this area.

b) The Whistleblowing Law provides that personal data of individuals involved in investigations must be processed in compliance with the principles and procedures provided under local data privacy laws as well as the GDPR ("**Data Protection Laws**"). Under the Data Protection Laws, the data controller (i.e. typically the employer) has the general obligation to notify the Information and Data Protection Commissioner ("**DPA**"), an independent public authority, of any data processing activities prior to the commencement of such activities. The notification is made through the submission of an official notification form, in which the data controller must disclose, among other things, who will receive the personal data and whether the data will be transferred internationally. In principle, once the notification is filed, a controller may move forward with the processing (except when authorisation of the DPA is required, i.e. for processing sensitive data or for transfers of data to third countries).

Per the Whistleblowing Law, violations of the Data Protection Law are referred to the DPA.

c) There is no legal obligation to inform local authorities before beginning an internal investigation. However, the Whistleblowing Law provides reporting obligations, which require the internal WUs to file an annual written report with the High Inspectorate of the Declaration and Control of Resources and Conflicts of Interest ("**ILDKP**"), describing any investigations of whistleblower complaints in the preceding year.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Even though not expressly provided by applicable law, the duty to support an investigation is implied in the Whistleblowing Law, which grants the WU or the relevant state authority conducting the internal investigation (i.e. ILDKP) the right to collect statements and conduct interviews. The Whistleblowing Law also provides investigators the right to collect relevant documents from the whistleblower as well as from third parties, if it is deemed necessary by the head of the investigation.

The company may impose disciplinary measures on employees refusing to cooperate during the investigation, as it may be subject to administrative or criminal penalties for such behavior. However, there are no legal penalties for employees, who refuse to participate in the investigation.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

The duty to terminate an employee immediately or with notice is triggered when the person or body with the authority to terminate the employee becomes sufficiently aware of the conduct warranting termination. However, there is no deadline by which these sanctions must be imposed.

In practice, it is advisable to wait until the end of an investigation, or at least until a late stage, before initiating any termination procedure. In any case, under the Whistleblowing Law, an investigation must be, barring special circumstances, concluded within 60 days of commencement of the investigation.

---

5. Are there relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

In accordance with the Data Protection Law, an interviewee should be notified, ahead of the interview, if applicable, that their data is being processed. The interviewee should also be informed of the reason for the processing, who is processing the data (i.e. the data processor), and the means of processing, unless the interviewee (i.e. the data subject) is already aware of such information.

b) Reviewing emails?

The reviewing/monitoring of emails is not expressly regulated by the Labor Code. The employer is allowed to collect, during the employment relationship, any information about the employee that relates to their professional capabilities or to the applicability of the employment contract. Notwithstanding this, the employee as well as their personal items cannot be subject to control, unless this is required to protect the assets of the employer, other employees, or third parties from an illegal violation.

Employers should therefore have in place clear policies regarding the use of email, outlining under which circumstances employees may be monitored, and explaining how any information gathered through monitoring may be used. Also, for the monitoring process to be lawful, it is important that the employee is aware of such activity. It is strongly advised to obtain their consent in writing.

c) Collecting (electronic) documents and/or other information?

From a data privacy perspective, collecting electronic documents does not trigger any notification obligation, unless such documents contain data classified as personal. Personal data is any information relating to an identified or identifiable natural person. Under the Data Protection Law, data controllers have the obligation to: (1) inform the data subjects that personal data are going to be collected; and (2) notify the DPA before starting data processing activities through the submission of an official notification form. The form should contain: the name and address of the controller; the scope of the processing; the categories of data subjects and personal data; the receivers and/or categories of receivers of the personal data; whether the controller intends to transfer the personal data internationally; and a general description of the safety measures for the protection of personal data.

d) Analyzing accounting and/or other mere business databases?

To the extent the business databases do not contain personal data, they are not subject to the Data Protection Law.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no legal obligation to provide an employee written instructions before conducting an interview.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no legal obligation to inform an employee of his right to remain silent during an internal investigation. Such a requirement exists only in criminal investigations led by prosecutors.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no legal obligation to provide an employee with an Upjohn warning at the beginning of an interview.

d) Be informed that they have the right that their lawyer attends?

There is no legal obligation to inform an employee of his right to counsel during an internal investigation. Such a requirement exists only in criminal investigations led by prosecutors.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

As explained above, employees' councils are very rarely formed in Albania. Therefore, an employee does not generally have a right to have an employee representative attend their interview. Nevertheless, where there is such a council, the employee's contract should be consulted to confirm that no such right exists.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

As explained above, under the Data Protection Law, an interviewee should be notified, ahead of the interview, if applicable, that their data is being processed. The interviewee should also be informed of the reason for the processing, who is processing the data (i.e. the data processor), and the means of processing, unless the interviewee (i.e. the data subject) is already aware of such information. Any international transfer should be disclosed to the data subject as part of this notification.

g) Sign a data privacy waiver?

An individual cannot waive his rights under the Data Protection Law. However, the controller may obtain a written declaration from the data subject, in which the subject freely and knowingly consents to the collection and processing of their personal data. Consent of the data subject constitutes one of the grounds for lawful processing of personal data.

h) Be informed that the information gathered might be passed on to authorities?

Under the Data Protection Law, data subjects must be informed by the controller about the recipients of their personal data.

i) Be informed that written notes will be taken?

There is no legal obligation to inform an employee that written notes will be taken during their interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

The Whistleblowing Law provides that the WU must take all the necessary measures to protect evidence of wrongful conduct from disappearance or destruction. Companies that do not take such protective measures may be subject to administrative or criminal penalties.

Although the question of the admissibility of document hold notices has not been tested by court practice, in light of the obligations under the Whistleblowing Law, they may be admissible. The internal policies of the company should provide that the company may issue hold notices from time to time and that employees agree to abide by them, otherwise they may be subject to disciplinary measures imposed by the employer.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Under Law No. 9109 ("**Legal Profession Law**") the attorney-client privilege extends to any facts or information that an attorney has obtained in the course of representing their client. An "attorney" is defined as an individual who is professionally licensed and registered with the tax authorities as an attorney, and who practices law, whether as a solo practitioner or in cooperation with other attorneys (i.e. in a law firm). The privilege protection applies to written documents and oral communications. Unfortunately, there is little case law in Albania concerning the scope

and application of the attorney-client privilege and the Legal Profession Law itself provides limited guidance. However, the findings of an internal investigation would likely be protected.

9. Does attorney-client privilege also apply to in-house counsel in your country?

Attorney-client privilege does not apply to in-house counsel, as they are not registered as attorneys with the tax authorities and are not practicing law, as defined under the Legal Profession Law. In-house counsel that are employed as independent contractors, rather than company employees, may be covered by the privilege, but this rarely occurs in Albania.

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There is no statutory legal obligation to provide early notification to insurance companies. The relevant insurance contracts should, however, be checked.

b) To business partners (e.g. banks and creditors)?

There is no statutory legal obligation to provide early notification to business partners. The relevant contracts should, however, be checked for specific stipulations.

c) To shareholders?

There is no statutory legal obligation to provide early notification to shareholders.

d) To authorities?

There is no legal obligation to inform authorities before beginning an internal investigation.

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There are no immediate measures that have to be taken in Albania once an investigation is started. However, pursuant to the Albanian Criminal Procedure Code, any person, who has knowledge of or suspects the commission of a crime, must report the information to the relevant prosecutor office. In addition, the company must make sure that ongoing criminal behavior in the company is stopped.

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutors do not generally have any particular concerns about internal investigations or ask for specific steps to be observed. However, prosecutors may try to use the findings of an internal investigation as evidence during criminal proceedings.

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Pursuant to the Albanian Criminal Procedure Code, search warrants and dawn raids must be authorized by a court of competent authority. Information concerning, among other things, the nature of the search, the person(s) to be searched, and the authority conducting the search must be provided in the court order. Once a search is over, all involved parties should sign a record documenting the results of the search. In case a party refuses to sign the record, such refusal should be noted in the record. Where the procedural prerequisites are not fulfilled, there is a risk that the search will be declared invalid. Findings from an invalidated search may not be used in subsequent criminal proceedings.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Pursuant to the Albanian Criminal Procedure Code, before the initiation of court proceedings, and in the case of crimes subject to a maximum penalty of seven years' imprisonment or fines ranging from 500,000 to five million Albanian lek, the prosecutor and the defendant (including corporations) may enter into a deal. In practice, however, deals are not common in Albania.

Non-prosecution agreements and deferred prosecution agreements are not available to corporations. However, there are several mitigating factors, such as remedying the damages and eliminating the consequences, which may reduce the penalty on a corporation.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

A legal person (i.e. corporation) is liable under Albanian law for crimes committed, through action or omission, in its name, or for its benefit, by its representatives, leaders, and managers (Law No. 9754 of 14 June 2007). A legal person is not liable for crimes committed by any employee, only those who are under the authority of the person, who represents, leads, and manages the entity. In practice, this includes managers of departments, who are directly under the authority of the administrator of the company. In addition, a legal person may be liable only for the omissions of the person, who leads, represents, and manages the entity (i.e. its administrator), where this results in an absence of control and supervision.

A legal person is subject to so-called "principal" and "complementary" penalties. Principal penalties include fines and liquidation of the entity. Complementary penalties include, *inter alia*, the placement of the legal person under supervised administration, a ban from public procurement procedures and from obtaining or using of licenses, and the revocation of the right to perform one or more activities or operations.

Pursuant to the Criminal Code, the liability of the company does not discharge the individual, who has committed the offense/crime. Individuals who have committed a criminal offense may be personally subject to principal penalties (mainly imprisonment and fines) and other complementary penalties in accordance with the Albanian Criminal Code. However, directors, administrators, and/or officers are not personally liable for crimes committed by other employees of the company.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Penalties for legal entities (i.e. companies) may be reduced if the legal entity has corrected the organizational deficiencies which have resulted in the criminal offense by implementing an efficient compliance system. The law seems to refer only to the case when the misconduct has already occurred, but in our opinion the mitigating factor

could *a fortiori* apply if the efficient compliance system has already been implemented prior to the alleged misconduct.

Regarding the criminal liability of directors, officers, or employees such persons are liable only personally and not for offenses committed by other employees of the company. The implementation of an efficient compliance system prior to the alleged misconduct does not seem in itself as a factor which may reduce their penalties. However it may have a certain role in establishing or excluding their criminal liability.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

As the Whistleblowing Law is relatively new, no notable case law has yet developed concerning its interpretation and application. Companies operating in Albania are becoming increasingly aware of the law and taking steps to comply, for example, by establishing internal WUs.

CONTACTS

Kavaja Avenue, Building 27, 5th floor
Administrative Unit 10
1001 Tirana
Albania

Tel.: +355 4 2233 532
+355 4 2224 727
www.kalo-attorneys.com

Founded in 1994, KALO & ASSOCIATES has been in the forefront of legal services in Albania and Kosovo in representing prominent business organizations and IFIs, including many Fortune 500. The Firm enjoys international reputation and is "best friend" to many international law firms and IFI-s, development agencies and embassies. The firm has significant contribution in drafting modern commercial legislation such as banking, commercial arbitration, concessions, renewable energy, gambling, insolvency, secured transactions, financial leasing, insurance, corporate and municipal bonds, pension funds and the collective investment funds law. It is a founding member of the South East Legal Group, the largest legal services provider in the Balkans, established in 2003 (www.seelegal.org). The firm has contributed in modernizing the practice in Albania, by adopting the structured practice areas, professional liability insurance, Corporate Social Responsibility, Pro Bono services, anti-corrupt' practices, art support, etc. which together give a law firm an undisputed reputation. The firm earned reputation is related with the reputation of its founder, Perparim Kalo, who was representative of IBA for Albania since 1992 and invited as speaker to many international business and legal forums in four continents.

Shirli Gorenca
Partner
KALO & ASSOCIATES Tirana
T +355 4 2233 532
sh.gorenca@kalo-attorneys.com

Shirli leads K&A employment, labor, and immigration team in the Tirana Office. She has joined the firm in 2007 and has been working on different departments and dealing with Employment, Tax, Real-Estate, Banking & Finance issues that enhanced her professional growth in offering services to several international clients and fortune 500 companies.

Shirli is an active Member of the National Reconciliation Office of Tirana, representing some prominent employers' organizations on collective labor disputes matters and has been admitted to Tirana Bar Association in 2012.

She has contributed with articles in various publications of our firm and has attended several conferences and training on the employment and labor matters.

Eni Kalo
Partner
KALO & ASSOCIATES Tirana
T +355 4 2233 532
e.kalo@kalo-attorneys.com

Eni is a Partner of the firm, head of the IP Department, and provides a strong knowledge of both IP practice and legal procedures that is of invaluable benefit both to the firm and clients. Her main focus is towards IP, commercial contracts, telecoms, advertising, consumer protection, pharmaceuticals, anti-corruption, data protection and whistleblowing. She is active in registration of patents, trademarks and domains and has forged good links with both the General Directorate of Patents and Trademarks, and the Commissioner of Information and Protection of Personal Data, through her long experience in this area, being the key contact for various clients.

Adi Brovina
Senior Associate
KALO & ASSOCIATES Tirana
T +355 4 2233 532
a.brovina@kalo-attorneys.com

Adi is a Senior Associate in the Corporate and M&A Department, consolidating his expertise in the field of all aspects of corporate issues, including but not limited to company establishment, business restructuring, M&A, competition, concessions/PPP etc. As part of the corporate department, Adi provides legal advice to companies across all sectors on M&As and restructuring of companies, legal due diligence and drafting of relevant legal reports, drafting of letters of intent, share purchase agreements, shareholder agreements and advises clients on various corporate issues through the corporate life cycle. His focus area also extends to competition and concessions/PPP procedures.

Austria

KNOETZL HAUGENEDER NETAL Rechtsanwälte GmbH

Bettina Knoetzl

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	
No					X The lack of "adequate procedures" has to be shown by the prosecution authority (see more details question 15) and may - if additional requirements are fulfilled - lead to the company's criminal liability.

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Whistleblower protection has become increasingly important in Austria. A recently introduced law imposes on companies listed on the stock exchange and certain financial institutions a duty to set up an internal, anonymous whistleblowing mechanism to flag violations. The law further grants whistleblowers criminal immunity with regard to the report and prohibits employers from discriminating against employees who notify the authorities of violations.

Companies which set up an internal whistleblowing protection mechanism need to report this measure to the data protection authority and comply with the following general principles: (i) complete separation of the whistleblowing department from all other departments; (ii) safeguards guaranteeing full protection of the identity of the whistleblower; (iii) access by the accused to the incriminating allegations, unless the investigation is jeopardized by such disclosure; (iv) deletion of all collected data within two months of the closure of the internal investigation; and (v) only data of executive employees may be passed on to the parent company.

The law does not stipulate explicit requirements of how to react to a whistleblower's report. Best practices suggest immediate action. Depending on the content of the report, appropriate steps have to be taken, including - for example - the initiation of an internal investigation and perhaps even the filing of a report to the criminal authorities.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) There is no provision under the Austrian Constitutional Labor Law which specifically concerns internal investigations. Moreover, there is no obligation to inform the works council about suspected cases or internal investigations already started, or to allow a works council representative to participate. However, if a company decides to set up a whistleblowing system, the works council has to be involved in the setup of the same and needs to provide its consent to the planned changes.

b) If data in an internal investigation will be processed or transmitted, the provisions of the General Data Protection Regulation ("**GDPR**") have to be applied. However, there are no provisions in the GDPR that impose an obligation to inform the data authority. It may nevertheless be advisable to inform the appointed data protection officer in order to ensure that the rights of data subjects under the GDPR are respected.

c) There are no other local authorities, which have a right to be informed about the investigation or to participate in it. However, if a company wishes to take advantage of the "Crown Witness" regulation or a leniency program, assuming all preconditions are met, it is advisable to involve the relevant authorities. The so-called "Crown Witness" regulation allows prosecutors to drop an investigation against a cooperating witness, who freely confesses his involvement in a serious offense and provides new information that contributes substantially to the investigation. Failure to involve the relevant authorities may preclude the company from obtaining the benefit.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees are under a duty of loyalty and information vis-à-vis their employer. Pursuant to these duties, employees are obliged to participate in investigation interviews. At the same time, the interviews have to be conducted within the confines set by law, notably the employer's duty of care vis-à-vis their employees. Pursuant to this duty, which extends also to executives and managers, the employer is, *inter alia*, required to respect the private life of employees, protect their honor, and treat them equally.

Although employees must participate in interviews, Austrian legal scholars are engaged in a contentious debate over whether employees are also obliged to answer the questions of private investigators, which may reveal personal misconduct.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Under Austrian law, an employer may only dismiss an employee with immediate effect if the employer exercises this right immediately after becoming aware of the justification for the dismissal. The employer forfeits this right, if they fail to immediately (i.e. "without delay") exercise it. In cases of doubt, the employer can suspend the employee until the investigation yields more evidence or terminate the employee in a consensual manner (with the option for re-employment in case the employee is exonerated).

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

On 25 May 2018, the GDPR came into effect. In Austria, the local, renewed, Law on Data Protection ("DSG") also came into effect.

The GDPR provides for, *inter alia*, the right to be informed about the processing of personal data. Moreover, companies with more than 250 employees or which process sensitive data are required to maintain a record of processing activities. Pursuant to the DSG, data may only be used in accordance with the law and in good faith, and only collected for specific legitimate purposes. The principle of proportionality also has to be respected.

b) Reviewing emails?

A search with the express consent of the user is generally permitted. Without the consent of the user, it is important that the email account belongs to the company and is deemed to be for professional use. The interests of the parties and proportionality need to be considered.

Emails with private content may not be searched. If private emails are identified (e.g. by the subject line), only spot checks are allowed to clarify that the email is indeed private. As soon as an email is identified as private, it must be excluded from the search. If it has been opened by coincidence or as part of the spot check, it needs to be closed immediately after identification or confirmation that it is private.

c) Collecting (electronic) documents and/or other information?

According to Article 5 of the GDPR, personal data may be collected only for specific, explicit, and legitimate purposes and, *inter alia,* be processed lawfully, fairly and transparently. In this regard, the processing of personal data is lawful only if, among other requirements, (i) the data subject has given consent, (ii) it is necessary for compliance with a legal obligation to which the data's controller is subject, or (iii) it is necessary for the purpose of the legitimate interests of the data's controller (see Article 6, GDPR).

The GDPR also provides for a catalog of rights applicable to data subjects, including the right to be informed about the processing and storage of personal data, the purpose of data processing, and the duration of storage. GDPR provisions must be closely followed when it comes to processing data. For this purpose, the term 'processing' is defined as any operation or set of operations performed on personal data or on sets of personal data, whether by automated means, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting upon, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying (see Article 4, GDPR). During an internal investigation, a considerable amount of evidence, including personal data, will be processed by collecting, storing, using, disclosing, etc. To comply with GDPR provisions, the identification of which data is classified as personal and which as non-personal should be well documented. Furthermore, investigating companies should document, in detail, the purpose of processing personal data and should comply with GDPR provisions regarding storage limitations, integrity and confidentiality. Besides that, companies should be especially careful when it comes to transnational data transfers, especially from or to non-EU Member States.

d) Analyzing accounting and/or other mere business databases?

If accounting/business data contains no personal data, the data privacy rules do not apply.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no legal obligation to provide the employee with written instructions prior to the interview.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

The applicability of the right against self-incrimination in internal investigations is unsettled. As long as legal uncertainty persists, it is advisable to inform interviewees of their potential right against self-

incrimination. There is, however, no duty of care between a company and third parties, who are not employees.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

If an interview is conducted by outside counsel, they will have to comply with the attorneys' Code of Conduct. This Code requires the avoidance of conflicts of interests. Therefore, the interviewee has to be informed that the outside counsel is only acting on behalf, and for the benefit of, the company.

d) Be informed that they have the right that their lawyer attends?

Prior to the interview, the employer (or third party acting for the employer) should inform the employee that they have a right to be accompanied by their own legal representative.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Employees have no specific right to have a works council representative attend their interviews or otherwise participate in the investigation. They, therefore, also do not have to be informed in that regard.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The GDPR and the Austrian DSG protect against the transmission of personal data abroad. Uncontrolled data transfer to the United States is, therefore, problematic. Mere notice to the affected person will not suffice. The employee will have to provide their informed consent prior to the transfer, which can be revoked at any time.

g) Sign a data privacy waiver?

Employees are under a duty to share any information, which they obtain in their capacity as employees, with their employer. Such data is not considered to be "private" and no waiver is required. The situation is different for data which qualifies as private. The employer must respect the employee's private sphere. A waiver to collect and use private data is required and may be legitimately withheld by the employee.

h) Be informed that the information gathered might be passed on to authorities?

The employer has a duty to inform the employee of the exact use of the information gathered in an internal investigation, including the persons outside the company with whom the information might be shared. It is of particular importance if information might be passed onto prosecution authorities.

i) Be informed that written notes will be taken?

It is common that written minutes are made of an interview and the interviewee should be informed of this. Data protection law requires, moreover, the respect of the principle of proportionality in using data gained from the interview. Therefore, the company should not collect more personal data than the minimal amount required to conduct the investigation properly.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

All persons are under a legal duty to refrain from destroying evidence, including material that may become relevant in a legal dispute. Under Austrian law, suppression of evidence is a criminal offense. In order to protect employees from violating the law, it is advisable to remind them of this duty. Such warnings contain clear instructions to refrain from deleting emails or documents from the system.

Best practices in Austria require the preservation of relevant data immediately (by, for example, "imaging" an employee's computer) if allegations of illicit behavior arise.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege only extends to attorney work product created for the purpose of defending the client and not to previously existing evidence. Hence, investigation reports are protected by the privilege.

To ensure privilege protection, it is advisable to store attorney work product in a way that the data remains in the custody of the attorney (e.g. sharing work product over a secure server provided by the attorney).

Attorney work product and correspondence of a client with his attorney or similar documents, which have been created in the context and/or for the purpose of the legal defense of this client, may neither be seized at the law firm nor at the client's site. Regarding data that is within the attorney's custody, more extensive legal remedies are available, such as the sealing and judicial review of the data upon objection by the attorney.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

In Austria, the attorney-client privilege applies only to outside counsel.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Austrian law does not require companies to issue notifications when starting investigations. Usually, insurance policies encourage policyholders to inform the insurer of internal investigations. If there is a concrete risk that the insurer will be asked to cover the event, if a claim arises, then the insurance company must be informed.

b) To business partners (e.g. banks and creditors)?

In general, there is no duty to inform business partners of the start of an investigation. For stock exchange listed companies, *ad hoc* or regular notification duties might apply. Banks tend to include provisions in their contracts, which require notification of events, which affect a partner company's creditworthiness.

c) To shareholders?

Companies publicly listed on the Vienna Stock Exchange are under a legal obligation to issue *ad hoc* notifications regarding inside information, i.e. information that has not been made public and which, if it were made public, would be likely to have a significant impact on the price of the company's shares or other related financial instruments.

d) To authorities?

There is no legal duty for private companies to report misconduct to law enforcement authorities. There may be such a duty for state companies exercising sovereign power.

Self-reporting may be advisable in circumstances in which the company can take advantage of a leniency program, such as the "Crown Witness" regulation or the so-called "diversion" or to gain the "victim status" in proceedings (as injured party).

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Authorities would expect among other measures: sanctions to be imposed, including the immediate termination of employment contracts or – if the situation needs to be clarified – at least a suspension; a revision of existing policies; a repetition or improvement of training programs; and the compensation of damages suffered by victims of the criminal conduct.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Internal investigations, which are conducted according to best practices, may be regarded as helpful if the results are openly shared with the prosecutor's office. The sharing of the results of an internal investigation may be taken into account and can be an important factor in leading the prosecutor to refrain from prosecution. It may happen that the prosecutor expressly asks for certain questions to be asked or certain investigative measures to be taken. Companies tend to comply with such requests.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

With the approval of the court, the public prosecutor may order the search of a specific location – for instance, an office building – to collect, temporarily secure, or seize evidence to be used in criminal and civil proceedings. In highly urgent matters, the public prosecutor may order the search warrant and subsequently seek court approval.

House searches shall only be ordered if there is a "founded suspicion" (this threshold is higher than the "initial suspicion" required to open investigations) and the coercive measure complies with the principle of proportionality, meaning that there are no less intrusive means available. If, for example, the information could be obtained through obtaining the cooperation of the defendant, the application of coercive means, such as house searches or dawn raids, could be deemed to lack the requisite proportionality.

Persons against whom a search warrant was issued or whose premises were subject to a house search can file an objection with the competent office of the public prosecutor within six weeks from the measure. The public prosecutor can either comply or, within four weeks, pass the objection on to the competent criminal court.

Improperly obtained evidence can be used against the company. Some exceptions apply, for example in cases of attorney-client privilege.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Non-prosecution agreements do not exist in Austria. There are, however, two related concepts: the so-called "diversion" and termination of proceedings. Owing, in part, to cultural opposition to "agreements" offered by the prosecution authorities, neither option is used frequently.

"Diversion" allows the prosecutor to end the criminal prosecution of a corporation, if punishment of the corporation does not seem to be necessary. A number of factors are considered, including the conduct of the corporation after the alleged offense (here, self-reporting is of particular importance), the weight of the alleged offense, the amount of the fine to be imposed, and the detriment suffered by the corporation due to the misconduct. In some instances, the prosecutor must pursue diversion if certain requirements are met.

While a termination of proceedings leads to a full acquittal, "diversion" is positioned in between a conviction and an acquittal. In contrast to a conviction, a "diversion" is not entered in the criminal register for corporations and the related fines are lower.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Corporations are liable for the unlawful and culpable actions of their "decision-makers" (i.e. higher-ranked individuals with authority to represent the company) and, under more restrictive conditions, also for the actions of their "normal" employees, provided that the offense was either committed for the benefit of the corporation or the offense violated duties incumbent upon the corporation itself.

If the offense was committed by a "normal" employee, it must have been either rendered possible or facilitated by the decision-makers' failure to take essential precautionary measures (e.g. implement a proper compliance system).

The prosecution bears the burden of establishing the lack of adequate procedures. In practice, the corporation will usually try to show the proper implementation of adequate procedures.

Corporations are subject to fines, which are measured in per diem units, as well as to court directives (e.g. to compensate harm done, to implement a proper compliance system, or to make charitable donations). The current maximal fine for offenses, such as severe fraud, embezzlement, or corruption is €1.3 million (the fine depends on the corporation's earnings).

Natural persons are subject to the whole set of penalties and other sanctions if they are found personally guilty of an offense.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Fines imposed upon corporations are determined according to aggravating and mitigating factors. As grounds for reduction of fines, the law explicitly and equally mentions both precautionary measures taken by the company to prevent crimes prior to the alleged misconduct and precautionary measures taken to prevent further misconduct installed after an offense was committed. Other mitigating factors for fines against corporations are e.g. significant assistance as the company may provide in clarifying the facts of the case, compensation for the consequences of the misconduct, and significant legal disadvantages that the company has already suffered as a result of the misconduct. Apart from a reduction, fines may be partially or fully suspended under certain preconditions.

Penalties imposed on natural persons are calculated according to aggravating and mitigating factors, which are based on the individual's personal culpability.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

In recent years there has been increasing public resentment about the often very long duration of proceedings in white collar crime cases. A great number of investigations in large, complex cases, often lasted 10 years or longer. Some of these proceedings have still not been concluded in a final court decision. In some cases, that have been pending for more than 10 years, there has not even been a decision yet as to whether charges will be brought at all. In other such cases, closure is not even in sight.

Prominent examples of these "monster proceedings" are numerous criminal proceedings relating to the insolvency of Hypo Alpe Adria Bank, the criminal proceedings relating to allegations in connection with the MEL equities, criminal proceedings in connection with the BUWOG case prosecuted against, among others the former Austrian Minister of Finance, and the criminal proceedings relating to alleged bribery payments in connection with the purchase of Eurofighter jets. These are only a few examples of a much longer list of less prominent, but similarly long, white collar crime cases.

To promote a possible acceleration of these proceedings, the provision for "Verification of the maximum duration of the investigation procedure" (Section 108a StPO) has been introduced. The provision stipulates that the duration of the investigation procedure may not exceed three years. After such time, either the indictment should be filed or, if sufficient evidence is still wanting, the criminal proceeding should be terminated.

However, in certain cases and at the request of the public prosecutor's office, the court may extend the duration of the investigation proceedings for an additional two years, and this extension process may be repeated indefinitely. In addition, various phases of the proceedings, including pending appeals, are not included in the maximum duration.

Since this new regulation only applies to proceedings initiated as of 1 January 2015, it will now gradually become clear whether this provision will actually result in speedier proceedings.

From a defendants' point of view, the acceleration of criminal proceedings is urgently necessary. The defendant's reputational financial and personal burden of pending criminal proceedings, demand a swift clarification of any suspicion.

CONTACT

KNOETZL

Herrengasse 1
1010 Vienna
Austria

Tel.: +43 1 3434 000
Fax: +43 1 3434 000 999
www.knoetzl.com

Bettina Knoetzl
Partner
KNOETZL HAUGENEDER NETAL
Rechtsanwälte GmbH
T +43 1 3434 000 200
bettina.knoetzl@knoetzl.com

Bettina Knoetzl is one of the founding partners at KNOETZL HAUGENEDER NETAL Rechtsanwälte GmbH, a leading Austrian based, international law firm in Dispute Resolution, Business Crime, Compliance and Corporate Crisis Management.

Bettina is a trial lawyer with 25 years' experience in international and Austrian matters of high profile, scoring notable successes in criminal defense work in insider trading, price fixing, fraud and corruption cases. For more than a decade Bettina has been assigned the highest tier rankings by international directories, such as Chambers, in both civil litigation and white collar crime. In 2017 she has been awarded worldwide recognition as "Lawyer of the Year" in Asset Recovery by Who's Who Legal, London Business Research Society. She is a designated thought leader in the legal community and is known for her vast, practical and creative, experience in structuring settlements in complex disputes. In addition to her civil litigation work, she handles business crime cases, internal investigations, including FCPA and "Me too" matters, in the banking, insurance, pharma and automotive industry, with a significant focus of her practice on investors' protection and asset recovery. Bettina advises clients in mission-critical and notorious disputes, including class actions, and has a demonstrable track record of winning judgments and strong, favorable, settlements for both companies, government instrumentalities and private clients.

Bettina is the President of Transparency International (Austrian Chapter), the exclusive Austrian representative of the ICC-FraudNet and lectures in the Austrian Lawyers' Academy (AWAK) in dispute resolution. She is heavily engaged in the International Bar Association where she co-chaired the global Litigation Committee throughout 2016/2017.

Belgium

Hogan Lovells


Fabien Roy


Raphaël Fleischer


Ivan Pico


Hélène Boland


Alexander Wenzel

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	
No					X No formal "Adequate Procedures Defense", but such procedures are recommended to show lack of intent/negligence.

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

There is no comprehensive statutory approach under Belgian law to whistleblowers and internal investigations. Such investigations must comply with general provisions of labor law or data privacy law.

Specific legislations in the private and public sector address the issue of whistleblower protection.

- The Law of 2 August 2002 on the Supervision of the Financial Sector and the Financial Services includes protection for whistleblowers. According to Article 69bis of the Law of 2 August 2002, the Financial Services and Markets Authority ("**FMSA**") must put in place effective mechanisms to enable potential or actual breaches of financial legislation to be reported to the FMSA. In addition, the whistleblower must be protected against retaliation and their identity is kept confidential.
- In the context of investigations related to bullying, violence or sexual harassment in the workplace, specific statutory provisions apply. The Law of 4 August 1996 regarding the welfare of workers in the performance of their work provides that a worker who believes that they are a victim of violence or moral or sexual harassment may file a complaint with the official in charge of surveillance (Article 32*nonies*). The worker may not be subjected to a prejudicial measure for having filed a complaint (Article 32*tredecies*). With regard to the public sector, specific legislations regulate the protection of whistleblowers.
- At the federal level, Law of 15 September 2013 on the reporting of a suspected integrity violation within an authority by a member of its staff includes provisions for the protection for whistleblowers. In the Flemish Community and Region, the protection of whistleblowers is governed by Article 17bis of Decree of 7 July 1998 establishing the Flemish Ombudsman.

– There is some Belgian case-law on the dismissal of employees that became whistleblowers, in addition to the case law of the European Court of Human Rights ("**ECtHR**") on this issue. In *Heinisch v Germany*, the ECtHR developed criteria that need to be considered when assessing the dismissal of whistleblowers in light of their freedom of expression.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) According to the Collective Bargaining Agreement ("**CBA**") No 81 or other applicable CBAs, employee representative bodies must be involved where specific tools such as monitoring of online communications are used. Failure to comply with these CBAs may result in criminal sanctions. In addition, companies may have included specific provisions in their internal labor regulations which obligate them to inform employees' representatives when an internal investigation is launched.

b) Internal investigations extensively involve the processing of personal data and the investigations should thus comply with the EU General Data Protection Regulation ("**GDPR**") and the Law of 30 July 2018 implementing the GDPR. In light of Article 38 of the GDPR, internal investigations will in principle involve the Data Protection Officer, provided the company has one. Infringement of the GDPR and the Law of 30 July 2018 may lead to administrative fines.

c) Some laws require the authorities to be informed when specific criminal offenses may have been committed. For instance, the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash provides that where covered entities are aware or suspect that a transaction is connected specifically with money laundering or terrorist financing, they must inform the Finance Intelligence Unit ("**CFI-CTIF**") (Article 33). Some laws impose reporting obligations to the Federal Agency for the Safety of the Food Chain ("**AFSCA/FAVV**") or the Federal Agency for Medicines and Health Products ("**AFMPS/FAGG**"). Such a report may trigger an investigation by one of these agencies. They will not participate in the internal investigation of companies. Failure to comply with an obligation to report is subject to criminal sanctions.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees must comply with the instructions of their employer within the context of their employment contract. This includes requests to take part in interviews in the course of an internal investigation. However, the employer may not use coercion, for instance, to prevent employees from leaving the interview room. Employers may impose disciplinary measures for failure to comply with its legitimate instructions.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

To immediately dismiss an employee (e.g. for serious misconduct), the employer must respect a strict deadline that lapses after three days. The deadline starts to run as soon as the employer obtained certainty about the facts.

An internal investigation may reveal important information. However, where the company already has knowledge of the relevant acts or omissions of the employee, the internal investigation does not suspend the strict deadline.

Even if some internal company regulations provide that an employee must be heard before being dismissed, companies that wish to dismiss an employee immediately must ensure that they do so in a timely manner.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

The GDPR governs the processing of personal data. When conducting an interview in the context of an internal investigation, the investigator will process personal data as soon as any personal information is written down or otherwise stored. The processing of any personal data collected during or after the interviews must comply with the requirements of the GDPR.

b) Reviewing emails?

The employer reviewing employees' emails must respect the general data protection principles and the requirements imposed by the GDPR. The Belgian Collective Work Agreement No 81 provides for rules concerning employers' monitoring of employees' emails. Further, Articles 124 and 125 of the Electronic Communications Act and Article 314bis of the Belgian Criminal Code ("**BCC**") prohibit the processing of some communications of employees including emails without the consent of all parties involved. In this context, we would suggest that employers draft a policy or Standard Operating Procedure ("**SOP**") that sets out how professional email addresses are to be used and how the employer may supervise or monitor the use of those email addresses.

c) Collecting (electronic) documents and/or other information?

Collecting electronic documents and/or other information also needs to comply with the general provisions of privacy law outlined under section 5a. In order to set clear standards and in order to ensure that employees have realistic privacy expectations, companies should put in place a clear corporate policy on the use of electronic devices provided by the employer or personal devices used for professional purposes. The GDPR will be applicable to the collection of any written or stored information that includes personal data. We would suggest to employers to draft relevant policies and SOPs.

d) Analyzing accounting and/or other mere business databases?

If the databases include personal data, such an analysis is likely to amount to data processing and the company must comply with the requirements of the GDPR. If these databases do not contain such personal data, their analysis is not subject to privacy legislation.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

Belgian law does not provide any specific rules concerning employee interviews during an internal investigation. However, it may be helpful to provide the employee with a document that contains the rights of the employee during the interview and to request the employee to sign that document.

The purpose of the signature is to prove that the employee had an opportunity to acknowledge the content of the document.

The purpose of the document is to diminish the risk that Belgian judges find the statements to be inadmissible as evidence. In some cases, Belgian judges have ruled that the employer or prosecutor may not rely on statements that were not made voluntarily as evidence. Judges may consider all the circumstances surrounding the interview during which the statements were made to determine whether the statements were made voluntarily. For example, judges may consider the use of misleading promises, physical violence or psychological violence by the interviewer as coercion to make the employee provide these statements.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

No. However, Belgian judges have ruled that there may not be any indication that the employee was coerced to make the statements or that the statement was made in conditions that raise questions concerning the voluntary nature of the statements. If the employee makes a self-incriminating statement, it may be scrutinized strictly as to its voluntary nature by a judge if the statement is used in court proceedings.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

Although so-called "Upjohn warning" is not a requirement, we would, however, suggest informing the interviewee that the lawyer attending the interview does not represent the employee. If the interviewer does not inform the employee about the identity and the capacity of all persons present, the employee may be able to claim that the employer gathered the statement through trickery, which deprives the statement of its credibility.

In light of the above, we would suggest informing the interviewee that the lawyer represents the company and not the employee. Should other persons attend the interview, it is advisable to introduce them to the interviewee as well.

Further, all Belgian lawyers are bound by a Professional Code of Conduct. The Code of Conduct provides that Belgian lawyers should be clear about who they do or do not represent during an interview. If the lawyer gives the employee the impression that they are representing the employee or both the company and the employee, that lawyer may be in violation of the Code of Conduct.

d) Be informed that they have the right that their lawyer attends?

No. However, it may be helpful for the company to decide that the employee may be assisted by a lawyer and inform them thereof. This may be helpful to make it credible in court that the employee has provided the statements voluntarily.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Belgian law does not impose the requirement on employers to inform the employee that they have a right to have a representative of the union or work council to be present at the interview.

It may, however, be helpful to inform the employee of their right to have a representative attend the interview. The presence of an employee representative may make the voluntary nature of the statements more credible in potential court proceedings.

Some employers include the possibility for employees to be assisted by a union representative during interviews in the employer's labor regulations.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Any transfers of personal data outside the European Union must be subject to an adequacy decision or appropriate or suitable safeguards in accordance with the GDPR. Whether the transfer may take place would need to be assessed on a case by case basis.

g) Sign a data privacy waiver?

No, the Belgian Data Protection Authority has taken the position that, in general, employees cannot give their consent freely to an employer. However, in accordance with Article 13 of the GDPR, the employer must provide the employee with a privacy notice which will include the intended purpose of the processing and the legal basis for the processing, if any records of the interview are made that include personal data. It may be helpful to request the employee to sign the document containing this information to be able to prove that the employer provided this information to the employee.

h) Be informed that the information gathered might be passed on to authorities?

If the employer may share personal data with the competent authorities, the employer shall inform the employee thereof as set out in section 6g of this question list. Further, documenting that the employee has been informed increases the credibility of the voluntary nature of the statements, if challenged during court proceedings.

i) Be informed that written notes will be taken?

No. However, if written notes are taken that include personal data; the GDPR will be applicable to the processing of the personal data. The employer will have to comply with the general principles of the GDPR and will then have to inform the employee of the personal data processing with a privacy notice in accordance with Article 13 GDPR.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Yes. If the documents contain personal data the GDPR will be applicable to their processing or storage. Personal data may not be kept longer than required for the purpose for which the data has been collected. The hold notice would be an exception to the employer's data retention policy. Any document hold notice should include the scope and purpose of the retention and be sent to the employee in a timely manner.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege, or legal professional privilege ("**LPP**"), may be claimed over findings of the internal investigation. In Belgium, LPP applies to lawyers (Avocat/Advocaat) who are members of the French and German Bar ("**OBFG**") or the Flemish Bar ("**OVB**"), as well as in-house counsel registered with the Belgian Institute for In-house counsel (Institut des Juristes d'Entreprise/Instituut voor Bedrijfsjuristen).

LPP protects any information received by an attorney (acting in his or her capacity as an attorney) or obtained in the context of the provision of legal advice, legal proceedings, or any dispute in general, or in matters determining the client's rights and obligations. This may include emails, correspondence, notes, advice, or preparatory documents.

In order to ensure the most stringent protection of LPP, it is essential for external counsel to conduct the internal investigation, in particular, if the investigation has cross-border elements (see response to question 9 below). In the context of seizure by the authorities of documents regarding the internal investigation drafted by a lawyer (e.g., an investigation or audit report), a specific procedure is in place for the assessment of the confidential character of documents, whereby the President of the Bar will prevent the authorities to take note of the content of those documents.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Under Article 5 of the Law of 1 March 2000 creating the Belgian Institute for In-house counsel, advice given by in-house counsel is confidential, provided that it is given for the benefit of the counsel's employer and in the framework of activity as legal counsel. The Brussels Court of Appeal confirmed this in a judgment of 5 March 2013 (18th Chamber, No 2011/MR/3). The Court of Appeal held that in accordance with Article 5 of the Law of 1 March 2000, read in conjunction with Article 8 of the ECHR (right to privacy), the Belgian Competition Authority could not seize documents containing legal advice provided by in-house counsel. The Brussels Court of Appeal held that LPP also covered internal requests for legal advice, correspondence relating to legal advice, draft opinions, and preparatory documents.

The judgment of the Brussels Court of Appeal stands in stark contrast with the Akzo judgment (C-550/07 P) handed down by the European Court of Justice ("**ECJ**") on 14 September 2010. In Akzo, the ECJ ruled that, under EU law, correspondence from or addressed to a attorney is not protected by LPP if the attorney is bound to his client by a relationship of employment. Thus, the ECJ excluded advice by in-house counsel from protection by LPP (as well as advice from non-EEA-qualified external counsel). However, the Brussels Court of Appeal considered that there was no inconsistency between its ruling and the Akzo judgment, since the European Commission's investigatory powers are different from those of national competition authorities. This difference can justify a distinction of the rules on LPP at EU level and at national level.

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Under Belgian law, a notification requirement to insurance companies does not exist. However, companies should assure themselves that their insurance agreements do not contain relevant provisions in this respect, which will often be the case. Indeed, insurance policy agreements will often contain clauses obliging the policyholder to notify the insurance company in case of potential claims within a specific period of time.

b) To business partners (e.g. banks and creditors)?

There is no general obligation to inform business partners of the conducting of internal investigations. Nevertheless, depending on the circumstances, it may be recommended to inform business partners, especially if those would be harmed by the outcome of an internal investigation. Such an act could in any event be considered as demonstrating good faith on account of a company performing an internal investigation. Regardless of the above, a decision to inform business partners of internal investigations must be subject to careful considerations of both the interests of the company and third party business partners.

c) To shareholders?

It should be borne in mind that performing an internal investigation amounts to sensitive information. Therefore, any disclosure of such internal investigation to shareholders (as with other disclosures) should be considered on a case-by-case basis and also in the context of applicable contractual/corporate obligations. Due to recent amendments made to the Company Code (see Articles 96 and 119 "**CC**"), certain companies may now be required to disclose internal investigations in their annual report, unless they invoke "the comply or explain" clause of Article 96 CC, and thus justify reasonably why they may deviate from this obligation. Simultaneously, companies must consider other applicable legislation as well (e.g. on insider trading statutes). For certain companies the obligation to inform the public of sensitive internal information that directly concerns the company is provided for by law (e.g. Article 17 Market Abuse Regulation which provides for such obligation for certain public market participants).

d) To authorities?

See section 2c.

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Once the company is aware of damages, it should take all reasonable measures to limit the aggravation of those damages. The company must, therefore, cease any ongoing criminal behavior. In addition, it will be in the interest of the company to distance itself from the wrongful behavior of its employee(s) and to undertake disciplinary actions against them to avoid suspicions of bad faith and complicity on the part of the entity.

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

It should firstly be reminded that Belgian prosecutors are under no legal obligation to take internal investigations into account. Indeed, internal and external investigations are independent from each other. Nevertheless, the company can decide to share the results of its internal investigation with the prosecutor's office, e.g. when the company files a criminal complaint against an employee. As a matter of fact, voluntary disclosure of the results of an internal investigation may be taken into account as mitigation factors when penalties are imposed. In case an entity intends to submit a file to the prosecutor, it is recommended to ensure its credibility by documenting every investigative measure and by entrusting it to external counsel. In addition, it should also be kept in mind that under Belgian Law, as a general principle, evidence obtained in breach of legal provisions (e.g. on the protection of

employees, on the protection of data privacy) may not be admissible. As a result, any internal investigation must comply with all relevant legal provisions.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

In principle, search warrants in criminal proceedings have to be executed by the investigating judge (Article 87 of the Code of Criminal Procedure ("**CCP**")), but they can and often are delegated to judicial police officers. For this purpose, the investigating judge is required to sign a reasoned search warrant, which should include the name of the appointed judicial police officer(s), the offense(s) the entity is being accused of, and a clear description of the location of the place that has to be searched.

According to the case law of the CoC of 2003, which is now enshrined in Article 32 of the preliminary title of the CCP, evidence that has been obtained without fulfilling those requirements can be used unless the irregularity (i) affects the reliability of the evidence, (ii) violates the right to a fair trial, or (iii) does not comply with formal requirements that are sanctioned by nullity. Whether these conditions have been met will be examined by the competent court on a case-by-case basis.

The situation is similar in relation to dawn raids for competition law purposes. These are also not lawful without a prior judicial warrant. The requirement of a prior judicial warrant has also been included in the Competition Act since 2013 (Book IV of the Economic Law Code).

On 26 April 2018, the CoC also confirmed that evidence seized during unlawful dawn raids or obtained pursuant to such unlawful raids should be excluded. The Belgian Competition Authority had argued that it could nevertheless use unlawfully obtained evidence on the basis of the so-called "Antigoon" case law. In criminal cases it is recognized that an error with regard to the gathering of evidence may only in certain circumstances lead to the exclusion of the evidence. However, the CoC that this case law is not applicable to competition cases. The judgment of 26 April 2018 states that an appropriate remedy for an unlawful dawn raid can only be provided by excluding all evidence obtained from and on the basis of the dawn raid.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Settlements (Article 216bis CCP) and guilty pleas (Article 216 CCP) are available for companies in Belgium. Guilty pleas have only been introduced in 2016 and are currently not common in Belgium. The Constitutional Court ruled in June 2016 that Article 216bis paragraph 2 CCP, is unconstitutional to the extent that the prosecutor can put an end to cases which are already being handled by a judge, without sufficient judicial control. The Law of 18 March 2018 has amended Article 216bis CCP in order to bring it in line with the Constitution and now foresees judicial scrutiny over the proportionality (thus not only the formal legality) of settlements. In addition, where a settlement concerns Tax or Social Security matters, the relevant public authorities are to be informed by the prosecutor that a settlement has been reached and those authorities must approve the settlement.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Companies can be held liable for the misconduct of individuals where the offenses have a sufficiently strong connection to the interests of the corporation. The BCC provides that the penalties for companies are fines, confiscation, dissolution, and prohibition to exercise an activity, the closure of one or more establishments, and the publication or dissemination of the decision. Further, the Act of 17 June 2016 concerning public procurements provides that persons may be excluded from participating in public tender procedures.

On specific conditions, directors, officers, and/or employees may be penalized for the misconduct of other individuals. The penalties that apply to individuals are fines, imprisonment, electronic surveillance, confiscation,

deprivation of civil or political rights, and autonomous probation sentences. Further, Royal Decree No. 22 of 24 October 1934 provides a legal basis for imposing a prohibition to pursue certain professional activities.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Belgian judges have a broad discretion to decide on and motivate any potential penalties. The judge may take all circumstances leading to the potential penalty into account. This includes the implementation of efficient compliance systems. Having efficient compliance systems in place prior to the ruling may be helpful to limit the penalties.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Recently the legislation on market abuse has been tightened in light of EU law. Whereas it used to be common practice to reach out to the police in case of alleged wrongdoing, recently internal investigations and internal audits have been increasingly used, as was demonstrated by a recent, heavily mediatized, case involving the Brussels social welfare provider Samusocial. As discussed elsewhere in this contribution, it will also be very relevant for companies envisaging internal investigations to consider very closely the implications of GDPR thereon – data-protection is very much at the forefront of many concerns. Finally, it should also be reminded that Belgium, as an EU Member State, will have to implement under Belgian law the provisions of the EU Whistleblower Directive of 7 October 2019.

CONTACTS

Pericles Building
Rue de la Science 23
Brussels 1040
Belgium

Tel.: + 32 2 505 0911
Fax: + 32 2 505 0996
https://www.hoganlovells.com/en/locations/brussels

Fabien Roy
Partner
Hogan Lovells
T +32 2 505 0970
fabien.roy@hoganlovells.com

Fabien Roy has been a member of the Brussels Bar since 2011 and a partner at Hogan Lovells since 2019.

His practice focuses on European Union (EU) and national regulatory matters involving medical devices and pharmaceutical laws and guidelines. Fabien follows the new regulations on medical devices (MDR and IVDR) and the GDPR very closely and regularly advises clients on the requirements applicable to their digital health technologies. Fabien is also a qualified lead auditor for ISO 13485 quality management systems. He consequently has a deep understanding of the range of quality issues encountered by companies and regularly advise clients in relation to internal/external audits and investigations.

Raphaël Fleischer
Senior Associate
Hogan Lovells
T +32 2 505 0914
raphael.fleischer@hoganlovells.com

Raphael has been a member of the Brussels Bar since 2012 and a Senior Associate at Hogan Lovells since 2019.

His practice focuses on handling the full range BeNeLux, EU and global antitrust aspects of M&A transactions. Raphael has worked with clients from around the world and across diverse industries to successfully navigate both, Phase I and Phase II merger investigations before the European Commission, the Belgian Competition Authority and national competition authorities in over 30 jurisdictions around the world. In addition to his work in M&A/merger control, Raphael has also been involved in various abuse, cartel, and other antitrust investigations in Belgium, the EU and beyond that. In that regard, Raphael very regularly advises clients in relation to internal/external antitrust-related audits and investigations.

Ivan Pico

Associate
Hogan Lovells
T +32 2 505 0969
ivan.pico@hoganlovells.com

Ivan Pico has been a member of the Brussels Bar since 2016.

Ivan Pico advises clients on a range of EU regulatory matters with a particular focus on EU competition law, including antitrust and merger control. His experience includes working on complex international mergers, global cartel investigations, distribution agreements, compliance and abuse of dominance cases.

He has advised various clients on competition law issues in the fields of semi-conductors, robotics, aerospace, and in the automotive industry. For clients looking at expanding and/or selling a part of their business, as well as clients setting up complex joint venture structures, Ivan can also help you in quickly determining the jurisdictions where merger filings are required or recommended. In this regard, Ivan frequently deals with the European Commission and national competition authorities, in particular the Dutch competition authority, in order to secure the necessary merger approvals within the commercial deadlines.

As a Belgian qualified lawyer, Ivan regularly pleads before the Belgian courts and helps international companies with complex queries under Belgian or EU law. Ivan also assists several companies active in the area of defense with EU and international law related advice.

Hélène Boland

Associate
Hogan Lovells
T +32 2 505 0976
helene.boland@hoganlovells.com

Hélène Boland has been a member of the Brussels Bar since 2017.

Her practice focuses on EU and national regulation of pharmaceuticals, biotechnology, medical devices, special foods and feed, personal protective equipment, cosmetics and other consumer products. She also assists clients in understanding the requirements introduced by the EU General Data Protection Regulation and various aspects of digital health technologies. Hélène regularly advises international companies with complex queries in relation to Belgian or EU law.

Alexander Wenzel

Associate
Hogan Lovells
T +32 2 505 0911
alexander.wenzel@hoganlovells.com

Alexander Wenzel has been a member of the Brussels Bar since 2018. He assists Life Sciences clients in navigating the requirements that govern their activities, including, compliance with anti-benefit, transparency and data protection requirements. He frequently assists clients that are being investigated by competent authorities.

Prior to joining Hogan Lovells, he was an external research assistant at an institute of the University of Vienna, and, a trainee with the European Commission's infringement procedure coordination unit for the Internal Market.

Bulgaria

Kambourov & Partners

Ivo Alexandrov

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X No criminal liability for companies, but administrative sanctions may be applied in case of employee misconduct.	X	X	X	
No					X No explicit legislation.

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Public interest in whistleblower protection has recently increased in Bulgaria as in the rest of Europe. However, Bulgaria has no specific legislation in relation to whistleblower protection yet. It will also take time for the Bulgarian legislator to catch up on other country's more developed legal systems. The new Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law ("**Directive (EU) 2019/1937**") must be implemented in local law by 17 December 2021.

In general, Bulgaria is a party to the United Nations Convention against Corruption, the Council of Europe ("**COE**") Civil Law Convention on Corruption, and the COE Criminal Law Convention on Corruption. To fulfill its treaty obligations, Bulgaria provides some protection to whistleblowers through its regulatory framework already now:

- Whistleblower reports and internal investigations in the public sector are regulated in the Administrative Procedure Code ("**APC**"). The APC generally protects whistleblowers in the public sector by protecting them from persecution by the authority against which they have filed a report. Anonymous reporting is not permitted under the APC.
- The Civil Servants Act ("**CSA**") regulates the functions of the inspectorates at the Ministries as the authorities competent to be notified of signs of corruption and to initiate internal investigations. Only civil servants are subject to the CSA. Pursuant to the CSA, the inspectors at the respective inspectorate shall conduct general and specific investigations in accordance with an annual plan endorsed by the Executive Director of the General Labor Inspectorate Executive Agency. Additionally, the inspectors may perform unscheduled investigations pursuant to complaints submitted by officers.

– The Bulgarian Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act ("**CCUAAFA**") created the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Commission (the "**Commission**") and its legal framework. Every citizen with information on corrupt practices will be able to report to the Commission, which has the authority to initiate proceedings against public officials. Anonymous reporting is not permitted under the CCUAAFA, but the Commission should not disclose the identity of the whistleblower to the public. Moreover, the Commission may take affirmative steps to protect the whistleblower from retaliation. Any whistleblower who has been dismissed, prosecuted or harassed, shall be entitled to compensation for any damages suffered thereby.

Whistleblowing in the private sector is less regulated. Sanctions against whistleblowers, including dismissal, are allowed under certain conditions. For instance, under the Labor Code ("**LC**"), an employee may be dismissed for abusing the employer's confidence or disclosing confidential data, although the dismissal may be challenged in court. However, the latest amendments in the Measures Against Money Laundering Act ("**MAMLA**"), provide some protection to employees who report internal signals of potential or actual violations of the MAMLA. Article 15(10) of MAMLA provides that the submission of a report by an employee shall not be grounds for termination of the employment relationship or civil-service relationship of such employee or for applying other disciplinary measures or sanctions.

In practice, due to the lack of specific local regulation, private companies apply different approaches in relation to whistleblowers' queries. International companies that have established branches in Bulgaria apply systems of disclosure of unlawful practices that are provided in their internal policies. Small and medium companies with predominantly local participation in the share capital have not developed specific internal rules and the human resources departments usually serve as point of contact for whistleblower reports.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Works councils do not exist in Bulgaria. The collective interests of employees are represented by trade unions and employee representatives elected by the employer. In general, trade unions represent and protect employees' interests before government bodies and employers. The trade unions enjoy, however, very limited rights. The LC does not require that trade unions be informed about internal investigations. Hence, the participation of trade unions in internal investigations is not prevalent.

b) Under the EU General Data Protection Regulation ("**GDPR**") the Data Protection Officer ("**DPO**") must consult with employees about their data privacy rights. An employer must, therefore, inform the DPO about all investigations that implicate data privacy. Furthermore, the Bulgarian Personal Data Protection Act ("**PDPA**") requires employers to inform the Bulgarian Commission on Personal Data Protection when personal data collected during investigations is intended to be transferred to a non-EU state.

c) The Criminal Procedure Code ("**CPC**") obliges employees to inform competent public authorities of criminal offenses, regardless of the status of an internal investigation.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees are not statutorily obliged to support an investigation, e.g. by participating in interviews. However, employees have a general duty to obey any lawful orders of the employer, to follow internal rules adopted by the employer, and to discharge other duties provided by law. Employers may adopt internal rules regarding the conduct

of investigations and may request that employees answer work-related questions during an investigation. An employee's refusal may be regarded as misconduct, which could justify imposing disciplinary measures. Prior to imposing disciplinary measures, however, an employer must consider an employee's verbal explanations or examine their written notes. Failure to do so may lead to revocation of the imposed disciplinary sanction by the court.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Under the LC, disciplinary sanctions (e.g. dismissal) must be imposed within two months after discovery of the breach and no later than one year after the commission of the offense. Sanctions imposed outside of the statutory period are invalid. Investigations should therefore, be concluded quickly.

In the public sector, the APC provides a prescription period for reporting of two years from the date that the unlawful practices occurred.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

"Personal data" is defined in the PDPA as any information related to an individual which, directly or indirectly, identifies the individual or makes them identifiable. If an employer plans to collect personal data during an interview, it is necessary to obtain the consent of the person whose personal data shall be collected prior to the interview.

b) Reviewing emails?

Before reviewing emails containing personal data or information, consent of the data subject should be obtained. The data subject has the right to be informed about the purpose of the processing, the categories of data concerned, and the identity of the recipient(s) of the data.

Although the constitutional right to confidential correspondence in Bulgaria is not thought to apply to business or private correspondence sent or received via, or stored on, a company's electronic devices, the European Court of Human Rights ("**ECHR**") recently ruled in *Bărbulescu v. Romania* that a company may not monitor an employee's work email without explicitly informing them in advance. As a member of the COE and a party to the European Convention on Human Rights and Fundamental Freedoms, Bulgaria is obliged to implement the decision of the ECHR.

c) Collecting (electronic) documents and/or other information?

While collecting electronic documents, one should take into account the obligations under the PDPA and the Electronic Document and Electronic Signature Act ("**EDESA**"). According to Article 43 (4) of the EDESA, only personal data relating to the data subject may be collected; data from a third person may only be gathered with their explicit consent.

d) Analyzing accounting and/or other mere business databases?

It is not necessary to obtain an employee's consent to review accounting or financial records that do not contain personal data.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

While there is no legal obligation to provide an interviewee with written instructions, such a requirement might be found in a company's internal rules.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no legal obligation to inform an interviewee about the right to be free from self-incrimination during an internal interview. During a criminal interrogation, however, prosecutors must inform the individual of their right to remain silent.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

Although there is no legal obligation to provide an "Upjohn warning", it is regarded as good practice to do so and may even be required by the employer's internal rules.

d) Be informed that they have the right that their lawyer attends?

There is no such obligation. The internal rules of the employer should also be consulted in this regard, as they may not allow third parties to attend interviews, including counsel for the interviewee.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Employees do not have the right to have trade union representatives attend their interviews.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Above all, the GDPR restricts transfers of personal data outside the European Economic Area, unless the rights of the individuals in respect of their personal data are protected in another way, or one of a limited number of exceptions in the legislation applies. Therefore, without the consent of the interviewee, the employer shall generally not transfer personal data cross-border. In addition, the PDPA requires employers to inform the Bulgarian Commission on Personal Data Protection when personal data collected during investigations is intended to be transferred to a non-EU member state.

g) Sign a data privacy waiver?

Employers must receive written, informed consent in order to process personal data.

h) Be informed that the information gathered might be passed on to authorities?

The interviewee must be informed that the information might be passed on to authorities, especially when it contains personal data.

i) Be informed that written notes will be taken?

There is no legal obligation to inform the interviewee that notes will be taken during the interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no law pertaining to the use of document hold or retention notices in Bulgaria. Employers must be careful not to retain certain documents in violation of the law. For example, retaining working files of a former employee may, under certain circumstances, be unlawful and could result in civil liability for the employer. Pursuant to the GDPR and the PDPA, processing of personal data outside its legitimate purpose is forbidden and the personal data should be deleted once the legitimate purpose for which it was collected is fulfilled. Therefore, employers should limit the processing of personal data, and not keep personal data once the processing purpose is completed. On the other hand, employers are able to retain certain administrative documents, such as payroll files, even after the end of an employment relationship.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege is provided for in the Bulgarian Bar Act ("**BA**"). According to Article 33 of the BA, correspondence and conversations between a lawyer and a client are confidential. Attorney papers, files, electronic documents, computer equipment, and other carriers of information may not be subject to inspection, copying, verification, or seizure. The scope of protection is broad in order to guarantee the protection of privileged

information. An internal investigation report would fall under the attorney-client privilege, as it is considered information exchanged in the course of an attorney-client relationship. The best way to ensure the applicability of attorney-client privilege is to engage outside counsel.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Communication with an in-house lawyer is not considered privileged under Bulgarian law. However, in-house counsel, as a regular employee of the company, should handle correspondence according to the internal rules of the company.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Pursuant to the Bulgarian Insurance Code, the insured entity is obliged to declare to the insurer all new circumstances, which the insurer has raised to the company at the conclusion of the contract. New circumstances must be revealed to the insurance company immediately after they are known. Early notification to the insurance company may be a subject of the terms and conditions of the insurance policy.

b) To business partners (e.g. banks and creditors)?

Early notification requirements may stem from contractual clauses. In addition, it is generally advisable to provide such notification to avoid future complication. It is common practice for banks to oblige borrowers to notify them in case of an adverse event, which may harm the interests of the bank.

c) To shareholders?

If an internal investigation may affect the stock market price of a publicly traded company, this information must be disclosed in accordance with Bulgarian law. However, the volume of the disclosed information shall be evaluated on a case by case basis, taking in consideration the imperative rules for trading with inside information and market manipulation (market abuse).

d) To authorities?

Prosecution authorities should be notified about any criminal offense that is discovered during an investigation, but no general early notification at the start of an internal investigation is necessary.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There is no law or regulation concerning the need to take immediate measures. However, companies must make sure that any ongoing criminal behavior in the company is stopped as soon as possible.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

As internal investigations are not regulated by Bulgarian law, the local prosecutor does not normally have specific concerns with them. Should the prosecuting authorities receive reasonable information about an act that could be considered a criminal offense, they are obliged to commence an investigation. If disclosed, the findings of an internal investigation may be the basis for the prosecutors to open a case and may also be useful to the prosecutors as they collect evidence during their criminal investigation.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Search warrants or seizure warrants are strictly regulated in Bulgarian law. A search or seizure may only be conducted where there is sufficient reason to believe that information significant to the prosecutors' investigation may be found.

A valid warrant must be in writing, signed by a judge, and contain the necessary material requirements. The individual subject to the search or seizure or, in the case of legal persons, a representative thereof, must be present during the search or seizure. Where no representative of a legal person can be present, the search and seizure may be carried out in the presence of a representative of the municipality.

In urgent cases, authorities may perform a search without prior judicial authorisation, should it be necessary to preserve evidence. However, in this case, a report documenting the investigative actions taken must be made and submitted for approval to a judge no later than 24 hours after the search or seizure.

Improperly gathered evidence may not be used against the company. Only evidence collected lawfully, as provided under the CPC, may be used in criminal proceedings.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Corporations are not subject to criminal liability under Bulgarian law. Thus, they cannot be subject to deals and non-prosecution agreements.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Companies are not subject to criminal liability, but may be subject to administrative sanctions, such as fines. Should the activities of a company be regulated by the state, the regulatory authority may suspend or revoke the company's license.

Individuals may be subject to the general criminal and administrative penalties for misconduct.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Given that the legal framework in relation to internal investigations and whistleblowers' protection is not comprehensive, as well as not codified in a specific legal act, the existing case law does not provide sufficient information on reduction of penalties. There is no case law that provides guidance on the implementation of an efficient compliance system as well as its effects and its assessment by the court.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Due to the lack of a centralized government agency that tracks whistleblower cases, the number of investigations and their outcome are not known. Many reports are made anonymously and sent to individual authorities. According to a European University Institute report, Transparency International Bulgaria's Advocacy and Legal Advice Center, a non-governmental organization providing free and confidential legal advice to witnesses and victims of corruption, has, thus far, received very few complaints from employees or civil servants reporting illegal activities or wrongdoing by their employers. Several whistleblowers accused of criminal defamation have been acquitted by the court, for instance individuals who disclosed mismanagement of municipal property and reported concerns in a police agency.

Given the increased discussion of whistleblowing at EU level and the new Directive (EU) 2019/1937, that must be implemented in local law by 17 December 2021, significant changes to Bulgarian law are expected.

CONTACT

KAMBOUROV & PARTNERS

ATTORNEYS AT LAW

37 A Fridtjof Nansen St.	Tel.: +359 2 986 9999
1142 Sofia	Fax: +359 2 986 9995
Bulgaria	www.kambourov.biz

Kambourov & Partners is a leading Bulgarian law firm with 30 years of experience. It is specialized in general business law and provides services under Bulgarian jurisdiction to domestic and international clients within various practice areas including Banking, Finance, Corporate, Employment, Competition, IP, TMT, Litigation & Arbitration, Restructuring & Insolvency, Real Estate, Tax, Energy, White Collar, Regulatory & Compliance, etc.

Ivo Alexandrov

Partner
Kambourov & Partners
T +359 2 986 9999
i.alexandrov@kambourov.biz

Ivo Alexandrov heads Kambourov & Partners' Regulatory & Compliance department, the Restructuring & Enforcement of Securities department and is a key member of the Banking & Finance and Corporate practices. Ivo represents local and international companies with respect to corporate crime-investigations as well as financial institutions, investment and hedge funds, project sponsors, etc., in a multitude of transactions, e.g. large syndicated financings, cross-border finance, transactions escrow of shares and financial instruments, enforcement of netting arrangements, custodian and escrow arrangements of financial instruments. He advises clients from a wide range of industries, including finance, banking, insurance, retail on complex domestic and EU regulatory requirements and is experienced in all areas of business and financial services regulation, as well in cross-border M&As, foreign investments, project finance, regulatory issues (public, commercial, economic, environmental, etc.).

Croatia

Babić & Partners Law Firm LLC


Iva Basarić


Lovro Klepac

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	
No					X No specific defense, but greater likelihood of liability for failure to implement anti-corruption programs.

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

The Croatian Whistleblower Protection Act (which came into force on 1 July 2019) sets out specific procedures that need to be observed in case a whistleblower report sets off an internal investigation. These in particular include (i) the employer's obligation to examine the whistleblower report within 60 days, (ii) the obligation to notify the whistleblower of the outcome of the internal investigation and – at their request – of actions undertaken in the course of the investigation, and (iii) the obligation to notify the competent authorities of the received whistleblower report. Furthermore, the law prohibits discrimination or unfavorable treatment of whistleblowers. The Croatian Labor Code also contains rules which prevent discrimination against whistleblowers who justifiably or in good faith report suspected corruption to the responsible parties or public authorities.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) The employer must obtain the consent of the works council prior to collecting, processing, or delivering the personal data of employees to third parties. Since internal investigations typically involve collecting and processing personal data and possibly delivering such data to third parties, employers practically cannot initiate such investigations without the prior consent of the works council. In addition, union

representatives, if appointed by the employer, generally also need to be informed of investigations concerning employees, who are members of the union.

b) Under Croatian data protection legislation, one of the duties of the data protection officer is to ensure that employees' rights with respect to personal data processing are observed. In this regard, it would be advisable to inform the data protection officer of the investigation and to provide the data protection officer with any information requested.

c) There is no legal requirement to inform the prosecution authorities of an internal investigation, unless the company has sufficient information to qualify the investigated misconduct as a criminal deed.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees have a general duty to cooperate in an investigation by providing information, which directly relates to their work. Violation of this duty may qualify as a breach of employment duties, especially if it leads to economic loss for the employer. Depending on the severity of the breach, non-compliance with an employer's request to support an investigation may result in termination of the employee. Company policies may provide more detailed rules governing employee duties and sanctions for violating such duties.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Investigative measures may initiate a 15-day deadline for summary dismissal for cause, in cases where the investigation uncovers gross misconduct of the employee. The deadline is triggered when the employer (i.e. a representative with authority to dismiss) becomes aware of the facts or circumstances reasonably leading to the conclusion that misconduct has been committed. To avoid triggering this deadline too early, the employer should be informed of the results of the investigation at a later stage, after comprehensive information has been gathered.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Before conducting interviews, in accordance with the transparency obligations set out in Croatian data protection laws, the employee must be informed of the purpose for which their personal data is collected and processed. Interviews should be limited to questions about work-related issues.

b) Reviewing emails?

Employees' electronic communications may be monitored only in extraordinary circumstances when the following prerequisites are met: (1) the processed data may only be collected to satisfy the specific purpose of such surveillance and cannot be used for any other purpose; (2) the possibility of electronic communication surveillance must be transparently communicated to the employees (e.g. by way of company policies); (3) there must be a legitimate purpose for monitoring; and (4) a proportionality test must be met, i.e.the surveillance should generally be limited to data traffic and not include content, which may only be monitored if absolutely necessary. The above principles also remain valid under Regulation (EU) 2016/679 ("**GDPR**"). In addition, such processing would be subject to a data protection impact assessment ("**DPIA**") obligation in accordance with Article 35 of the GDPR and the review of the list of kinds of processing operations that are subject to the DPIA adopted by the Croatian Data Protection Agency.

c) Collecting (electronic) documents and/or other information?

Although communication with authorities can trigger applicability of data protection laws, a request of an authority will often be a sufficient justification for gathering and using data to comply with the legal obligation which the controller is subject to.

d) Analyzing accounting and/or other mere business databases?

A company is generally free to analyze any accounting and other mere business databases.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

Croatian law does not provide for an express obligation on the employer to deliver written instructions to the employee before starting an interview. However, employees should always be timely informed about the processing of their personal data as required by GDPR transparency obligations. As a best practice, it is advisable to provide the employee with general information about the investigation and to document this in writing.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

In contrast to investigations initiated by the prosecution authorities, there is no right to remain silent during an internal investigation conducted by a company. However, the employer should avoid putting any pressure on the employee to self-incriminate in order to mitigate potential future duress claims by the employee.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no duty under Croatian law to provide an "Upjohn warning" to the interviewee, though it is advisable to do so.

d) Be informed that they have the right that their lawyer attends?

Croatian law does not expressly provide that an interviewee has a right to have an attorney present at their interview. However, if the employee requests to have their attorney present, it is advisable to allow it.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Employees do not, under the default rules of Croatian labor law, have a right to have a works council representative present at their interviews. Company policies and collective agreements, if any, should be consulted in order to assess whether such rights are provided therein. In any case, it is advisable to allow the attendance of a member of the works council or other representative body upon employee request.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Transfer of data to non-EU states or organizations is only permissible if compliant with Chapter V of the GDPR, i.e. if it is based on an adequacy decision, appropriate safeguards etc. With respect to the United States, transfers based on Decision 2016/1250 on the adequacy of the protection provided by the EU - U.S. Privacy Shield are illegal. Transfer of data to United States may be based on appropriate safeguards (e.g. standard clauses) if the controller or processor adopts supplementary measures which, along with the appropriate safeguards, ensure the level of protection essentially equivalent to that in European Union. In some cases of occasional and non-repetitive transfers, the controller may rely on derogations from Article 49 GDPR. Employees must be informed about the transfer in accordance with GDPR transparency obligations.

g) Sign a data privacy waiver?

The interviewee does not need to sign a data privacy waiver before conducting the interview. This is because the employee's consent would not be required for processing of employees' data obtained during the interview or otherwise in the course of internal investigation. However, the employee should be informed of processing of their data in accordance with the GDPR transparency obligations.

h) Be informed that the information gathered might be passed on to authorities?

The data subject should be informed about the recipients of their personal data, including authorities. If the information is not obtained directly from the data subject, the controller may be exempted from the obligation to inform the data subject if the obligation to pass on information to authorities is expressly regulated by law. If an interview yields evidence of a crime, the employer must pass on such information and evidence to the authorities and does not need to inform the employee either (1) that there is a duty to deliver

such information to authorities; or (2) that the information will be passed on to prosecution bodies. Processing of such data is expressly mandated by the rules of criminal procedure.

i) Be informed that written notes will be taken?

There is no obligation under Croatian law to inform the interviewee that notes of the conversation will be taken. It is, nevertheless, advisable to inform the employee and to ask the employee to co-sign the notes, as confirmation of their accuracy, in case any litigation is subsequently initiated.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Croatian law does not address document hold or retention notices. However, the rules of criminal procedure provide for a general duty of any legal entity reporting a crime to preserve existing traces or evidence of a committed offense. In addition, special procedural rules exist to secure evidence in civil litigation. An application may be filed by any of the parties before or during (civil) litigation proceedings if justified doubt exists that certain events would hinder the examination of evidence at a later stage of the proceedings. If such an application is filed before the proceedings are initiated, the evidence shall be examined by the competent court in the territory where the evidence is located.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege may generally only be claimed with respect to correspondence with outside counsel and documents in the possession of outside counsel. In order to ensure privilege protection, internal investigations, including interviews, should be conducted by/through outside counsel.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Under Croatian law, attorney-client privilege does not extend to in-house counsel.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Generally, early notification to insurance companies will be required where circumstances are uncovered that may form the basis for an insurance claim. However, notification obligations depend on the agreement and the type of insurance.

b) To business partners (e.g. banks and creditors)?

The company may be required to inform its business partners of internal investigations and related findings, if required by the agreements with the respective partners. The company may also be required by the good faith principle to inform its business partners of an investigation, if the investigation and its consequences may have significant impact on the business partners. This should be assessed on a case-by-case basis, balancing the opposing interests.

c) To shareholders?

Depending on the information and/or misconduct uncovered and any provisions to this effect in the company's internal policies, the management board may be obligated to notify shareholders. However, the management board has rather broad discretionary power in assessing whether to notify shareholders or maintain confidentiality.

According to Croatian securities trading legislation, if the information gathered by an internal investigation is of a precise nature and would probably significantly influence the price of financial instruments issued by the company, it is the duty of the management board to report such information to the public.

d) To authorities?

There is no general duty to notify the State Attorney's Office or any other authority of an ongoing internal investigation. However, every person is obliged to report criminal activities. In some instances, such as for company directors or officers, violation of this duty may result in criminal prosecution.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Depending on the nature and severity of the alleged wrongful conduct, the company should strive to mitigate any further damage. Subject to the company's code of conduct and other policies, employees may be sanctioned for uncovered misconduct. In addition to sanctioning employees, the company should re-evaluate and improve its compliance system.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices do not generally have concerns about internal investigations conducted by companies. Documents gathered during a corporate internal investigation may be used in subsequent proceedings initiated by the local prosecutor. Therefore, the company should ensure retention of documents and any information that may be later requested by the prosecutors.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

A dawn raid may be undertaken when it is probable that a person who committed a criminal deed and the object of a criminal offense or traces of evidence can be found in particular spaces. Dawn raids conducted by the Croatian competition regulator must be approved in advance by the High Administrative Court. Warrants required to conduct a dawn raid are governed by the Croatian Competition Act and subject to special rules. The court must render a decision within two days of the regulator's request. The warrant, which is issued by the High Administrative Court, must identify the object(s) of the search, the legal basis for the raid, the person(s) authorized to conduct the raid and the deadline for execution of the warrant. The warrant must be presented to the owner or operator of the premises on which the dawn raid is conducted. Authorized officials conducting the dawn raid may: inspect the entire premises; inspect and copy business records and other documents; and seal the premises, business records, or other documentation as long as necessary to conduct the raid.

Search warrants must be issued by a competent court, unless an immediate search is necessary to preserve evidence directly related to a crime, which is in danger of being lost or destroyed. A search warrant must identify the object of the search and its purpose and name the authority conducting the search. A search warrant must be issued in writing and signed by a judge. The search must be conducted within three days of issuance of the warrant. The warrant must be presented to the person whose premises are to be searched and the search must be witnessed by at least two persons of legal age. An authorized representative of the company must be informed of their right to attend the search. Failure to inform is a violation of criminal procedure, but would not lead to the inadmissibility of evidence uncovered during the search.

Not every procedural infringement during a search will lead to the evidence collected being deemed inadmissible. Croatian criminal law and Supreme Court practice both recognize that only serious procedural violations may lead to a finding of inadmissibility in criminal proceedings. Specifically, only evidence gathered during a search undertaken without a warrant or without the required witnesses may be excluded from criminal proceedings.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Deals, non-prosecution agreements, and deferred prosecution agreements are available and encouraged in Croatian criminal law and the practice of the State Attorney's Office. For a non-prosecution agreement or deferred prosecution agreement to be implemented, several substantive and procedural requirements must be met. First, the penalty prescribed for that particular offense cannot be more than five years' imprisonment. Second, the suspect or the accused must undertake either to compensate the injured person for damages suffered by the crime, donate to humanitarian or social causes, or participate in community service. If the suspect or accused satisfies the requirements within one year, the State Attorney must dismiss the criminal charge.

Plea bargains are also available under Croatian criminal procedural law. The accused and the State Attorney may negotiate the conditions of the plea and the subsequent sanctions. During such negotiations, the accused must be represented by an attorney. The deal negotiated between the accused and the State Attorney must be executed in writing, signed by both parties, and confirmed by the competent criminal court. Criminal procedural rules concerning the content of such deals must also be observed.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Under Croatian law, companies and other legal entities may be subject to criminal liability for the criminal conduct of officers and directors. Companies that are found liable are subject to monetary fines, dissolution, and associated protective measures, such as operating bans, disgorgement of profits, exclusion from public tenders, and exclusion from obtaining licenses, permits and concessions. Administrative or misdemeanor fines may be imposed for less serious violations.

A company's directors and officers may be held liable for failing to report misconduct of other directors, officers, or employees and may face up to three years' imprisonment.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Croatian laws do not expressly determine efficient compliance systems as mitigating factors in determining penalties. However, in practice, efficient compliance systems (whether implemented prior or following the alleged misconduct) may be argued as a mitigating factor with the intention of the courts/authorities reducing the fines to be imposed (especially in competition law cases).

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The adoption of the Croatian Whistleblower Protection Act recently attracted significant public attention, as it introduced additional obligations for employers, including obligations to appoint a person authorized to handle reporting of irregularities, to protect whistleblowers and confidentiality of reported information, as well as to undertake measures to remedy reported irregularities.

CONTACTS

BABIĆ & PARTNERS
LAW FIRM

Nova cesta 60/ 1st floor
10000 Zagreb
Croatia

Tel.: +385 1 3821 124
Fax: +385 1 3820 451
www.babic-partners.hr

Iva Basarić
Partner
Babić & Partners
T +385 1 3821 124
iva.basaric@babic-partners.hr

Iva Basarić is a partner at Babić & Partners. Iva earned an LL.M. degree in International Transactions and Comparative Law at the University of San Francisco, USA. She regularly advises clients from diverse industries on various corporate/commercial, regulatory and data privacy issues. Iva has vast experience in assisting international clients with all aspects of internal investigations conducted in their Croatian subsidiaries. In 2006/2007 Iva participated in the Willem C. Vis international Commercial Arbitration Moot, as a member of the University of Zagreb moot team that was awarded second place in the oral rounds of the competition.

Lovro Klepac
Senior Associate
Babić & Partners
T +385 1 3821 124
lovro.klepac@babic-partners.hr

Lovro Klepac is a senior associate and member of employment law group at Babić & Partners. After graduating from the University of Zagreb, Faculty of Law, he earned an LL.M. degree in international business law at the Central European University in Budapest. Lovro's practice comprises all aspects of the firm's employment law practice, including advising on data privacy issues and employee investigations. He was a member of the University of Zagreb moot team at the Willem C. Vis international Commercial Arbitration Moot that was awarded honorable mention for Memorandum for Respondent in 2015/2016.

Cyprus

Chrysses Demetriades & Co LLC

Demetris L. Araouzos

Sophia Nearchou

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X Depending on the type of offense.	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

In general, Cyprus does not have a specific law to protect whistleblowers against retaliation and to provide whistleblowers with appropriate reporting channels.

Although ambiguous, certain legislation, set out hereunder, suggests that indirectly there is a shield for public and private sector employees who report wrongdoing.

Under the Public Service Law, employees of the public sector are required to report wrongdoing, as non-reporting may lead to criminal prosecution. Whistleblowers are protected: retaliating against a whistleblower is a crime in Cyprus. Affected employees are entitled to compensation if they suffered financial or emotional harm. An additional shield of protection is offered by the Labor Law to both private and public sector employees, as this law requires objective grounds for dismissal of officials.

The only body issuing provisions exclusively for whistleblower protection in the private sector is the Cyprus Securities and Exchange Commission ("**CySEC**"). CySEC issued a circular under Article 12(1) of the Market Abuse Law of 2016 by which it establishes procedures for the receipt of whistleblower reports and follow-up measures. Whistleblowers can submit reports of infringement by submitting the 'Whistleblowing External Disclosure Form' by email or post, or can make a report through the CySEC's hotline.

A draft bill providing additional measures for whistleblower protection, the Reference of Acts of Corruption Law of 2017, is currently pending before parliament. Until its passage, whistleblower protection can be sought under the provisions of the Council of Europe ("**COE**") Civil Law Convention on Corruption and the COE Criminal Law Convention on Corruption. According to these laws, an employee shall not face any sanctions for whistleblowing,. According to Article 22 of the Criminal Law Convention, authorities and agencies must ensure effective and appropriate protection for whistleblowers and witnesses, who cooperate with authorities to prosecute offenses listed in Articles 2 to 14.

Furthermore, Article 69B of the Anti-Money Laundering Law 188(i)/2007, as amended, protects individuals who submit a report. When a suspicious activity report (SAR) is submitted by an employee, the internal reporting officer evaluates the submission and may create an external report that is forwarded to the Unit for Combating Money

Laundering ("**MOKAS**"). Article 69B protects whistleblowers from being exposed to threats or hostile action and, in particular, from adverse or discriminatory employment actions.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Although employee representative bodies do not have a legal right to be informed of the start of an investigation, it is considered a best practice to allow an employee to have a union representative attend their interview, if the employee requests such attendance.

b) According to the Personal Data Protection Law ("**PDPL**"), the Data Protection Officer ("**DPO**") must supervise all processing of personal data to ensure data security and prevent unauthorized disclosure or unfair treatment. "Personal data" means any information relating to an identified or identifiable natural person. Hence, the DPO should be notified before starting an internal investigation, which will require the collection and processing of personal data. The PDPL will be superseded in May 2018 by the European Union's General Data Protection Regulation ("**GDPR**"). Pursuant to the GDPR, a company conducting an internal investigation must also inform the DPO of all processing activities being conducted for the investigation.

c) No other local authority needs to be informed of an internal investigation, other than the regulators (if necessary) and/or the prosecution authorities, who must be notified if criminal conduct is uncovered during the investigation. The Public Service Law and the Code of Ethics of the Public Services oblige civil servants to report suspected cases of corruption or bribery to their respective authority. Failure to do so constitutes an offense.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

No law in Cyprus provides an affirmative obligation for an employee to cooperate with an internal investigation. However, pursuant to the Employment Law (24/1967), if an employee's refusal to cooperate clearly and unequivocally shows that the employment relationship can no longer be continued, the employee can be dismissed without notice.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

No reference to the initiation or waiver of labor law deadlines is made in the Employment Termination Law of 1967.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

The PDPL applies to any processing of personal data, including the gathering or recording of such data in an interview. Before personal data may undergo any kind of processing, the data subject must be informed who is collecting the data, for what purpose, and with whom the data is to be shared. The consent of the data subject must also be obtained. Consent must be freely given.

b) Reviewing emails?

According to the PDPL, personal data, such as emails, may only be collected and processed when: (1) the data subject has given explicit consent; (2) the processing is necessary for the data controller to fulfill its obligations or to perform its duties; and (3) the Data Protection Commissioner, the data protection authority in Cyprus, has authorized the collection, where data will be transferred outside of the European Union.

c) Collecting (electronic) documents and/or other information?

The PDPL must be observed not only with respect to emails but to all documents and information containing personal data.

d) Analyzing accounting and/or other mere business databases?

Analyzing mere business databases does not fall under the definition of personal data processing. Therefore, the provisions of the law regarding the right to be informed do not apply.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no statutory obligation to give written instructions to an employee before an interview, but the employee must be given advance notice that an interview may occur.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

Only when an individual is interviewed by criminal authorities, such as the police, do they have the right to remain silent.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no obligation under Cyprus law to provide an "Upjohn warning".

d) Be informed that they have the right that their lawyer attends?

Parliament is currently debating a bill that would provide an individual the right to request the presence of their lawyer during questioning by police and/or prosecutors. Currently, no such right exists. The bill does not apply to internal investigations.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

It is considered a best practice to allow an employee to have a union representative attend their interview, if the employee requests such attendance. However, the employee does not have a legal right to have the representative attend.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The PDPL requires that the data subject be informed of data transfers, as the data subject's consent is required. If the data is to be processed for any purpose other than that for which it was originally obtained, the data subject must again be informed. According to the PDPL, the cross-border transmission of data must be authorized by the Data Protection Commissioner. The Data Protection Commissioner will typically only authorize a transfer to another country if the country to which the data will be sent provides an adequate level of protection.

g) Sign a data privacy waiver?

Under the PDPL, a waiver may be required if the personal data of the employee may be used for a purpose other than the original purpose given for the collection or may be given to third parties. The employee must be informed of the purpose and give their consent.

h) Be informed that the information gathered might be passed on to authorities?

There is currently no legal obligation under the PDPL to inform an employee that information gathered during the interview may be passed on to authorities. However, under the GDPR, the data subject must be

informed why their data is being collected and how it will be processed. The data subject must also be informed if their data will be transmitted to a third party, including authorities.

i) Be informed that written notes will be taken?

There is no legal obligation under Cyprus Law to inform the employee that written notes will be taken, but it is common practice to do so.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific provision in the law on whether document holds or retention notices are allowed. As internal investigations are not yet common in Cyprus, such notices are also not customary.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The Legal Professional Privilege derives from the Advocates' Law (Cap. 2) and the Advocates' Code of Conduct 2002 (the "**Regulations**"). According to the Regulations and, as a general rule, communications and dealings of advocates with their client are protected by the Legal Professional Privilege. The advocate is under a duty to keep strictly confidential information derived from communication with the client, once the advocate-client relationship has been established. However, the privilege only extends to legal communications, i.e. communications seeking/obtaining legal services or advice. As internal investigations are not yet common in Cyprus, it is unclear whether the Legal Professional Privilege would apply to them. The privilege does apply in criminal and regulatory investigations by authorities.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Legal Professional Privilege also applies to in-house counsel in Cyprus, provided that in-house counsel is admitted to the Cyprus Bar.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Early notification requirements may stem from individual insurance policies, but there is no statutory notification obligation.

b) To business partners (e.g. banks and creditors)?

Notification to business partners is only necessary if required by the agreement between the partners and the company.

c) To shareholders?

A shareholders' agreement may provide an early notification requirement. Otherwise, if a company's shares are publicly traded, it has a duty to inform the public about information that could affect the stock price. However, a company is not required to provide notification at the start of an investigation.

d) To authorities?

Generally, there is no obligation to inform authorities about internal investigations within a company. The obligation may arise if a criminal offense is involved.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There is no law concerning the need to take immediate measures, but best practices would mean that any criminal conduct is stopped immediately. Mitigation measures may include the dismissal of wrongdoers and the protection of whistleblowers against unfair dismissal or other punishment.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Generally prosecutors play no role in internal investigations. However, prosecutor offices may become involved if they are notified by the company that an internal investigation is ongoing and their involvement is deemed necessary.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

For searches and dawn raids of companies in Cyprus, certain prerequisites must be fulfilled.

According to Section 27 of the Criminal Procedure Law, a judge can issue a search warrant on the basis of a sworn statement that there are reasonable grounds to believe that evidence, which may be used as proof of the commission of an offense, will be found. The search warrant authorizes the person named in the sworn statement to enter the premises and seize such evidence.

Various regulatory authorities, including CySEC and the Competition Commission, as well as government agencies, such as tax authorities, have the right to enter and seize evidence for their administrative purposes without warrants (dawn raids).

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Cyprus law has no provisions regarding plea agreements, settlement agreements, prosecutorial discretion or similar means without trial.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Depending on the type of criminal offense, a company may be fined and its directors, officers, and employees imprisoned and/or fined.

For administrative violations, regulatory authorities may, among other things, impose administrative fines, suspend professional licenses, order disgorgement of profits earned through wrongful conduct, and/or ban individuals from discharging managerial responsibilities.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

There is no statutory defense pertaining to any compliance systems. However, such compliance systems may be taken into account by the court as a mitigating factor in case of conviction.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Political efforts to strengthen whistleblower rights began in 2011 following a catastrophic explosion at a central army base in Cyprus, which killed 13 people. The committee investigating the incident reported in its findings that the disaster may have been avoided had whistleblower protections been in place.

In 2014 Transparency International-Cyprus ("**TI-C**") launched the European program "Speak UP II" to provide support, guidance, and information to victims of corruption and to whistleblowers. TI-C has recommended 43 measures to the Minister of Justice and Public Order in Cyprus to prevent corruption and promote integrity. The latest EU Commission anti-corruption report found that perceptions of corruption in Cyprus were generally similar to the average for Europe as a whole.

However, in the opinion of the EU Commission, the small number of cases investigated, prosecuted or adjudicated in Cyprus indicates the need to strengthen the enforcement system. This should be done by implementing transparency and integrity safeguards facilitating detection and collection of evidence. The EU Commission further recommended additional efforts to ensure closer coordination of relevant bodies. It also made several suggestions including the introduction of new legislation offering protection to whistleblowers who disclose abuse of power or other illegal behavior in the public and private sector.

CONTACTS

CHRYSSES DEMETRIADES & CO LLC

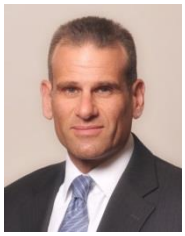
13 Karaiskakis Street
3032 Limassol
Cyprus

Tel.: +357 25 800 000
Fax: +357 25 588 055
www.demetriades.com

Established in 1948 – Chrysses Demetriades has always been instrumental to the development of Cyprus as an offshore and international financial center. Widely acknowledged and consistently ranked as one of the leading law firms in Cyprus by the independent legal directories the Legal 500, Chambers and Law Firm Directory.

Chrysses Demetriades & Co. LLC is a Cyprus law firm providing a comprehensive range of legal services to local and international clients. We have long established relationships with many of the world's leading international financial institutions, professional advisers and regulatory bodies, are consistently highly rated in independent research studies and regularly lead offshore league tables. Our success is founded on our ability to provide practical, creative and cost-effective advice, combined with an uncompromising service commitment to our clients and a strong dedication to our lawyers, staff and the communities in which we practice. We have been instrumental to the development of Cyprus as an offshore and international financial center and are widely acknowledged as one of the leading law firms in Cyprus in the key areas of corporate activity:

- Banking & Finance
- Capital Markets
- Corporate and M&A
- Employment
- EU & Competition
- Intellectual Property
- Private Client
- Property
- Regulatory Compliance
- Shipping
- Tax
- Litigation & Dispute Resolution



Demetris L. Araouzos

Partner
Chrysses Demetriades & Co. LLC
T +357 25 800 000
demetris.araouzos@demetriades.com

Demetris has extensive experience, *inter alia*, in commercial/corporate contentious matters that often involve large and well-known local or international groups or wealthy individuals, the proceedings of which invariably have to take place in multiple jurisdictions. Amidst the banking crisis in Cyprus in 2012-2013 and the collapse of one of the two major banks, Demetris was instructed to advise and bring proceedings on behalf of a failing bank against some of its ex-directors. He was also appointed by the Government of Cyprus as member of the legal team that defends Cyprus in ongoing ICSID proceedings that have been brought against it by certain Greek shareholders with substantial participation in the failing bank. He is occasionally retained to act for listed companies and their directors/officers on various regulatory issues and, as he invariably undertakes criminal work, he has been retained to defend ex-directors and senior officers of the largest Cyprus bank in market abuse criminal cases. Although Demetris spends most of his time before the Courts, he is often engaged in the negotiation and drafting of different types of agreements.

Sophia Nearchou

Associate
Chrysses Demetriades & Co. LLC
T +357 25 800 000
sophia.nearchou@demetriades.com

Sophia is a lawyer in the Compliance department of our firm, dealing with all Anti-Money Laundering ("AML") cases and regulatory compliance.

During the course of her employment, Sophia has also completed various courses relating to the Anti-Money Laundering (AML) compliance as well as various other forms of regulatory compliance such as in the fields of Personal Data Protection and tax related fields such as FATCA/CRS.

In July 2016, Sophia successfully passed the Financial Services and Regulatory Advanced Examination of the by Cyprus Securities and Exchange Commission (CySEC), which is recognized by the Charted Institute for Securities and Investment.

She further participated on the drafting of advice for clients involved in the sector and assisted in matters including CRS/FATCA reporting and compliance. Furthermore, in order to provide more quality to the services and advice offered, during June 2018 Sophia took the examination of CISI on Global Financial Compliance and alongside the Certificate in Global Financial Compliance (Cyprus) which she successfully passed and was awarded the CISI Level 3 Award in Global Financial Compliance. Since then she has been an Associate of CISI.

More recently, in June 2019, following a successful examination, she has obtained the Worldwide recognized and top level certificate in Money Laundering, the ACAMS certificate and is a member of CAMS Cyprus.

Czech Republic

Kinstellar

Michal Kníž

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Currently, there is no comprehensive law dealing with whistleblowers in the Czech Republic. State employees are protected by a regulation prohibiting any form of discrimination or retaliation against them. However, this regulation is considered vague by most. There were several legislative initiatives to adopt specific whistleblowing protection laws in the past but none of them was successful. The Czech government should now work on the implementation of EU Directive no. 2019/1937 on the protection of persons who report breaches of Union law.

Should an employer receive a whistleblower report, it might have a general obligation to prevent certain crimes (e.g. bribery) from being committed or to report certain crimes that have been committed to respective authorities under the Criminal Code. No other specific obligations (e.g. reporting back to the individual) currently exist pursuant to Czech law.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Pursuant to Sections 279 and 280 of the Czech Labor Code, certain matters must be discussed with, or at least, brought to the attention of employee representative bodies. However, internal investigations do not fall within the scope of these matters.

b) Given that personal data is most likely going to be processed in course of any internal investigation, the data protection officer must be informed on such processing. As regards the data privacy authority, since the implementation of the GDPR, there is no longer a general data processing notification (which existed under previous Czech data protection legislation) but only personal data breaches pursuant to the European

Union's General Data Protection Regulation ("**GDPR**") should be notified pursuant to Articles 33 and 34 of the GDPR.

c) A public prosecutor has neither the right to participate nor to be informed about an internal investigation, but voluntary disclosure of the results of the investigation may be advantageous in the event of subsequent criminal proceedings. However, a voluntary disclosure must be considered carefully. Due to insufficient regulations on structured criminal settlements and very few specific cases of leniency, the impact of voluntary disclosure on the outcome of a criminal proceeding is highly uncertain.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

While the obligation to cooperate with the investigation is not explicitly stipulated by law, such obligation may be inferred from general employee duties, such as the duty to protect the employer's property, the duty not to act in violation of the employer's legitimate interests, and the duty to prevent damage to the employer. Refusal to cooperate with the investigation may be treated as a breach of the employee's duties. Therefore, the employee would be subject to disciplinary proceedings, which may eventually lead even to dismissal. The employer may also claim damages. However, the calculation of such damages, in practice, might be complicated.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Investigative actions may trigger labor law deadlines under the Czech Labor Code. A supervisor, manager, or other person with authority must terminate or instantly dismiss an employee within two months after being informed of the employee's misconduct. To avoid triggering these deadlines, information about the investigation or its results should be shared with these decision-makers at a late stage in the investigation.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

It is essential to take into account data protection laws when conducting interviews, especially the GDPR, including the Czech implementing Act no. 110/2019, on Personal Data Protection. The Czech data protection authority has not issued any specific guidelines in connection with internal investigations yet.

b) Reviewing emails?

As when conducting interviews, data protection laws must be considered before reviewing emails. General provisions of the Czech Civil Code and Labor Code regarding privacy protection should also be considered.

c) Collecting (electronic) documents and/or other information?

Pursuant to the Czech Civil Code, electronic documents enjoy the same level of protection as paper ones. Therefore, while collecting documents, the relevant provisions of the GDPR, Civil Code, and Labor Code should be taken into account.

d) Analyzing accounting and/or other mere business databases?

No specific laws have to be considered when analyzing accounting and/or other mere business databases.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no obligation under Czech law to provide written instructions. However, it is advisable in certain cases to provide background information on the investigation to help expedite the investigation (i.e.no time has to be spent clarifying during the interviews).

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

In contrast with criminal proceedings, no warning regarding self-incrimination must be provided under Czech law during an internal interview.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

Czech law does not require providing an "Upjohn warning" to an interviewee, but it is advisable to do so.

d) Be informed that they have the right that their lawyer attends?

There is no obligation under Czech law to inform the employee of the right to counsel, as there is no right to counsel during an internal investigation. Participation in an interview is merely a fulfillment of an employee's duties and, therefore, there is no need for a lawyer to attend the interview.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

An employee has no right to have a representative from an employee representative body present during the interview.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Pursuant to the GDPR, an interviewee must be notified of potential cross-border data transfers. Privacy Shield provisions should also be considered.

g) Sign a data privacy waiver?

Generally, the consent of the data subject is necessary to process any personal data. However, the data controller (i.e. the employer) may process personal data without the data subject's consent if it is necessary for the rights or legitimate interests of the controller or another person. As this exception requires a balancing test between the legitimate interests and the rights and freedoms of the data subjects, the application of this exception should be considered carefully on a case-by-case basis.

h) Be informed that the information gathered might be passed on to authorities?

There is no legal obligation to inform the interviewee that information gathered might be passed on to authorities.

i) Be informed that written notes will be taken?

There is no legal obligation to inform the interviewee that written notes will be taken during the interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There are no specific laws governing hold or retention notices in the Czech Republic.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege is defined differently under Czech law than in common law jurisdictions. In the Czech Republic, it is an obligation of confidentiality on attorneys-at-law, which extends to all information that the attorney receives while providing legal services (with a few particular exceptions). The best way to ensure privilege protection over the findings of an internal investigation is to hire outside counsel. Only attorneys-at-law are exempt from the general duty to report to law enforcement certain crimes (e.g. suspicion of bribery). Any third parties involved in the investigation (e.g. forensic accountants) should be subcontracted by the external counsel.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Pursuant to Czech law, in-house lawyers do not enjoy the attorney-client privilege.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Notification to insurance companies is not required by law, but each insurance policy should be reviewed for such a possible obligation.

b) To business partners (e.g. banks and creditors)?

There are no statutory requirements when it comes to notifying business partners, but such an obligation may arise from agreements between the partners.

c) To shareholders?

Shareholders do not need to be notified at the start of an internal investigation. Publicly traded companies do not have any general notification requirements.

d) To authorities?

Generally, there is no duty to notify the prosecutor or any other authority of the start of an investigation. However, it is essential to take into account the reporting duty arising from the Criminal Code. This duty applies only to a limited list of crimes, including bribery offenses. A breach of this duty is a criminal offense. Every investigation should be therefore structured in a way to minimize the risk of falling under this reporting duty by, for example, hiring external counsel to conduct the investigation, as attorneys-at-law are not subject to the reporting duty.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Apart from the above-mentioned reporting duty, there are no special immediate measures to take into consideration once an investigation has started. However, the company has to make sure that ongoing criminal behavior is stopped as soon as possible.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

It is uncommon in the Czech Republic for local prosecutor offices to be involved in any way in internal investigations.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Search warrants as well as dawn raids must be pre-approved by the courts. Evidence obtained without prior court approval may not be used in subsequent criminal proceedings.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Corporations are able to enter into so-called "plea bargain" agreements with the prosecution, wherein the defendant pleads guilty to certain offenses and accepts a certain sanction. Plea bargains must be approved by a court.

Corporations charged with misdemeanor offenses (i.e. offenses with maximum penalty of five years' imprisonment) are also able to receive a conditional suspension of criminal prosecution and a settlement.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

The most common sanctions for individuals are imprisonment or fines, but the Czech Criminal Code recognizes a wide range of sanctions, e.g. prohibition of an activity or forfeiture of assets.

The range of sanctions for companies under the Corporate Criminal Liability Act is even broader and includes, among other penalties: fines; forfeiture; prohibition of certain activities; publication of judgment; prohibition on receiving grants or subsidies; prohibition on taking part in procurement, concession proceedings, or competitive bidding; and dissolution.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

A company may be discharged from corporate criminal liability if it implemented an efficient compliance system prior to the crime having been committed. The Czech Supreme Prosecution Office has published guidelines on what factors should be taken into account when assessing whether a compliance system is effective. While these guidelines are not binding to courts (they are addressed to state prosecutors), they are useful for companies to assess their own compliance systems. The guidelines are in general consistent with best practices from other countries. If an effective compliance system is implemented only after the crime has been committed, the law does not set out an explicit discharge option. However, such implementation can be taken into account by the court as a mitigating circumstance.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

According to the Czech government plan of legislative works, the Czech Republic should implement the EU Directive on protection of whistleblowers (EU Directive no. 2019/1937 on the protection of persons who report breaches of Union law) by November 2021. No further details on the implementing act are known yet (e.g. whether its scope would be broader than the scope of the directive).

Another widely discussed topic in the Czech Republic is when a new Code of Criminal Procedure will be adopted. The current Code dates back to 1961. A draft of the new Code of Criminal Procedure produced by a committee of judges, attorneys and scholars has been published on the website of the Ministry of Justice for public comments. However, no deadline for the adoption has been announced yet.

CONTACT

Palác Myslbek
Na Příkopě 19
117 19 Prague 1
Czech Republic

Tel.: +420 221 622 111
www.kinstellar.com

Kinstellar is a leading independent law firm in Emerging Europe, Turkey and Central Asia, with offices in Almaty (Kazakhstan), Belgrade (Serbia), Bratislava (Slovakia), Bucharest (Romania), Budapest (Hungary), Istanbul (Turkey), Prague (the Czech Republic), Sofia (Bulgaria) and Kyiv (Ukraine).

Operating as a single fully integrated firm, Kinstellar delivers consistently high quality services across all jurisdictions in an integrated and seamless style. We are particularly well suited to servicing complex transactions and advisory requirements spanning several jurisdictions.

We have the leading Compliance, Risk and Sensitive Investigations and White Collar Crime Practice in Emerging Europe and Central Asia. Our strengths include a multi-jurisdictional approach, deep knowledge of the region's anti-corruption laws and culture, familiarity with regional enforcement trends and proficiency in dealing with local authorities.

We have experience in crisis management and communications, and expert knowledge in matters of legal privilege, data protection, employee privacy, document retention, security, and corporate and director liability.

Michal Kníž
Senior Associate
Kinstellar
T +420 221 622 111
michal.kníž@kinstellar.com

Michal Kníž is a senior associate in Kinstellar's Prague office. He is a member of the Corporate group and his specialisation includes compliance, risk and sensitive investigations, white collar crime defense, corporate matters and personal data protection. Michal graduated from the Faculty of Law and the Faculty of Economics of Masaryk University in Brno. During his studies, he spent one semester at the University of Bergen, Norway, and he completed an internship at the Supreme Administrative Court of the Czech Republic. Michal has advised various clients in matters relating to internal investigations (including a global pharmaceutical company) and white collar crime matters (including global IT company, international professional services firm and a major Czech insurance company).

Denmark

Kromann Reumert


Hans Jakob Folker


Tina Brogger Sorensen


Martin Dahl Pedersen

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	
No					X

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

The legal implication of whistleblowing or whistleblower reports should always be considered in connection with internal investigations, including whether any special protection should be afforded to the whistleblower. However, no specific legislation is in place in this regard. Typical questions arising out of whistleblowing concern workplace related issues, including whether laws, internal policies or confidentiality obligations have been disregarded by the involved.

Pursuant to the Danish Financial Business Act, financial institutions are prohibited from exposing employees or former employees to unfavorable treatment or adverse consequences as a result of the employee or former employee reporting the institution's breach or potential breach of the financial regulation to the Financial Supervisory Authority or to a whistleblower scheme within the company.

For entities subject to the Danish Anti-Money Laundering Act, the management and key persons are obliged to report to the senior management, without undue delay, warnings about money laundering or financing of terrorism received from i.a. whistleblowers.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) No. However, it is always advisable to check whether there exist special agreements or local practices calling for labor law considerations.

b) No.

c) There exists no general obligation in Danish law to notify authorities of internal investigations. However, the individual matter must always be assessed since there may exist special obligations to notify authorities of safety incidents or similar. These questions will depend on the industry involved. A number of industries are subject to reporting of suspicious transactions.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

This will depend on the nature of the investigation. From a criminal law perspective, participation in interviews generally is voluntary and a general principle of non-self-incrimination applies. From a labor law perspective, employees in work related matters will be obliged to support the investigation in a loyal and truthful manner. Non-cooperation may warrant disciplinary actions against the employee. The specific situation will have to be considered.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Generally, the commencement of an internal investigation will not trigger labor law deadlines. However, an employer must be careful of inaction if clear evidence of sanctionable behavior is presented. Typically, the investigation process and subsequent labor law assessment must be kept separate not to short circuit each other.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Danish data privacy laws apply with regard to processing of personal data, which includes collecting, recording, structuring, reviewing and using data. The laws also apply to the creation of work product such as interview file notes and final reports.

b) Reviewing emails?

Private communication is protected by both GDPR and the Danish Criminal Code. Pursuant to the GDPR, the employer is generally obligated to inform any data subject whose personal data are being processed on the identity and contact details of the data controller, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the recipients or categories of recipients of the personal data, etc. (please see Articles 13 and 14 of the GDPR). However, such obligation does not exist if the data subject's interest in this information is found to be overridden by essential considerations of private interests, including the consideration for the employee themself.

c) Collecting (electronic) documents and/or other information?

The data privacy laws and jurisprudence and guidelines from the Danish Data Protection Agency ("**DDPA**") should be complied with in connection with collecting documents and/or other information comprising personal data. The collection must be for a legitimate purpose and be of relevance to the case. In addition, personal data may only be stored for a limited period. Under Danish law, there is no specific time limit for which the data may be stored. Therefore, the allowed period will always depend on an assessment of whether the processing is still necessary for the legitimate purpose for which the data is stored in the specific case.

d) Analyzing accounting and/or other mere business databases?

Only documents that contain personal data are subject to the general principles of the GDPR and the DDPA.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no statutory obligation to instruct an employee before conducting an interview. However, it is advisable that the employer informs the employee of the background of the investigation. Further, it is, depending on the circumstances, recommended that the employer gives the employee the opportunity to have a representative present during the interview, e.g. the employee's lawyer, a union representative, a family member or a friend.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

It will depend on the situation and there may rest an ethical obligation on qualified lawyers to caution an interviewee of potential later implication of the statement, including with respect to self-incrimination.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

The role of external counsel should always be explained to participants in an interview carried out as part of an internal investigation.

d) Be informed that they have the right that their lawyer attends?

There is no explicit legal obligation to inform an employee about the right to counsel under Danish law. However, according to the Association of Danish Law Firms' guidance, persons affected by the investigation have, at all stages of the investigation, the right to appoint an "assessor", e.g. a lawyer, union representative, or a union member representative.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

The employee is not entitled to have an employee representative present during the interview. However, it is recommended that the employer gives the employee such an opportunity.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The employee should be informed about any potential cross-border data transfer. Under the GDPR, an additional legal basis is required when transferring personal data to non-EEA countries and such transfer is only permitted if adequate safeguards are established or an exemption applies. An adequate safeguard may be entering into the EU standard contractual clauses with the recipient of the personal data. Only in exceptional cases, the consent from the employee will be the appropriate legal basis to allow the transfer of data to countries which do not ensure an adequate level of protection (see GDPR Article 49(1)(a)).

g) Sign a data privacy waiver?

The protection granted under the GDPR and the DDPA cannot be deviated from to the detriment of the data subject. Consequently, the rights of the data subject cannot be legally waived.

h) Be informed that the information gathered might be passed on to authorities?

There is no general requirement in Danish law that an employer must inform the employee that a matter is passed on to the authorities. However, as part of litigation, it may be necessary to inform the employee of this.

i) Be informed that written notes will be taken?

This will depend on the nature of the internal investigation.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Yes. Retention notices and legal holds should be discussed early in the process. There are no specific requirements which must be observed.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Legal privilege is a procedural guarantee protected by the Danish Administration of Justice Act covering civil as well as criminal proceedings. Under Section 170 of the Danish Administration of Justice Act, defense counsels and lawyers may not be required to provide evidence about matters having come to their knowledge in the course of the exercise of their functions. The protection also extends to written advice and reports prepared by them in connection with such proceedings.

In civil proceedings, a similar protection is afforded with regard to advice received from the acting counsel provided the advice relates to legal proceedings. Generally, the privilege will apply if material covered by the privilege is clearly marked as privileged.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Legal privilege does not apply to work products and advice provided by in-house counsel to management of a company. In order for legal privilege to apply the advice must be provided by external counsel.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Any obligation to notify an insurance company of an investigation would stem from the individual insurance agreement. Where the investigation may reveal information that could form the basis of an insurance claim, the policy holder should notify the insurer.

b) To business partners (e.g. banks and creditors)?

There are no statutory duties in this regard. Notification requirements may arise from the contractual obligations between the company and its business partners, including banks.

c) To shareholders?

Internal investigations may deal with important matters that could be seen as inside information. On a case-by-case basis, the company needs to evaluate if there is a duty to notify its shareholders and the public, in accordance with the EU Market Abuse Regulation. Violation of disclosure requirements is a criminal offense (see Section 248 of the Danish Act on Capital Markets).

d) To authorities?

See above under 2. In general, there is no statutory obligation to inform the prosecutor or any other authority about an internal investigation or potential misconduct within the company.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There is no general statutory obligation to take any immediate measures, unless for safety reasons or similar. However, the company has an ordinary obligation to minimize damages and take adequate steps to prevent new ones. In this regard, ongoing criminal behavior must be stopped. The company may also have to re-evaluate its compliance system in order to eliminate potential deficits and to improve its existing system.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Danish authorities, including police and prosecution, are designed to investigate matters within their competence on their own and therefore do not depend on results from internal investigations. However, if an internal

investigation is undertaken, the involved authority typically will be interested in the results of the internal investigation.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Under Chapter 73 of the Danish Administration of Justice Act, search warrants must fulfill formal and material requirements stipulated by law. Search warrants are issued by the court. A search warrant may be issued if there is a reasonable suspicion that an offense under public prosecution has been committed and the search is of material importance to the case. The police may carry out a warrant-less search, where there is a risk that the evidence sought by the search would be lost should the police wait for a warrant.

Generally, even when the formal prerequisites for search warrants are not observed, the seized evidence may still be used against the company.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Deals, non-prosecution agreements, and deferred prosecution agreements are not available in Danish law. Nevertheless, corporations can and commonly do accept fixed penalty notices when offered by the prosecution.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Both legal and natural persons are subject to criminal liability under Danish law.

Pursuant to Chapter 5 of the Danish Criminal Code, any legal person may be subject to fines where so provided by, or pursuant to, statute. For example, Section 306 of the Danish Criminal Code states that companies and other incorporated bodies (legal persons) may incur criminal liability, under the rules of Chapter 5, for violations of the Criminal Code. Section 306 covers all offenses in the Danish Criminal Code. In addition, legal persons may be subject to disgorgement and debarment. Sanctions in relation to legal persons generally are tied to gross revenue, but it depends on the regulatory regime governing the industry in question.

The ordinary penalties for individuals are imprisonment and/or fines, but individuals may also be subject to disgorgement and debarment.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

There are no specific rules or guidelines which set out principles for determining penalties in case a company has implemented an efficient compliance system. Penalties will be determined on a case-by-case basis based on the specific circumstances, including aggravating and mitigating circumstances which must be taken into consideration when determining penalties.

However, from recent Danish case law it appears that it may have an impact on the court's decision on the penalty if companies have introduced stricter compliance procedures and guidelines for their future business after the violation has occurred.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Danish lawmakers have increased their focus combatting especially corporate criminal offenses and financial crime. Enforcement agencies have done the same. At the same time, companies experience a greater pressure in terms of e.g. cyber and fraud. All of which has resulted in a greater need for carrying out internal investigations. Internal investigations are also important as part of preparing civil litigation, in particular damage and claw-back claims following internal violation of policies and laws.

CONTACTS

KROMANN REUMERT

Sundkrogsgade 5
2100 Kopenhagen
Denmark

Tel.: +45 7012 1211
www.kromannreumert.com

Hans Jakob Folker
Partner
Kromann Reumert
T +45 61 61 30 09
hjf@kromannreumert.com

Hans Jakob Folker heads Kromann Reumert's corporate criminal law practice, focusing on financial crime, corruption and civil fraud litigation as well as internal investigations in Denmark and abroad.

He joined Kromann Reumert in 2013 after having served as deputy public prosecutor with the State Prosecutor for Serious Economic and International Crime.

As a seasoned litigator, Hans Jakob has acted as prosecutor and defense counsel in complex government investigations and proceedings. He deals with corporate criminal law matters and damage claims within all main business sectors, including anti-corruption, conflicts of interest, money laundering and financial regulation. In recent years Hans Jakob has handled a number of large international matters regarding compliance with sanctions laws.

Tina Brøgger Sørensen
Partner (CIPP/E)
Kromann Reumert
T +45 61 20 35 33
tib@kromannreumert.com

Tina Brøgger Sørensen is primarily engaged in data protection, employment and labor law. Tina is head of Kromann Reumert's Personal Data and Whistleblower Schemes practice group and is an internationally Certified Information Privacy Professional (CIPP/E). Tina became a partner in January 2011.

Tina is widely engaged in data protection, including processing of employee data, demands of permission from the Data Protection Agency, preparation of data processing agreements, international data transfers, preparation of policies, setting-up of Whistleblower Schemes, etc.

Tina has considerable experience in advising employers on employment law, discrimination issues, mergers and acquisitions, dismissals in connection with restructuring, rationalisation or closure of businesses, stock exchange listings, incentive programs, and senior management issues.

In addition, Tina has advised clients in several cases of general public importance, and has also represented a company in a discrimination case before the European Court of Justice.

Martin Dahl Pedersen
Partner
Kromann Reumert
T +45 24 86 00 17
mdp@kromannreumert.com

Martin Dahl Pedersen is part of the corporate compliance and litigation practice. He specializes in civil fraud cases and damage claims, including claw back litigation following from internal investigations. He has deep insight in advising clients in the media and entertainment industries, particularly the newspaper, publishing and sports sectors.

In addition to providing advice and negotiating agreements, Martin has also conducted cases before Danish and international courts, arbitration tribunals and commissions, including the European Court of Justice, the international Court of Arbitration for Sport (CAS), and national and international complaints boards for domain names.

Estonia

Cobalt


Jaanus Mody


Karina Paatsi


Egon Talur

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

As Estonia has not adopted any laws or regulations on whistleblowing, there are no specific procedures that need to be considered in case a whistleblower report sets off an internal investigation.

Estonia must bring into force the laws, regulations and administrative provisions necessary to comply with the directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law by 17 December 2021.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) There is no statutory obligation of informing employee representative bodies about an internal investigation.

b) The European Union's General Data Protection Regulation ("**GDPR**") or the Personal Data Protection Act ("**PDPA**") does not expressly require informing a data protection officer about an internal investigation. However, according to Article 38 (1) of the GDPR, the data controller must ensure that the data protection officer is involved in all issues relating to the protection of personal data, therefore, depending on the nature of the internal investigation and actions taken in the course of the investigation, the data controller must be aware whether there is a possible friction with the GDPR and/or the employee's privacy rights and if yes, the data protection officer should be consulted in order for the data protection officer to be able to fulfill their duties pursuant to Article 39 of the GDPR.

The need to consult with a data protection authority could arise on the basis of Article 36 of the GDPR, whereby as a result of a data protection impact assessment conducted prior to the investigation, the processing would result in high risk in the absence of specific safety measures taken by the controller.

c) Generally, no such obligation exists. However, certain exceptions may apply under specific regulations, e.g. credit institutions are required to report a money laundering or terrorist financing suspicion.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

The employees have no statutory obligation to support the investigation. One could claim that the employee's duty of loyalty to the employer involves also certain cooperation obligation in case of investigation of a possible breach in the employer's company, but no practice has developed in this matter. Therefore, it is questionable whether any legal measures could be applied to the employee who refuses to cooperate in the investigation.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

The laws of Estonia do not provide for the employer's right to sanction (or discipline) the employee. Instead, legal measures under civil law can be used (such as damage claims, termination of contract, contractual penalty claims).

According to the Employment Contracts Act, the time-limit for filing a claim for the recognition of rights arising from employment relationships and for the protection of violated rights for the purpose of recourse to a labor dispute committee or court is four months as of the time the employer became or should have become aware of the violation of employer's rights.

An employer's claim for compensation for damage against an employee for damage caused upon performance of duties expires within 12 months as of the time when the employer became or should have become aware of the damage caused and the employee obligated to compensate for it, but not later than three years after the damage was caused.

In case the employee has committed a theft, fraud or another act bringing about the loss of the employer's trust in the employee, the employer may extraordinarily terminate the employment contract only within a reasonable time after the employer became or should have become aware of the circumstance serving as the basis for the termination.

Considering the above, different labor law deadlines will mainly be triggered as of the time when the employer became or should have become aware of the circumstances serving as the basis for the claim (in the course of the investigation or by other means). There is no specific action that could be taken to avoid triggering the deadlines.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Under the GDPR, a legal basis and a lawful purpose is required for each data processing activity. Therefore, the employer must identify and determine a legal basis for conducting the interviews. Therefore, conducting an interview (and presumably retaining information from that interview) must be considered by the employer as a form of personal data processing, and the employer must comply with the requirements of the GDPR, e.g. having the legal basis in place, ensuring the security of the data, etc. The employee as the data subject must be presented the necessary information, as required under Article 13 of the GDPR, prior to the interview.

b) Reviewing emails?

The revision of the contents of work-emails is allowed as work-related emails are not protected based on the applicable data protection legislation. However, as a rule, the employer is not entitled to access personal

emails. The employer is under an obligation to presume, unless there are internal rules in place (which have been duly made available and introduced to the employee) which prohibits such use, that the employee uses the employer's devices and email address for personal purposes as well.

In case private use was prohibited, the employer is entitled to browse through the documentation, including emails, as it presumably contains no private documentation. However, key-word specific searches should be preferred. In case private documentation is still found, the documentation should be returned to the employee and in case of emails, such emails should remain unopened and the employee notified.

In case private use was not prohibited, then it should be firstly inquired whether the employee was under an obligation to specifically mark or designate its private documentation and emails in any manner, which would give the employer an overview where the private documentation and emails are located. For example, in case there is a folder titled "Personal" then such folder should be left untouched. In case no internal rules regulate this issue, then the employer must presume that the mailbox contains a mixture of personal and work-related emails, and the employer's possibilities to access the mailbox are limited. For example, it may be justified in case the employer accesses the mailbox for specific searches only – choosing specific dates combined with specific keywords (e.g. addressees, topics, clients) for the searches of specific non-personal correspondence. No general browsing is allowed. However, in case private documentation is still found as a result of a specific search, then the documentation should be returned to the employee and in case of emails, such emails should remain unopened and the employee notified.

In case there are reasonable suspicions that the employee has breached some material obligation (e.g. non-competition obligations or confidentiality obligations) deriving from their employment/service agreement, then the employer is entitled to search the mailbox in the limits of that suspicion, regardless of whether there are any internal rules in place. However, the Estonian Data Protection Inspectorate has taken the position that in the aforementioned cases the mailbox (or suspicious emails) should be reviewed together with the employee, as thereby the employee can provide necessary explanations and is more aware of their personal data processing. Additionally, specific key-word searches are advised, as there is a possibility for a breach of private life.

In case there is a risk of processing personal data, the requirements of the GDPR must always be followed.

c) Collecting (electronic) documents and/or other information?

The same rules as described in our answer to section 5b above must be taken into account for this section.

d) Analyzing accounting and/or other mere business databases?

Non-personal data, e.g. accounting information is not protected. However, in case the employer would like to outsource the investigation function, it is recommended that relevant confidentiality agreements are put into place with the third-party service provider to protect the employer's own business critical data.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no statutory obligation of giving the employee any written instructions.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no statutory obligation of informing the employee that they must not make statements that would mean any kind on self-incriminations.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no statutory obligation of informing the employee that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee.

d) Be informed that they have the right that their lawyer attends?

There is no statutory obligation of informing the employee that they have the right that their lawyer attends.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is no statutory obligation of informing the employee that they have the right of a representative to attend.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

According to Article 13(1)(f), the employer must inform the data subject of any transfers to third countries, meaning, to countries outside of the EU/EEA. For such transfers, the employer must adhere to the requirements stated in Chapter V of the GDPR.

g) Sign a data privacy waiver?

The European Union's privacy legislation does not make it possible to waive any privacy rights to the detriment of the data subject, meaning, the employee. The data subject is always entitled to exercise its rights stipulated in the GDPR, insofar as those rights have not been limited by the GDPR or by the national laws of the member states in compliance with the GDPR and/or in compliance with the fundamental rights or other legal acts in case falling outside of the regulatory scope of the GDPR.

The employer has to communicate to the employee information required in Article 13 of the GDPR. It is recommended that this information is provided in writing and the employee confirms in writing that such information has been provided to them.

h) Be informed that the information gathered might be passed on to authorities?

According to Article 13(1)(e) of the GDPR, the employer has to make the employee aware of the recipients to which the data is disclosed. This means that, in case the information might also be disclosed to the authorities, the employee has to be made aware.

i) Be informed that written notes will be taken?

There is no statutory obligation of informing the employee that written notes will be taken, nor is there an obligation to provide the employee with a copy of notes from an internal interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific regulation regarding the matter. However, an obligation to preserve documents and evidence may derive from general principles of law, including contract law. E.g., elimination of documents may be unlawful and entail civil claims. Moreover, the elimination of evidence is a criminal act punishable with a pecuniary punishment of €4,000 - €16,000,000 for a legal person. A natural person can be punished with a pecuniary punishment or imprisonment from one to five years.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Assuming that the internal investigation was conducted by attorney, if it reveals that the client has committed a crime, the communication between the client and the attorney and the information found in the internal investigation report will be protected by the attorney-client privilege. However, if the investigation reveals that the client wishes to commit a first-degree (see section 10d) crime, the lawyer may request the court to terminate the attorney-client privilege protection and take the necessary steps to prevent the crime. The lawyer is also obliged to terminate the client relationship in this case. Attorney-client privilege also does not apply to suspicions of money laundering or terrorist financing. In all other cases, the lawyer shall be required to maintain the confidentiality of the information which has become known to them during client relationship, unless the client waives this obligation in writing.

In no case should a lawyer assist a client in committing a crime or misleading the court system, e.g. by knowingly submitting incorrect information.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Attorney-client privilege does not apply to in-house counsel. The parties have the power to make the necessary adjustments to the employment contract so that the employer would be protected as much as possible, however, the legal protection provided by law does not extend to in-house counsel.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

It depends on the substance of the investigation and applicable terms and conditions of the insurance contract. Generally, no early notifications are required to report an investigation. However, there is an obligation to notify the insurer of an increase in the probability of the insured risk, unless the increase is caused by circumstances which are common knowledge and which does not affect the insured risk of the policyholder alone. Nevertheless, it is required to immediately notify the insurer of the occurrence of an insured event.

b) To business partners (e.g. banks and creditors)?

There is no general mandatory requirement. However, there may be specific situations when a notice is required by contract law, e.g. in cases when starting an investigation entails a risk of non-performance of an agreement with the business partner. In other cases, the terms and conditions of the agreement shall determine a possible obligation to notify.

c) To shareholders?

There is no automatic obligation to inform the shareholders unless otherwise is provided by the articles of association or shareholders' agreement. Nevertheless, shareholder of a public limited company may request information on the activities of the company to be given at a general meeting. The company may refuse to disclose such information if there are grounds to assume that this might significantly damage the interests of the company. Shareholders of a private limited company may request information on the activities of the company to be given at all times, i.e. it is not restricted only to general meetings. Moreover, shareholder of a private limited company may also request to examine documents. The company may refuse the request for disclosure if there are grounds to assume that it might significantly damage the interests of the company.

d) To authorities?

In general, there is no obligation to inform the authorities of conducting an internal investigation *per se*. However, in specific situations, the substance of the investigation might be required to be disclosed. E.g., if the substance of the internal investigation is a criminal offense in the first degree, then the company's failure to report the crime can be punishable by a pecuniary punishment of €4,000 - €16,000,000. Natural persons may also be imprisoned of up to three years. A criminal offense in the first degree is an offense for which the maximum punishment prescribed for a natural person is imprisonment for a term of more than five years or life imprisonment.

In addition to the above, credit institutions are also required to report a suspicion of money laundering or terrorist financing, should this be the substance of the internal investigation.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There is no such practice in Estonia. Often an explanatory press release is issued, and the employment relationship may be terminated with the person responsible for a breach that is being investigated to improve the company's reputation.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

No, if criminal proceedings are not initiated. Usually the Prosecutors' Office is not aware of internal investigations. Therefore, they are not able to have any specific concerns or request any specific steps to be observed. However, a prosecutor may get involved and issue requests in the course of criminal proceedings.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

In criminal proceedings, the objective of a search is to find an object to be confiscated or used as physical evidence, a document, thing or person necessary for resolving the criminal matter, assets to be seized in criminal proceedings, or a body, or to apprehend a fugitive in a building, room, vehicle or enclosed area. A search may be conducted if there is a reasonable suspicion that the object to be found is at the place of the search. A search may be conducted at the request of the Prosecutor's Office based on an order of a preliminary investigation judge or based on a court order. In urgent matters, the search may also be conducted by a preliminary order of the prosecution, but not in law firm or notary's office.

A search warrant shall set out what is being searched for as the objective of the search, the reasons for the search and the place where the search is conducted. If a search is conducted, the search warrant shall be presented for examination to the person whose premises are to be searched. The search report shall be signed to confirm that explanations of the circumstances were provided. In the course of a search, all objects may be taken away which are subject to confiscation or are evidently the evidence in the criminal proceedings if they were discovered without any search in a clearly visible place or in the course of reasonable search undertaken to find the objects to be found.

The court has the right to refuse evidence if it was collected in breach of the applicable rules of criminal procedure.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Non-prosecution or deferred prosecution agreements are not available. However, deals are still available and common. Generally, a settlement procedure can often be applied in criminal proceedings. The outcome of the settlement is that the person is declared guilty and punished, but on agreed terms and conditions. There is also an option for the prosecutor to terminate the criminal proceedings in case of lack of public interest in proceedings and negligible guilt. If the object of criminal proceedings is a criminal offense in the second degree and the guilt of the person suspected or accused of the offense is negligible, and they have remedied or have commenced to remedy the damage caused by the criminal offense or have paid the expenses relating to criminal proceedings, or assumed the obligation to pay such expenses, and there is no public interest in the continuation of the proceedings, the Prosecutor's Office may request, with the consent of the suspect or accused, that the court terminate the proceedings. Usually it is agreed that both the costs of the proceedings and the compensation for the damage caused by the crime are to be paid.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

A company's directors, officers or employees are not punished due to the misconduct of another individual in the company unless they are personally involved in the misconduct. The punishment depends on the type of misconduct. However, a company can be punished with a pecuniary punishment of €4,000 – €16,000,000 for the criminal acts committed by its director, officer or a managing employee, if the crime was committed for the benefit of the company.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

The liability of companies, their directors, officers, or employees may be excluded, or the penalties may be reduced for them in case the company or its representatives have implemented an efficient compliance system (i.e. have taken reasonable measures to avoid offenses from occurring). The foregoing applies only in case the efficient compliance system had already been implemented prior to the alleged misconduct.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The Estonian Supreme Court has asked the European Court of Justice for a preliminary ruling on the permissibility and legality of the use of people's data (e.g. communications data, video surveillance data, biometric data) in criminal cases. There are concerns about the proportionality of personal electronic communications data used in proceedings related to minor crimes. Currently it is being publicly discussed when court hearings should be public and when held privately and recorded on camera. It may be necessary to impose certain restrictions that protect business secrets, for instance, but some decisions are made too arbitrarily without enough argumentation.

CONTACTS

Kawe Plaza, Pärnu mnt 15
Tallinn 10141
Estonia

Tel.: +372 665 1888
tallinn@cobalt.legal

COBALT is one of the largest full service business law firms in Estonia that belongs to COBALT alliance covering 4 jurisdictions - Estonia, Latvia, Lithuania and Belarus – uniting approximately 200 lawyers.

COBALT is awarded with:

- The Most Innovative Baltic Law Firm of the Year 2019 Award by IFLR
- The Baltic Law Firm of the Year 2019 Award by The Lawyer
- CEE Legal Matters Deal of the Year Award for Estonia, Latvia, and Lithuania, as well as the overall Baltic Deal

Jaanus Mody

Managing Partner
COBALT
T +372 665 1888
jaanus.mody@cobalt.legal

Jaanus Mody is the Managing Partner of COBALT Estonia and the head of the Dispute Resolution and Restructuring & Insolvency practice group since 2001.

He has represented and advised clients in many high-profile and complex cases that have attracted wide public interest.

As a widely recognized insolvency expert with a legal practice of over 20 years, Jaanus has advised the market's most successful restructuring and recovery plans.

He has also a strong track record in different complex disputes.

Karina Paatsi

Partner
COBALT
T +372 665 1888
karina.paatsi@cobalt.legal

Karina Paatsi is a Partner of COBALT Estonia and head of the Corporate and Employment practice group.

She possesses wide-ranging expertise in matters concerning the legal regulations specifying the employer-employee relationship and disputes thereof.

She also provides legal advice in daily corporate governance and contract law matters, corporate restructurings and all aspects related to commencement of business.

Egon Talur

Partner
COBALT
T +372 665 1888
egon.talur@cobalt.legal

Egon Talur is a Partner of COBALT Estonia and head of the Tax and IP/IT and Data Protection practice groups.

Egon has vast experience in IP assets' restructurings, and he has been advising clients in designing and implementing tax efficient business structures for IP rights management.

In addition, Egon has considerable experience in corporate taxation, including M&A transactions, restructuring and reorganising corporate and business structures, as well as solving clients' day-to-day tax matters.

Finland

Borenius Attorneys Ltd

Markus Kokko

Jani Syrjänen

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X Criminal corporate fines possible in case an offense has been committed in the operations of the company.	X	X	X	
No					X

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

In Finland, there is no comprehensive whistleblower protection legislation. Some limited industry-specific regulations have been adopted, e.g. in the financial sector, where the Financial Supervisory Authority maintains a system for receiving reports of any suspected infringements of financial market provisions. The Financial Supervisory Authority protects the personal information and identity of the whistleblower.

On a more general level, the Finnish Employment Contracts Act (55/2001, as amended) and other employment laws provide some measure of protection to whistleblowers by requiring an employer to have a substantial reason for dismissing an employee and to first provide a warning prior to dismissal. In other words, the employer would need to demonstrate that the employee seriously breached or neglected their obligations by filing a whistleblower report. Dismissal may also be justified if the employee disclosed information with the clear intention to damage the employer. However, if the employee had a duty to report the information to the authorities, dismissal is unlawful.

Generally, the employee should disclose information internally before reporting to the authorities or going public, unless there is a clear legal duty to report directly to the authorities. The employer has no duty to investigate the whistleblower report. However, should the authorities investigate the matter and find that the employer has been aware of the state of affairs; this would likely constitute an aggravating circumstance.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) There are no specific regulations that grant employee representative bodies the right to be informed about, or to participate in the investigation process. However, under the Finnish Act on Cooperation within Undertakings (334/2007, as amended, "**Act on Cooperation**"), companies that regularly employ 20 or more employees must negotiate policies and processes for collecting employee personal data with the employees or their representatives. Some collective agreements may include more specific obligations and, therefore, should be consulted before beginning an investigation. Non-compliance with the Act on Cooperation may be sanctioned with a fine.

b) A Data Protection Ombudsman ("**DPO**") has the right to access any personal data being processed, as well as any information necessary to supervise the processing and assess its legality. Under the Finnish Data Protection Act (1050/2018) that is based on the European data protection regulation (EU) 2016/679 ("**GDPR**"), the DPO is charged with advising employees on their data privacy rights and monitoring data protection. Consequently, the company is required to, on the DPO's request, report to the DPO any data privacy-related procedures and processes that are part of an investigation.

c) There is no obligation to inform the prosecution authorities before starting an internal investigation. However, voluntary involvement of the authorities can be beneficial depending on the circumstances of the specific case.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees have a general duty of loyalty toward their employer. The scope of this duty depends on the employee's position in the company. For example, supervisors owe a greater duty to the employer than employees in non-supervisory positions. Ultimately, the employer has a general right to direct and supervise its employees and can, therefore, require them to participate in an internal investigation.

An employee's refusal to participate can, in some cases, be deemed misconduct and justify a warning or even dismissal, if the employee has previously received a warning for the same or similar misconduct.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

According to the Employment Contracts Act, if an employee's misconduct leads to a warning or dismissal, these measures should be initiated within a reasonable period after the relevant facts have become known. The reasonable period of time is evaluated on a case-by-case basis depending on the circumstances.

The employer may only with substantial cause cancel an employment contract with immediate effect. However, the right to cancellation lapses if the employment contract is not cancelled within 14 days of the date on which the employer was informed of the existence of the grounds for cancellation.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Data privacy regulations apply to the processing of all personal data. That includes personal information obtained from interviews. Therefore, it is essential to assess which data protection laws may or may not apply and to document the measures taken before conducting interviews.

b) Reviewing emails?

Pursuant to the Finnish Act on Protection of Privacy in Working Life (759/2004, as amended), the employer can only process personal data that is directly necessary for employment. This is a mandatory legal provision that may not be waived by the employee. Under the Act, an employee's work-related emails can only be viewed if detailed provisions are observed. If these requirements are not met, reviewing employees' emails can constitute a criminal offense.

By contrast, employers are not permitted to review employees' personal emails. Personal correspondence may only be reviewed by authorities in connection with a criminal investigation. Therefore, careful assessment of possible legal risks should always be carried out before reviewing emails.

c) Collecting (electronic) documents and/or other information?

Finland has no blocking statute regime. Finnish data protection statutes are based on the GDPR, which has been implemented in Finnish legislation by the Finnish Data Protection Act.

Pursuant to these statutes, the processing of personal data must be appropriate and justified. This means that, before the employer can process any personal data, the purpose of the processing, the data sources, and the data recipients must be determined. Processing or using personal data in a manner incompatible with the specified purpose (e.g. processing irrelevant data) is prohibited. At the employee's request, the employer must inform the employee of any personal data collected. As noted above, the employer can only process personal data that is directly necessary for employment. Processing of other personal data can only occur in connection with investigations by the authorities.

d) Analyzing accounting and/or other mere business databases?

Data privacy laws do not apply to analyzing accounting and other mere business databases.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

In Finland, there is no statutory obligation to give written instructions to the interviewee, but it is advisable to do so. Generally, the instructions would include a brief explanation of the background and focus of the investigation. It is advisable to provide these instructions in writing and ask the interviewee to sign them.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

With regard to internal investigations, there is no right to remain silent to avoid self-incrimination, as is the case during criminal interrogations. Nevertheless, it is advisable not to pressure interviewees to incriminate themselves, especially if the interviewee is also subject to a criminal investigation.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

An Upjohn warning is only mandatory if there are links to U.S. law. However, in general, it is advisable to avoid behaviors that could mislead the employee into thinking that the company's lawyer represents them.

d) Be informed that they have the right that their lawyer attends?

In Finland, employers are free to handle internal matters independently without the involvement of outside lawyers. However, should the employer seek to terminate the employee or cancel the employment contract, the employee has the right to be heard in the matter. Under such circumstances, the employee has the right to have a lawyer and should be informed of this right.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

In Finland, there is no statutory obligation to inform the employee of the right to have an employee representative present during an interview, even though such right usually exists. However, the specific rights of an employee and corresponding obligations of an employer might vary depending on the applicable collective agreement.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Pursuant to the GDPR and the Finnish Data Protection Act, the subject of the data must always be informed of the identity of the controller as well as of the purposes of the gathered personal data.

The employee should be informed of any potential cross-border transfers of personal data. Under Finnish data privacy legislation, the transfer of data to non-EU states is only permitted if an adequate level of data protection is guaranteed in the recipient country. All transfers of personal data to third countries or international organizations must be performed in accordance with Chapter V of the GDPR.

g) Sign a data privacy waiver?

Under the Finnish Data Protection Act, an employee's consent is needed, as far as personal data is concerned and as far as no legal exceptions apply. A data privacy waiver is particularly advantageous if the personal data of the interviewee may be used in future legal proceedings.

h) Be informed that the information gathered might be passed on to authorities?

It is highly advisable to inform the employee that information gathered may be passed on to authorities. This is particularly true if information may be passed on to U.S. authorities.

i) Be informed that written notes will be taken?

There is no legal obligation under Finnish law to inform the interviewee that written notes will be taken, but it is advisable to do so. It is also advisable that the documentation of the interview (e.g. for reports and potential court proceedings) be shown to the employee for approval. There is, however, no statutory obligation to provide the employee with physical copies of notes from an internal interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

In Finland, there are no document hold notices or document-retention notices. However, as previously mentioned, the employer has the right to direct and supervise its employees and, based on this right, can instruct them to preserve relevant documents and records. An objection to the employer's instruction can constitute misconduct.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Findings of internal investigations are generally not protected by attorney-client privilege, which is not absolute in Finland. To ensure privilege, it is advisable to consult outside counsel. In principle, documents in the possession of outside counsel are protected. Documents and communications from outside counsel to in-house counsel in the possession of in-house counsel are not automatically protected. Whether such documents and communications are protected depends, in part, on when they were provided by the outside counsel. For example, documents and communications containing general advice provided prior to any investigation by the authorities, have a smaller chance of enjoying protection than documents and communications given by outside counsel during a trial or a criminal investigation. It is advisable to clearly label correspondence and documents between in-house and outside counsel as being under the scope of attorney-client privilege. Ultimately, however, the courts will rule on what is admissible as evidence.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Generally, communication with in-house counsel and documents created by inside counsel are not privileged under Finnish law.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There is no statutory duty. However, if there is a risk that the circumstances at hand could give rise to a claim, the policyholder should notify the insurer of these circumstances.

b) To business partners (e.g. banks and creditors)?

The decision to notify business partners must be determined on a case-by-case basis. For instance, a contractual obligation may provide that such information must be disclosed to the business partner. However, even absent such a contractual provision, a company may still owe a general duty of loyalty to its business partners.

c) To shareholders?

Insider information that could influence stock prices must be disclosed to shareholders of publicly listed companies. A company may be liable for damages for breach of its reporting duties, in accordance with Chapter 16 of the Finnish Securities Market Act (746/2012, as amended).

d) To authorities?

In general, there is no obligation to inform the authorities of an internal investigation or potential misconduct within a company. However, voluntary cooperation with the authorities can prevent harmful or unexpected measures by the local prosecutor or other authorities. The benefits of such cooperation must, therefore, be considered.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

According to general tort law principles, the company must minimize damages and try to prevent further damages. The company can, for example, impose sanctions, such as warnings, on the concerned employees to deter from future misconduct. Additionally, the company should conduct an assessment of its compliance systems to eliminate potential deficits and, if necessary, make improvements. In any case, ongoing criminal conduct in the company should be stopped immediately.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

As previously mentioned, depending on the nature of the investigation, early engagement with the local prosecutors can help ensure satisfactory cooperation and prevent unwanted measures. It is of paramount importance that the company does not destroy or otherwise remove any potential evidence or give the local prosecutors reason to fear that such conduct could occur.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

According to the Finnish Criminal Investigation Act (805/2011, as amended), a search warrant must be issued by an official with the power to arrest, i.e.certain police officers. A search warrant may be issued if there is reason to believe that the search will reveal objects or information relevant to the investigation of an offense. The general principles of proportionality, minimum intervention, and sensitivity apply.

It is worth noting that even if these legal prerequisites are not met, the evidence can usually still be used in court proceedings, unless the use of such evidence would jeopardize a fair trial. This assessment must take into account, among other factors, the nature of the matter, the severity of the infringement relating to the obtaining of evidence, and the reliability and significance of the evidence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

While plea bargaining is available for individuals under some circumstances, it is not an option for corporations under Finnish law. Deals are also not available for corporations. However, cooperation with authorities might, in some cases, be taken into account as a mitigating circumstance in sentencing.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Corporations can be fined up to €850,000 for certain criminal offenses, such as bribery. Individuals can face sanctions, such as imprisonment, fines, or business prohibition. In some cases, e.g. failure to adequately supervise, a manager or director may be liable for the misconduct of other employees.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Yes, an efficient compliance system may reduce or even suspend penalties. The existence of an efficient compliance system may be considered an indication of no misconduct. In addition, the amount of a corporate fine shall be determined based on, amongst other things, the nature and extent of the misconduct. When evaluating the significance of the misconduct, for example, the nature and seriousness of the offense and whether the misconduct manifests carelessness as to the law or authorities shall be taken into account. If the company had implemented an efficient compliance system, the misconduct could be considered less serious.

Generally, an efficient compliance system would only suspend or reduce penalties if it was implemented before the alleged misconduct.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

As there is no comprehensive legislation in Finland providing whistleblower processes or governing internal investigations, the practices are somewhat inconsistent. In recent years, several authorities and NGOs have taken up this issue. Consequently, some industry-specific tools were introduced. For example, the Finnish Financial Supervisory Authority (*Finanssivalvonta*) has established a whistleblower tool, effective since 1 January 2016. Whistleblowers can now report violations of supervisory provisions. Moreover, on 17 June 2016, Finland's Ministry of Justice published a report (25/2016) recommending the establishment of an anonymous online whistleblowing tool to report suspected corruption. Whistleblower legislation in Finland is expected to evolve substantially in the near future.

On 23 October 2019, the EU enacted Directive 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with the Directive by 17 December 2021.

CONTACTS

BORENIUS

Eteläesplanadi 2	Tel.: +358 20 713 33
00130 Helsinki	Fax: +358 20 713 3499
Finland	www.borenius.com

Borenius Attorneys Ltd is one of the largest leading law firms in Finland. Borenius has been providing high quality services in all areas of law since 1911. Borenius employs over 100 lawyers at offices based in Helsinki, Tampere, St. Petersburg, New York, and London and is ranked as a top tier firm by all leading legal directories.

Markus Kokko

Partner
Borenius Attorneys Ltd
T +358 20 713 3482
markus.kokko@borenius.com

Markus regularly advises major domestic and international clients on dispute resolution and corporate crime cases.

Markus has in-depth experience of domestic and international corporate and commercial disputes and he has acted as lead counsel in numerous extensive cases. His field of experience encompasses cases related to a wide variety of business sectors, such as the chemicals industry, financial markets, international trade, retail and wholesale, mining, services and consultancy. Markus also has an exceptional track record in handling a broad range of litigation and arbitration cases, including *ad hoc* proceedings as well as proceedings governed by ICC Rules, SCC Rules and the Arbitration Rules of the Finland Chamber of Commerce.

In addition, Markus frequently advises companies and executives in relation to complex corporate crime cases and criminal investigations regarding, *inter alia*, insider trading, environmental violations, corruption, imports and exports and tax.

Markus' efficient and client oriented approach has earned him an excellent reputation which has been recognised by rankings in Chambers Global, Chambers Europe, Legal 500 and Best Lawyers. Furthermore, Markus also serves as an arbitrator and he has written many articles on litigation and arbitration.

Markus heads the Litigation & Arbitration and Corporate Crime teams at Borenius.

Jani Syrjänen

Partner
Borenius Attorneys Ltd
T +358 20 713 3565
jani.syrjanen@borenius.com

Jani advises international and domestic clients in all employment law and pension & benefits related questions including also occupational safety, discrimination and immigration matters. Jani has extensive experience in litigating employment law matters; negotiating and drafting top management agreements, company policies and procedures; as well as advising employers confronting a wide range of employment law issues including, *inter alia*, outsourcing, reorganizations and redundancies.

He is also an accredited mediator of the Finnish Bar Association and a frequent speaker about employment law issues at domestic and foreign seminars.

Jani heads the Employment team at Borenius.

France

Hogan Lovells (Paris) LLP


Arthur Dethomas


Christelle Coslin


Marie Voutsas

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	
No					X

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Under statute No. 2016-1691 of 9 December 2016 (the "**Sapin II Law**"), companies with at least 50 employees must implement a whistleblowing policy. The Sapin II Law defines the whistleblower as a natural person who reveals, in good faith, an offense, a violation of international commitments ratified by France, or a serious threat or injury to public (general) interests. A whistleblower alert must be first brought to the attention of the whistleblower's employer. If the alert is not addressed within a reasonable time, the whistleblower may refer it to judicial, administrative, or professional authorities. If the latter fail to address the alert within three months, the whistleblower may go public. In cases of serious or imminent danger, or when there is a risk of irreversible damage, the whistleblower may go directly to the authorities or the public.

The identity of the whistleblower and any individuals targeted in the alert are to remain confidential and may not be disclosed to anyone, except to judicial authorities. Any unauthorized disclosure is punishable by up to two years of imprisonment and a €30,000 fine for natural persons (€150,000 fine for legal entities).

A whistleblower, whose alert is filed in accordance with the procedures set out above, is protected both under employment and criminal law. The whistleblower, as defined in the Sapin II Law, may not be retaliated against by their employer and may not be held criminally liable for the disclosure of secrets protected by law, if the procedures were followed and the disclosure was necessary and proportionate to protect the interests at stake.

The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés,* "**CNIL**"), an independent administrative body entrusted with ensuring that data processing does not violate fundamental rights, has set out mandatory rules to be complied with when a whistleblowing report is filed in accordance with the Sapin II Law. The CNIL's guidelines of 18 July 2019 define, *inter alia*, the categories of data that can be collected in connection with a report, the confidentiality measures to be implemented and the retention periods applicable to the collected data.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) The French Labor Code requires, *inter alia*, informing and consulting employee representative bodies, where they are in place, before implementing employee monitoring tools and techniques. Thus, such bodies must be informed and consulted whenever the internal investigation process uses such monitoring tools and techniques. Non-compliance may result in a criminal fine of up to €7,500 for hindrance of the rights of the employee representatives. Evidence collected without adequate consultation of representative bodies might not be invoked against the employees.

b) Under the GDPR and French law, there is no legal obligation to declare data processing or request an authorisation from the CNIL. It is however now required to draft a Data Protection Impact Assessment ("**DPIA**") and to record the corresponding data processing into the records of processing activities of the company.

c) Under French law, there is no legal obligation for an employer to report its decision to conduct an internal investigation or its findings to judicial authorities, including prosecution authorities, unless the investigation uncovers conduct that could qualify as a crime (i.e. offenses punishable by at least 10 years' imprisonment).

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees are not legally required to support an internal investigation. Due to stringent French labor law requirements, it may be difficult to sanction an employee for refusing to cooperate. However, the silence or the refusal of an employee to participate in an investigation could be construed negatively in the event of subsequent litigation.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Disciplinary sanctions must be imposed on an employee within two months of the employer becoming aware of the employee's wrongdoing, unless it has given rise to criminal proceedings within the same period of time. After this two-month period, no sanctions can be taken for the concerned wrongdoing. If the employer conducts a fact-finding investigation, the two-month deadline starts running on the day on which the findings are issued.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Data protection

Provisions of the GDPR, the updated French Data Protection Act, its implementing decree and the CNIL's guidelines have to be taken into account when implementing a whistleblowing system and when conducting investigations. Failure to comply is punishable by administrative sanctions of up to €20,000,000 and 4 percent of the total worldwide annual turnover, and criminal sanctions of up to €300,000 fine and five years' imprisonment for natural persons (€1,500,000 maximum fine for legal entities).

b) **Secret State Law**

French banking law provides that employees working in the financial sector are bound by professional secrecy. Consequently, credit institutions cannot share information covered by banking secrecy absent a court order (this covers information including, but not limited to, names, account numbers and transactions). Violation of banking laws is punishable by up to one years' imprisonment and a €15,000 fine for natural persons (€75,000 for legal entities).

Since 2009 the communication of national defense secrets is punishable by five to seven years' imprisonment and a fine of up to €75,000 or €100,000 for natural persons, depending on how the discloser learned of the defense secrets (e.g. in the course of their work). The fine may reach €375,000 or €500,000 for legal entities. Negligent or reckless receipt of national defense secrets is punishable by three years' imprisonment and a fine of up to €45,000 for natural persons.

c) Blocking Statute

The French Blocking Statute punishes anyone who tries to obtain or transfer documents or information for use in foreign judicial or administrative proceedings. Its broad scope covers any information or documents of an economic, commercial, industrial, financial, or technical nature. This broad scope may be interpreted as including information gathered in the course of interviews for use in foreign judicial or administrative proceedings. Breach of the Blocking Statute is punishable by six months' imprisonment and a fine of up to €18,000 (€90,000 for legal entities).

The Blocking Statute provides a legal defense to parties facing discovery requests abroad. However, it has rarely been enforced by French courts since its adoption in 1968. Foreign jurisdictions, thus, tend to disregard the Blocking Statute as a valid defense against discovery requests. The U.S. Supreme Court notably dismissed this defense in the *Aérospatiale* Case.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no legal obligation to give written instructions to an interviewee beforehand, unless an internal procedure provides otherwise. Yet, it is advisable at the outset of the interview to explain the general subject matter of the investigation, thank the interviewee for participating, and ask the interviewee to treat the interview as confidential. In practice, this information is generally provided in writing and the interviewee is asked to sign an acknowledgment of receipt. Written instructions, if provided, should be in French. The employee may be invited formally although there are no legal requirements providing so. At this occasion, the employee may be granted the possibility to be assisted during such interviews.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no legal obligation to inform the interviewee of their right against self-incrimination. It is advisable to frame the interview as a discussion, rather than an examination. Accordingly, the interviewer should not subject the interviewee to any type of pressure during the interview.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

In September 2016 the Paris Bar Council published a Vade mecum for lawyers conducting internal investigations, advising them to inform interviewees that their exchanges are not covered by attorney-client privilege, as they represent the company and not the interviewee (see Article 2.2).

d) Be informed that they have the right that their lawyer attends?

No binding rules govern an interviewee's right to legal assistance in connection with internal investigations. However, the Paris Bar Council recommends informing interviewees that they can be assisted by an attorney when they are under serious suspicion of misconduct.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Although employees have the right to be assisted by an employee counsellor during a meeting prior to dismissal (*entretien préalable*), the French Labor Code does not provide for such assistance during interviews conducted in connection with an internal investigation. The French Supreme Court ruled that an employer remains free to refuse assistance to the employee in this context. However, it is not unusual to allow attendance of an employee counsellor.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Under Article 13 of the GDPR, there is a legal obligation to inform interviewees of any transfers of personal data outside the European Union. In addition, the implementing decree (Article 148) of the updated French Data Protection Act states that the interviewee must be provided with the following information: country/ies of data recipients, categories of transferred data, purpose of the transfer, categories of data recipients, and the appropriate safeguards adopted to ensure the protection of the transferred personal data.

g) Sign a data privacy waiver?

It is not possible for data subjects to sign a data privacy waiver.

h) Be informed that the information gathered might be passed on to authorities?

There is no legal obligation requiring a company to disclose the findings of an internal investigation to judicial authorities and, accordingly, there is no obligation to inform the interviewee of this possibility. This being said, it is common practice to inform the interviewee of such possibility where relevant.

i) Be informed that written notes will be taken?

There is no legal obligation to inform interviewees that written notes will be taken. However, it is a best practice to allow the interviewee to read a transcript of their statements after the interview, so their statements can be used. It is not advisable to give the interviewee minutes of the interview in order to preserve confidentiality.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Document preservation notices are admissible, but this practice is not common yet. No specific legal provisions govern the issuance of legal holds. They shall, however, be written in French and comply with mandatory retention periods imposed by the Data Protection Act.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

French professional secrecy applies to communications between outside counsel and clients in all matters, whether advisory or litigation related. Lawyers cannot waive privilege.

Judicial authorities have the possibility to issue a production order or perform a dawn raid to gather evidence, including the findings of an internal investigation. However, they cannot seize documents covered by professional secrecy. Having outside counsel conduct the internal investigation can ensure that its findings are protected by privilege.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

There is no attorney-client privilege for in-house counsel in France. They are considered as a distinct profession and do not benefit from the same status as members of the Bar.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There is no legal obligation to notify insurance companies of the launch of an internal investigation. Such notification could even be detrimental to the investigation and jeopardize confidentiality. However, it is advisable to check whether applicable insurance policies contractually require disclosure.

b) To business partners (e.g. banks and creditors)?

There is no legal obligation to notify business partners of the launch of an internal investigation. Such notification could even be detrimental to the investigation. However, it should be confirmed that disclosure is not contractually required.

c) To shareholders?

There is no legal obligation to inform shareholders of the launch of an internal investigation *per se*. However, in case an investigation's findings may be characterized as inside information, publicly listed companies must disclose this information (unless an exception allows a delay of disclosure). A duty to disclose the findings of an internal investigation may also be inferred from shareholders' general right to information. Company bylaws or shareholders' agreements may provide enhanced information rights about internal investigations and their findings.

d) To authorities?

There is no legal obligation to disclose the start of an internal investigation to authorities. However, auditors are legally required to reveal to the prosecutor any criminal offense they become aware of when performing their duties.

As an exception to attorney-client privilege, lawyers are bound by a similar obligation to disclose suspicious transactions regarding money laundering or terrorist financing when acting in an advisory capacity (e.g. advising on the sale or purchase of real estate), rather than as litigators. Generally speaking, a lawyer is considered to be acting as a litigator when they are representing the client in judicial proceedings. In all cases, if the lawyer is acting as a litigator, attorney-client privilege will not be waived.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There is no legal obligation *per se* to take immediate measures once an investigation is started in France. However, failing to do so in the presence of a potential offense renders the company susceptible to later being held liable as an accomplice or for other offenses. In parallel, companies launching internal investigations should be particularly cautious when considering employee sanctions due to very stringent labor law requirements.

Internal investigations and their findings may also be disclosed to authorities in a cooperation effort. Such cooperation effort may be taken into account should the company later face prosecution or sentencing or in order to reach a settlement with the prosecutor, in particular to enter into a Judicial Convention of Public Interest (*Convention Judiciaire d'Intérêt Public* or "**CJIP**"), which is a French type of deferred prosecution agreement.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Internal investigations are not completely part of the French legal culture yet, even if they become more and more common. Traditionally, prosecutors did not have specific concerns and did not expect the company to take specific steps. This has significantly changed with the creation of the CJIP. It is highly advisable that a company which is willing to enter into a CJIP with the prosecutor participates in the determination of the truth and shows good faith. Conducting an internal investigation may be part of this cooperation effort.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Dawn raids may be performed (i) as part of a flagrancy enquiry; (ii) as part of a police preliminary enquiry under the authority of a prosecutor; or (iii) under a judicial investigation headed by an investigating judge. Prerequisites for dawn raids vary depending on the type of investigation. For example, absent special circumstances, express written consent of a company's legal representative is required to carry out a dawn raid that is part of a preliminary enquiry, which is not required for a dawn raid that is part of a flagrancy enquiry. Specific conditions may apply to dawn raids carried out in the context of tax, competition, data protection, anti-corruption, and consumer law proceedings.

Save under specific circumstances, dawn raids can only be launched between 6 a.m. and 9 p.m., though they may extend past these hours. Police officers or investigating authorities must establish an inventory of all documents and articles seized and sealed. If these prerequisites are not fulfilled, the seizure of documents may be deemed void and seized documents may not be used as evidence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Negotiating deals with prosecutors is not a common practice in France yet. However, the option of entering into deals has become increasingly relevant since the creation of the CJIP.

A guilty plea procedure (*Comparution sur Reconnaissance Préalable de Culpabilité* or "**CRPC**") is available to both individuals and legal entities for most criminal offenses. CRPC is mainly used for non-complex cases, which do not require trial, and for which penalties and fines are capped by law. CRPC requires an admission of guilt by the defendant.

In December 2016, the Sapin II Law introduced the CJIP. The scope of CJIP is narrower than that of CRPC: CJIP only applies to legal entities and for criminal offenses related to corruption, influence peddling, money laundering, and tax fraud. Unlike CRPC, CJIP does not require an admission of guilt from the defendant. Penalties incurred under a CJIP must be proportionate to the benefits derived from the misconduct and may not exceed 30 percent of the company's average annual turnover calculated by reference to the previous three annual turnovers. The company may also be obliged to implement a compliance program monitored by the French Anti-Corruption Agency.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Managers and employees of a legal entity may be held criminally liable if they willfully participated in the commission of an offense. Mere knowledge of the commission of an offense by an employee working under one's supervision is not sufficient to establish the supervisor's criminal liability, provided they did not participate in the wrongful conduct. However, a CEO may be held criminally liable when the decision to commit an offense falls within the scope of their authority and such decision is, in practice, approved by the CEO.

Individuals can be fined, imprisoned, and/or subject to additional penalties, such as forfeiture, court-mandated treatments, affirmative injunctions, impoundment, closure of a business, and publication of the conviction.

Like individuals, legal entities may be held liable for criminal offenses committed by their corporate bodies or representatives. Legal entities may be punished by a criminal fine and/or additional penalties, such as restrictions on running the business, judicial control of the company, and debarment.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

There is no specific requirement in French law providing for a reduction or suspension of the penalties in case companies implement an efficient compliance system. However, the behavior of the company is carefully observed when it comes to determining potential sanctions and the possibility for the prosecutor to propose to the company to enter into a CJIP. The implementation of compliance program by legal entities which do not fall within the scope of Article 17 of the Sapin II Law is a favorable indicator for a CJIP to be proposed by the prosecutor. Likewise, spontaneously strengthening the existing compliance program after acts of bribery or corruption have been discovered may lead the prosecutor to consider the possibility to propose to the company to enter into a CJIP. Such behavior is also taken into account to determine the amount of the fine to be paid by the company under a CJIP.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Internal investigations, compliance programs, and deal negotiations are a growing practice in France. To date, 11 CJIP have been concluded. The ability to enter into deals with the prosecution authorities is a key factor for the growth of internal investigations. Increasing public interest in compliance-related matters has led to intense media coverage of these topics.

One particular case had wide media coverage: A non-listed French company has been inspected by the French Anti-Corruption Agency. The French Anti-Corruption Agency first came to the conclusion that the company had not implemented any proper compliance program. The French Anti-Corruption Agency then referred the case to its Sanctions Committee, which finally found that the company was "*fully compliant with the requirements*" of the Sapin II Law because the company's compliance program had been strengthened following the French Anti-Corruption Agency's inspection and in parallel to the sanctions proceedings.

CONTACTS

17, avenue Matignon
CS 30027
75378 Paris cedex 08
France

Tel.: +33 1 53 67 4747
Fax: +33 1 53 67 4748
www.hoganlovells.com

Arthur Dethomas
Partner
Hogan Lovells Paris
T +33 1 53 67 1877
arthur.dethomas@hoganlovells.com

Renowned for his experience in corporate, stock exchange and financial litigation and in white collar criminal law, Arthur Dethomas is licensed in Paris and in New York. Arthur has developed a recognized competency in complex cases and represents clients before courts as well as regulatory authorities. He has been involved on numerous internal investigations and has substantial experience representing clients in cross-border matters, including insider trading, financial fraud and the Foreign Corrupt Practices Act.

According to the Chambers & Partners guide "Arthur Dethomas receives very positive commentary from clients who 'have only positive things to say about him; he is extremely competent, very well known in the market and calm and measured in his work. He is highly experienced in shareholders' dispute and financial liability claim" and "wins praise for his ability to design and execute strategies".

Christelle Coslin
Partner
Hogan Lovells Paris
T +33 1 53 67 4706
christelle.coslin@hoganlovells.com

Christelle Coslin advises global companies on cross-border issues and mass tort litigation. For nearly 15 years, she has been helping large businesses by offering them pre-contentious advice and representing them in commercial disputes.

She also provides assistance to clients in a wide range of compliance matters, in particular the drafting, review and implementation of compliance policies and programs in light of French law. She also conducts risk assessments with respect to potential criminal liability and evaluates compliance programs. She can train employees on these matters and prepare clients' organization for dawn raids or authorities' visits.

She regularly advises clients on anti-corruption laws in both the private and public sectors. She also has significant experience in handling cross-border and/or internal investigations. Thanks to her understanding of the way global groups operate, Christelle is perfectly fit to supervise clients' internal investigations, whether the investigation was initiated by an authority or follows a whistleblower complaint.

Marie Voutsas
Associate
Hogan Lovells Paris
T +33 1 53 67 3824
marie.voutsas@hoganlovells.com

Marie Voutsas joined Hogan Lovells' Paris office in 2016. She focuses on commercial and product liability litigation.

Marie also provides assistance in matters regarding commercial contracts and unfair competition and has experience in multijurisdictional issues. Marie has developed a significant experience in helping clients shape and strengthened their policies and compliance programs.

Marie holds a postgraduate degree in Litigation, Arbitration, and Alternative Dispute Resolution from the University of Paris II Panthéon – Assas.

Germany

Hogan Lovells International LLP

Dr. Sebastian Lach

Matthias Samol

Overview

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X No criminal liability of companies, but administrative fines possible in case of misconduct of employees.	X	X	X	X
No					

Question List

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

There is no specific German law on whistleblower protection. However, case law allows dismissals and other sanctions of whistleblowers only under certain conditions. In particular, an employee cannot be dismissed instantly if they reported misconduct to fulfill their legal duties.

On 7 October 2019, the European Union adopted a Directive (EU 2019/1937) on the protection of persons reporting breaches of Union law (the "Whistleblowing Directive"). Member states have to transpose the Whistleblowing Directive into national law within two years. The rules aim to set common minimum standards for the protection of whistleblowers. They introduce i.a. mandatory safe reporting channels, the obligation to report back to the whistleblower within certain deadlines and an obligation to protect whistleblowers against dismissal, demotion and other forms of retaliation. In case a personnel measure against the whistleblower is taken, the burden of proof is with the company to show that the measure was not the reaction to the whistleblower submitting a report. A draft to transpose the Directive into German law has not been published yet.

The new Protection of Trade Secrets Act ("**GeschGehG**"), adopted on 18 April 2019 already now expands protection of whistleblowers to certain cases in which they are disclosing a trade secret. According to the law, there is no liability for disclosure of trade secrets where disclosure is in the *public interest* and if directly relevant misconduct, wrongdoing, or illegal activity is disclosed.

Despite these developments towards protection, a recent court decision of Regional Labor Court Baden-Wurttemberg (decision dated 20 December 2018 – 17 Sa 11/18) pointed out that the right to information based on the EU General Data Protection Regulation ("**GDPR**") may in some cases prevail whistleblower protection. In the specific case, a manager had been dismissed following an internal investigation. The manager was then granted access to a copy of all HR reports containing his personal data (Article 15 GDPR). This led to the exposure of the whistleblower's identity who initiated the investigation.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) According to Section 80 paragraph 2 of the German Works Constitution Act ("**BetrVG**") the employer is obliged to inform the works council about the investigation. The involvement of the works council is required if electronic data and emails are reviewed, transferred to external servers or analyzed with software (Section 87 paragraph 1 No. 1 BetrVG, see also "District Labor Court Cologne decision dated 9 May 2019 – 9 TaBV 125/18"). Further, the works council has the right to participate if uniform questionnaires are used which allow a conclusion to the employees' performance (Section 94 paragraph 1 BetrVG). Interviews performed as part of an internal investigation are generally not conducted based on such uniform questionnaires. In addition, an exemption from this participation requirement could be achieved by guaranteed anonymization of these questionnaires' results.

b) According to Art. 38 GDPR, controllers and processors shall ensure that the data protection officer ("**DPO**") is involved in all issues which relate to the protection of personal data. One of the DPO's duties is to generally consult the employees concerning their data privacy right. In addition, the DPO has the duty to monitor compliance with data protection regulations. Therefore, the company in general has to inform the DPO about all data privacy related procedures and processes of an investigation.

c) The prosecution authorities do not have the right to be informed, but a voluntary involvement can be advantageous.

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

In general, employees have the labor law duty to cooperate as far as the facts to be investigated relate to activities conducted or perceptions made as part of their work life. They must answer work-related questions truthfully and completely. If unrelated to work, a balancing of interests test is required to determine if a duty to cooperate exists. A relevant factor may for example be the employee's position in the company. A supervisory function may lead to greater cooperation duties. A balancing of interests also has to be performed in case the employee would be subject to self-incrimination. However, even then, the duty to cooperate generally applies.

In case the employee is required to participate, the employee's refusal may be regarded as misconduct. Such misconduct may justify a dismissal if the employee had already received a formal warning for the same or similar misconduct before.

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Investigative measures may trigger the two-week deadline for instant dismissal for cause. This deadline starts when the person of the company authorized to dismiss employees receives knowledge of the relevant facts. To avoid triggering this deadline too early, the employer should be informed of the results of the investigation at an advanced stage of the investigation after comprehensive information was gathered. Further, the interviewer should especially avoid using terms such as "interrogation", "hearing", or "questioning". Using such terms increases the risk of triggering labor law deadlines, especially for possible sanctions. Therefore, the interviewer should rather refer to

terms like "meeting" or "interview". Moreover, employees are also generally more willing to participate in an "interview" than in an "interrogation".

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Data privacy laws apply to any processing of data. This includes securing, collecting and reviewing data, as well as the creation of work products such as interview file notes and final reports. Therefore, it is very important to perform an early assessment of the applicable data privacy laws, to document the steps taken and generally to inform the data subjects accordingly.

b) Reviewing emails?

Private communication is highly protected under German law. Reviewing such emails may even constitute a criminal offense (breach of telecommunications secrecy) if data privacy requirements are not observed. Therefore, before conducting such an e-data-review a thorough analysis of legal exposure should always be performed.

c) Collecting (electronic) documents and/or other information?

Germany does not have a blocking statute regime. Its data protection statutes are based on the Data Protection Act and the EU General Data Protection Regulation.

Although communication with authorities can trigger applicability of data protection laws, the request of an authority will often be a sufficient justification for gathering and using data. In critical cases, it may be advisable not to produce data on a voluntary basis but to await a written formal request with the announcement of enforcement from the authority. In addition, the rules of international data transfer apply to document requests by foreign (non-EU/EEA authorities).

d) Analyzing accounting and/or other mere business databases?

There is no specific regulation for the analysis of accounting and business databases. In case the databases contain personal data, an assessment of the German and European data protection regulation has to be performed.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no general and statutory obligation to instruct an employee about the legal circumstances and his rights. Nevertheless, many companies in Germany consider explanations to be ethically required and advisable. In general, this includes a brief description on the background of the investigation and the subject matter. For documentation and transparency purposes, it can be advisable to provide these instructions in written form to be countersigned by the interviewee. Such information should also contain a data privacy notification.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

In contrast to an individual's right to remain silent in case of self-accusation during interrogations of criminal authorities, there is no corresponding right with regard to employee interviews as part of internal investigations. However, there are non-binding provisions of the German Federal Bar Association that recommend avoiding any behavior of the interviewer that might put pressure on the interviewee to incriminate themselves.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

An Upjohn warning must be conducted if relations to U.S. law exist. In addition, giving an Upjohn warning is an accepted best practice in Germany, too. However, there is no explicit legal obligation to do so under German law.

d) Be informed that they have the right that their lawyer attends?

Whether or not the employee has a general right to attendance of own counsel has not yet been fully confirmed or denied by case law. The companies often allow such attendance to have a fair set-up and/or if the employee is suspected of having committed criminal offenses.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

The employee does not have a strict legal right to be attended by a representative of the works council. However, to reduce potential risks of escalation with the works council and to ensure "equality of arms", companies often allow such attendance.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The employee should be informed and their consent should be requested. Transferring data to a recipient outside the EU/EEA is now only allowed if (in addition to a legal justification for the processing) the requirements for international data transfers with respect to ensuring an adequate level of protection at the recipient outside the EU/EEA are met (Arts. 44 *et seqq*. GDPR). In addition, adequate safeguards need to ensure that sufficient data protection is provided.

g) Sign a data privacy waiver?

There is no specific law requesting the signing of a data privacy waiver (i.e. consent of the data subject concerned) before conducting an internal investigation. At the same time, consent constitutes a legal basis for the processing of personal data in accordance with GDPR and BDSG. However, there are strict requirements for consent under the GDPR, in particular for consent requested by employees. Therefore it is generally advisable to (also) rely on the available statutory justifications for data processing (e.g. legitimate interest of the employer or a works constitution agreement). In certain cases it may however be necessary to request a waiver on the secrecy of telecommunications to mitigate potential criminal liability risks.

h) Be informed that the information gathered might be passed on to authorities?

Articles 13, 14 GDPR require that amongst other information the data subject is informed of the recipients or categories of recipients of the personal data. This includes the (potential) disclosure to authorities. In practice, interviewees are also often informed of potential disclosure to authorities.

i) Be informed that written notes will be taken?

For reasons of transparency, it should be explained how the information provided will be documented. As far as the documentation contains personal data, the interviewee also has a general right to be informed of the documentation and might also have a right to request access to the data. However, the interviewees' rights are limited to their personal data and do not extend to the entire documentation of the investigation.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law governing this question, but issuing such notices is a common procedure. Such notices should be clear, be sent to all potentially relevant addressees and be issued as early as possible. In addition, the data hold has to comply with applicable data protection regulations, e.g. retention periods and deletion duties.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

German privilege rules are very limited. Privilege protection depends mainly on where the documents are located and for what reason they were created.

To ensure privilege, the safest way is to involve outside counsel. In general, documents in custody of external counsel are protected. Documents in custody of the company are, however, only protected in isolated cases. Ideally, newly generated work products should therefore only be available on outside counsel's servers instead of keeping them on company's premises. This does not mean, however, that any existing document should be moved to outside counsel as this could mean a violation of German criminal laws.

Further, privilege protection will more likely be granted if the advice is provided in relation to a (potential) investigation by authorities. This can be shown by setting up a separate engagement letter for the internal investigation.

It may also be helpful to label privileged documents accordingly to prevent investigators' accidental access. However, the labelling itself does not automatically entail privilege.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Communication with and documents created by inside counsel are generally not privileged under German law. Only individual case law provided higher privilege protection to documents prepared by an inside counsel. According to this decision, documents prepared by inside counsel can be protected if drafted for the purpose of defense by outside counsel. This decision is, however, not yet established. Therefore, there is at least a significant risk that documents created by inside counsel are not privileged.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

As far as circumstances arise which could give reason to a claim against the insurance company, the policy holder should generally make a notification of circumstances to the insurer. In addition, the individual policy should be reviewed.

b) To business partners (e.g. banks and creditors)?

Information duties may arise from contractual obligations between the company and the business partner. Even if there is no explicit provision in the contract, there may be an obligation in case starting an internal investigation is highly important information for the other party and relevant with regard to the purpose of the agreement. These interests of the business partner need to be evaluated against the legitimate interests of the company. Therefore, it depends on the individual case whether and when the business partner needs to be notified.

c) To shareholders?

Potential reporting duties towards shareholders compete with the company's intention to maintain (business) confidentiality. Internal investigations are highly important aspects and could be seen as insider information that may possibly influence the stock price. The company has to evaluate case by case if there is an *ad hoc* duty to report to the shareholders. If the internal investigation affects the market price significantly and fulfills different criteria (e.g. risk of the internal investigation, scope, involved suspects) an obligation to disclose generally exits. In case of a violation of the reporting duties, the company and individuals acting may be held liable to pay damages according to Section 97 paragraph 1 of the German Securities Trading Act ("**WpHG**").

d) To authorities?

In general, there is no duty to inform the prosecutor about an internal investigation or potential misconduct within the company. There may only be exceptions for very significant crimes. However, a cooperative

approach with the local prosecutor may prevent adverse and unexpected measures by the authorities, such as dawn raids. It also has to be checked whether the company has a standing cooperation agreement with the authorities.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

The company has to minimize damages and try to prevent new ones to fulfill its supervisory duties. Additionally, the company may have to re-evaluate its compliance system in order to eliminate potential deficits and to improve its existing system. Further, the company may impose sanctions on the concerned employees to show that misconduct is not tolerated inside the company.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices generally appreciate internal investigations through external investigators e.g. law firms. Early involvement, communication and coordination may be helpful for a good cooperation with local prosecutors. In this regard, it is crucial that the company does not destroy any potential evidence or convey the impression that evidence is or will be destroyed. Therefore, data-retention orders should be communicated at the earliest stage possible.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Both search warrants and dawn raids must fulfill formal and material requirements stipulated by law.

The search warrant in general has to be issued by a district court, or – in case of imminent danger – by the prosecutor. It has to be written and signed (unless in case of imminent danger). Further, it has to describe the alleged facts and the offense that the individual is being accused of. The search warrant also has to indicate what evidence is expected to be found and why it is expected to be found at the particular place of the search. Further, there must be a reasonable suspicion that an offense was committed based on the experience of a criminal investigator. In addition, the search warrant, but also the dawn raid itself, has to be based on reasonable balancing of interest decisions. According to German case law, a search warrant is only valid for six months.

In case these legal requirements are not fulfilled, generally, the seized evidence may still be used in court proceedings. In Germany, there is no absolute "fruit of the poisonous tree" doctrine. Only in severe cases of illegally obtained evidence, the evidence may not be used in court. This may be the case if there was no reasonable suspicion of a criminal offense or if the decision was made without balancing the interests of the searched individual/company with the state's interest to prosecute. Formal legal requirements, such as a missing signature, will generally not lead to a prohibition of use of the seized evidence. According to German case law, exceptions can only be made in very severe cases, e.g. if the investigating authorities acted arbitrary.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

While deals and non-prosecution agreements are available for individuals, they are not provided for corporations under German law yet. The current draft law on the sanctioning of companies (***"Verbandssanktionengesetz – VerSanG"***) aims at introducing alternative sanctions that would correspond to deals and non-prosecution agreements.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Although companies are not subject to criminal responsibility under German law they can be subject to legal consequences, as administrative fines, disgorgement and debarment.

Individuals may face sanctions not only for their own misconduct but also for misconduct of other employees when they failed to implement a sufficient supervisory structure. Therefore they may face sanctions as imprisonment, fines or official debarment from their profession.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

An efficient compliance system is a key factor for preventing or reducing corporate sanctions in Germany. If a company does not have an adequate compliance system to prevent misconduct and criminal offenses of its employees it might be sanctioned with an administrative fine of up to €10 million plus disgorgement of profits according to Articles 30 and 130 of the German Administrative Offenses Act ("**OWiG**"). Such a fine requires an administrative or criminal offense constituting a breach of business related duties by an employee in a managing position or a breach of supervisory duties.

To avoid such a breach, an efficient compliance system should already be in effect when the alleged misconduct occurred. If this can be shown to the authorities, the compliance system will most probably have a reducing effect on a sanction or may even prevent a sanction in the first place. Even if an efficient compliance system has just been established as a consequence of misconduct, the implementation might have a reducing effect on a fine in case the new system ensures the prevention of similar future misconduct (see Supreme Court decision dated 9 May 2017 – 1 StR 265/16). In practice, prosecutors often tend to assess the compliance measures in place as insufficient. Therefore, documentation of the measures taken is very important.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

In June 2020, the German Government published a draft law for the sanctioning of companies (*"**Verbandssanktionengesetz – VerSanG**"*). The draft includes the introduction of the obligation of the Public Prosecutor to initiate proceedings upon strong and grounded suspicion of a company's offense and a much wider range of sanctions for companies. Specifically, the draft law stipulates a penalty for corporations in the amount of up to 10 percent of the average annual turnover for companies with an annual turnover of over €100 million. This could allow for higher sanction even if disgorgement of profit is not an option (e.g. if there was no profit made). For companies with a lower annual turnover, the current upper limit of €5-10 million will remain in effect.

The draft law also introduces new alternative sanctions, e.g. a warning combined with a suspended sanction, the duty to update and/or audit the company's compliance system or the publication of a sanction in an "appropriate way".

Additionally, the number of dawn raids continues to be on the rise. Therefore, preparing for dawn raids is becoming even more important.

CONTACTS

Karl-Scharnagl-Ring 5
80539 Munich
Germany

Tel.: +49 89 29012 0
Fax: +49 89 29012 222
www.hoganlovells.com

Dr. Sebastian Lach
Partner
Hogan Lovells Munich
T +49 89 29012 187
sebastian.lach@hoganlovells.com

Sebastian Lach is partner at Hogan Lovells Munich and head of the German IWCF practice. Sebastian Lach handles compliance and investigation issues, as well as complex product safety and liability cases. In the field of compliance and investigations, he has advised various clients on the creation of global compliance systems. Sebastian has successfully advised on criminal matters (e.g. bribery, fraud, embezzlement) and internal investigations relating to more than 50 countries worldwide, including FCPA, SEC/DOJ implications. Throughout his career, he has handled more than 20 multi-jurisdictional investigations, most of them for Fortune 500 and DAX 30 clients.

Matthias Samol
Senior Associate
Hogan Lovells Munich
T +49 89 29012 691
matthias.samol@hoganlovells.com

Matthias Samol works for national and international companies on all issues of corporate compliance as well as administrative and criminal aspects. He advises on cross-border internal investigations for Fortune 500 and DAX 30 clients in particular. His focus lies on the automotive and transportation sector. Throughout his career, he has supported clients on the set up and management of internal investigations. While doing so, Matthias has provided legal risk assessments and assisted on data collection and data reviews. Moreover, Matthias has conducted interviews and advised clients during dawn raids. During his legal training at the Higher Regional Court of Freiburg, Matthias worked, *inter alia*, at the Public Prosecutor's Office of Freiburg and an international law firm in Frankfurt and London.

Greece

Ovvadias S.Namias Law Firm

Dr. jur. Ovvadias Namias

Dr. jur. habil. Vasileios Petropoulos

Overview

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X Legal entities may only be liable for administrative violations, though company directors may be held criminally liable.	X	X	X Only in bribery cases.	X
No					

Question List

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

There is no specific procedure governing corporate internal investigations in Greek law. There are, however, some aspects that must be considered concerning whistleblower reports in bribery cases in the public sector.

A whistleblower reporting bribery in the public sector may receive some protection if granted "witness of public interest" status under Article 47 of the new Greek Criminal Procedure Code. The status is granted by order of the special anti-fraud prosecutor and confirmed by the Supreme Court Prosecutor competent for the supervision of the anti-fraud prosecutors. The "witness of public interest" is protected from retaliation in criminal, administrative, and labor law proceedings. For example, if a criminal complaint is filed against a "witness of public interest" for defamation as a result of their report, the prosecutor can decide to refrain from pressing charges. Similarly, a public servant with "witness of public interest" status may not be fired or otherwise retaliated against due their report.

Apart from this special status, there is no institutional protection for whistleblowers in the private sector and there is no specific rule governing internal investigations. In cases of internal reports, whistleblowers without "witnesses of public interest" status are not protected against criminal allegations of defamation and they can be subject to labor law sanctions, including dismissals. OECD recently proposed Greece to adopt its guidelines on protection of whistleblowers in bribery cases in the private sector as well; however this has not happened in the latest reform of the Greek criminal and criminal procedure law.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

There is no specific Greek law concerning the conduct of an internal investigation. There are, however, some rules which could apply:

a) Presidential Order 240/2006 (which implemented Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002) concerning the relations between employees and employers indicates that a works council has the right to be informed about an upcoming internal investigation and an obligation to keep it secret. There is, however, no provision concerning the active participation of the works council in an internal investigation.

b) Greek data protection legislation (Greek Data Protection Law 2472/1997 as well as the EU General Data Protection Regulation 2016/679) provides an obligation to inform the data protection authority before starting an internal investigation, if the investigation results in the processing of employee personal data, unless the data subject consents to the processing.

c) Performing an internal corporate investigation falls within the employer's managerial authority. This means that there is no general obligation for the company to inform other public authorities thereof. On the other hand, if the internal investigation reveals an upcoming performance of a felony, not reporting this to the criminal authorities would result in the misdemeanor of harboring a criminal.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

In general, there is no specific labor law obliging employees to support internal investigations and employees are generally not obliged to report misconduct. However, an obligation to participate in an internal interview could derive from the general fiduciary duty towards the company (the "bona fides rule" under Articles 288 and 652 of the Greek Civil Code, as recognized in the Greek jurisprudence).

In addition, employees with a special duty to report misconduct, e.g. members of the compliance department, must support the company's internal investigation or face criminal liability. Imposing disciplinary measures on an employee for refusal to cooperate during an investigation is a matter of internal company regulation.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

There are no specific deadlines to dismiss for cause if a company uncovers employee misconduct. Although a company should, in practice, act as quickly as possible, the company must be careful when sanctioning employees so as not to give the wrong impression (e.g. that the only aim of the internal investigation is to release employees without compensation).

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Greek constitutional law protects the privacy of telephone and email communication as well as access to personal data. If an interview is recorded or summarized, the company should seek the employee's consent.

Creating an archive of all employee interviews must additionally be announced to the Greek data protection authority.

b) Reviewing emails?

Telephone and email communication is protected by communication privacy laws during the communication itself. The content of the communication is protected as personal data by the data protection legislation. If an internal investigation results in the processing of employee personal data, the Greek data protection authority must be notified in advance, unless the employee consents to the processing.

Emails that have been sent from or received by an employee via their corporate email address are protected as personal data (Article 9A of the Greek Constitution and Law 2472/1997). However, this protection is not absolute. Recently, the Greek Supreme Court decided in plenum that it can be limited according to the proportionality principle (Article 25 of the Greek Constitution), when the employee has acted against the company. It is not clear whether this limitation can also apply to employees who have not acted against the interests of the company, but may be implicated in an investigation. In such cases, it is, therefore, recommended to seek the employees' consent. In any case it is crucial that the company has previously enacted internal rules concerning the proper use of the corporate computers.

c) Collecting (electronic) documents and/or other information?

Collection of electronic documents and/or other information might violate Greek data protection legislation. It is, therefore, recommended to either inform the Greek data protection authority about the classification of this information during the internal investigation or to seek the employees' consent. Once more, it is crucial for the company to enact internal rules concerning the proper use of corporate computers, forbidding the employees from using them for personal reasons.

d) Analyzing accounting and/or other mere business databases?

The Greek data protection authority should be informed in advance if the databases contain personal data.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no specific labor law on this topic. It is, therefore, a matter of internal company regulations.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

In contrast to criminal procedure, the "nemo tenetur" principle does not apply in private law. Therefore, there is no legal obligation for the company to instruct the employee about self-incrimination. Internal company rules may, however, provide such an obligation.

If the company provides the interview material to the prosecution authorities, a criminal procedure may not start against the interviewee, exclusively based on his interview, as this would violate the "nemo tenetur" principle. However, in practice, the prosecuting authorities will most likely proceed with the initiation of a criminal procedure using supplementary material (e.g. interviews with colleagues).

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no such obligation according to Greek labor law. However, without prejudice to the internal rules of a company, a general briefing of the interviewee on this point is advisable.

d) Be informed that they have the right that their lawyer attends?

There is no such obligation according to Greek labor law. However, without prejudice to the internal rules of a company, informing the employee accordingly is recommended.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is no such obligation according to Greek labor law.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

It is recommended to advise the employee about potential data transfers, as it would indicate that the data subject consents to the processing of their data. Informing the employee may count as silent consent if the employee is not opposed to the transfer.

g) Sign a data privacy waiver?

It is recommended to ask the employee to sign a data privacy waiver. Informing the Greek data protection authority before starting with the processing of the data is generally mandatory, unless the data subject consents to the processing.

h) Be informed that the information gathered might be passed on to authorities?

As with cross-border data transfers, it is recommended to advise the employee about potential recipients of the data, as it would indicate that the data subject consents to the processing of their data. Informing the employee may count as silent consent if the employee does not object.

i) Be informed that written notes will be taken?

It is recommended to inform the employee that notes will be taken as these notes might be considered "personal data" as well. Informing the employee may count as silent consent if the employee does not object.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Internal investigations are not common in Greek practice yet. Documents-hold notices or document-retention notices can be issued by a company and the employees will have to comply with them on the basis of the bona fides rule (Articles 288 and 652 of the Greek Civil Code, as recognized in the Greek jurisprudence).

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege is established in the Code of Lawyers and is binding for all lawyers registered with the Bar, irrespective of their status as freelancers or in-house counsel. The privilege protection extends to documents, objects, data, or information obtained in the course of their representation of the client and applies to internal investigations.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

The attorney-client privilege is binding for all lawyers registered with the Bar, including in-house counsel. Nonetheless, it is possible that, according to internal company policy, only specific employees of the company, e.g. the President, Vice President, or the members of the Board of Directors, are considered the "clients" of in-house counsel. Hence, not all employee communications with in-house counsel may be protected by this privilege.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There is no general legal obligation to notify an insurance company with regard to the start of an investigation. Nonetheless, such an obligation might be provided by the insurance contract.

b) To business partners (e.g. banks and creditors)?

A company is not generally obliged to inform its business partners as soon as it starts an investigation. However, the relationship between the parties might give rise to a notification obligation.

c) To shareholders?

If a company's shares or other financial instruments are traded in the stock exchange, the company is generally obliged to inform the public about important issues, including an ongoing investigation, if the internal investigation would be considered insider information under applicable capital market regulations. However, the company is not obliged to provide early notification of the start of an investigation.

d) To authorities?

Companies are not obliged to notify criminal authorities about the initiation of internal investigations, unless there is certain knowledge that a felony is about to be committed. Nonetheless, informing data protection authorities about such investigations might be required, as described above.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Measures to eliminate or limit compliance violations should immediately be taken (e.g. giving the legal department control of production or finance, sanctioning of liable personnel, and rethinking the compliance structure of the company). Depending on the alleged conduct and the sensitivity of each case, company management is typically advised to contact the competent administrative authorities (e.g. the Capital Market Commission or the Competition Commission) or, if applicable, the prosecuting authorities, and declare the company's willingness to minimize damages and prevent new harms. The competent state authorities might call on the company to re-evaluate its compliance system or to impose sanctions on employees. The company's cooperation is a clear mitigating factor, should the authorities impose administrative fines.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Greek prosecutor offices have little experience with internal investigations. The results of an internal investigation may lead prosecutors to officially open a criminal proceeding by ordering a pre-trial inquiry. Within this inquiry the company's officials are likely to be summoned either as witnesses or, more probably, as defendants. This has been the case in several recent criminal cases in the pharmaceuticals industry. On the other hand, in a very recent market manipulation case, the Greek prosecution authorities started using the results of an internal investigation, delivered to them by the company itself, without conducting own investigative measures.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

According to the Greek Criminal Procedure Code and the Greek Constitution, every search performed by law enforcement officers in the suspect's residence or the company's seat, requires the presence of a judge (including magistrate judges) or prosecutor (prosecutors in Greece are part of the judicial authority in the broad sense). Therefore, there is no procedure prescribed in Greek law concerning the issuing of a search warrant by the court. Dawn raids are similarly performed by prosecution (police) officers in the presence of a judge.

In practice, searches and dawn raids are usually performed at the stage of primary investigation of a felony. However, in cases of flagrant offenses, or if there is imminent danger of losing important material evidence, law enforcement officers may directly proceed with a search or raid. They are then obliged to compose a written report (e.g. about the material they confiscated), which must be immediately submitted to the prosecutor.

Further serious investigative actions, such as surveying the company's seat, can only be performed after approval by a Judicial Council and only in serious cases as described in Art. 254 and 255 of the Greek Penal Procedure Code. If the prerequisites for performing searches or dawn raids are not fulfilled, the evidence is, in most cases, considered illicit and cannot be used against the company.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Up until July 2019 there were no legal provisions for non-prosecution agreements or deferred prosecution agreements in Greece. Since then, Greek prosecution authorities are entitled to perform under the principle of opportunity. The new Articles 48 and 49 of the Greek Penal Procedure Code permit them to refrain from prosecuting several crimes, including several financial felonies, under specific conditions (e.g. full restitution of the victim, donation to charity programs etc.). However, NPAs or DPAs are still not common yet. In practice, the behavior of the defendant during the procedure is generally evaluated by the court at the hearing stage either as a mitigating factor or as an indicator of a lack of *mens rea*.

With respect to white collar crimes against the Greek State (e.g. tax and economic crimes), there is also a growing trend that criminal authorities do not press charges or press only minimal charges against defendants who fully compensated the State.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

There are no criminal sanctions for companies in Greece. There are, however, administrative sanctions, mainly fines, as well as the sanction of exclusion from business with the Greek State or revocation of permission. These are mainly described in the special anti-money laundering legislation.

Directors may, in contrast, be held criminally liable for the misconduct of employees, but only when, according to their duties, they were appointed with the specific obligation to prevent the misconduct at issue. Hence, it is important for a company to maintain a clear corporate governance diagram.

Felonies are severely penalized with up to 15 years of imprisonment, though actual prison time differs from case to case. Misdemeanor incarceration sentences are usually suspended. However under the new Penal Code they can no longer be converted to pecuniary penalties but only to community service.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

There is no such provision obliging Greek criminal authorities to reduce or suspend a penalty imposed on the company officers due to the implementation of an efficient compliance system. On the other hand, the full absence of such a system might trigger criminal liability for directors in cases of bribery in the public sector. However, an efficient compliance system is always a mitigating factor when imposing administrative penalties on the company.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

As of July 2019, Greek criminal authorities operate under a new Penal and Penal Procedure Code. Active bribery in the public sector was changed from felony to misdemeanor in July 2019 and back to felony in November 2019. This change affected the statute of limitation in several pending cases. Furthermore, the scope of bribery in the public sector, which used to be extended to corporations serving public interests, to banks and to companies subsidized by the Greek State, is now confined only to the public sector in a more narrow sense. Pending cases of bribery in the

public sector, which no longer falls under this scope, are now being prosecuted under the scope of bribery in the private sector. Bribery in the private sector was criminalized only after 2007. However, this has not prevented a first instance court of felonies from convicting several defendants for bribery in the private sector for crimes committed before 2007. Such a case is now pending in the court of appeal.

Furthermore, according to the new Penal Procedure Code it is no longer possible to seek civil damages through the criminal process. The previously known "civil party" of the criminal trial, e.g. the victim damaged by the crime, previously could raise a civil action within the criminal trial. Now, it may participate in the criminal procedure only to support the prosecution. This put an end to a trend that had occurred in several bribery cases, when the Greek State had named corporate entities as defendants in civil actions within the criminal procedure. The institution of the "civilly liable person" has been abolished.

On the other hand, financial crimes against the Greek State remain severely punished. Although the previous law, which could result in lifetime incarceration, has been abolished, Greek prosecutors tend to press charges aggressively. In the last years, asset confiscation, which is provided for under criminal tax legislation, anti-money laundering legislation, and legislation for the combat of public and commercial bribery, has been frequently used. Furthermore, according to Greek law, anti-money laundering legislation applies also in cases when the previous crimes, from which money derives, have come under the statute of limitation.

Finally, as of July 2019, Greek prosecution authorities operate for the first time under the principle of opportunity. At first glance it seems, however, that they are reluctant to proceed with closing NPAs or DPAs with the defendants.

CONTACTS

OVVADIAS S.NAMIAS
Law Firm

16, Voukourestiou Street
106 71 Athens
Greece

Tel.: +30 210 7239738
+30 210 3639793
Fax: +30 210 7239773
www.namiaslaw.gr

Dr. jur. Ovvadias Namias
Managing Partner
Ovvadias Namias Law Firm
T +30 210 7239738
+30 210 3639793
ovvadias.namias@namiaslaw.gr

Ovvadias was born in Athens in 1964 and has been a member of the Athens Bar Association since 1993. He graduated from the Law Department of the University of Athens and received his PhD in Criminal Law from the University of Bonn in Germany. He lectured in the Law Department of the University of Athens and was an Attorney at Law of the national Bank of Greece for criminal matters from 1999 to 2006. He has been a member of the Board of Directors of the Hellenic Criminal Bar Association since 2004 and he was awarded the Babakos Prize by the same Association in 2001. He is the acting President of the General Assembly of the Jewish Community of Athens. In 2006 Ovvadias established the Law Firm Ovvadias Namias. As a managing partner of the Firm he managed major penal cases for crimes relating to the banking, stock-exchange, tax, customs office sector, crimes relating to the legalisation of profits from illegal activities (money laundering), the environment, personal data and sports, in all instances of the criminal courts.

Ovvadias is fluent in English, German, and French.

Dr. jur. habil. Vasileios Petropoulos
Associate
Ovvadias Namias Law Firm
T +30 210 7239738
+30 210 3639793
vasileios.petropoulos@namiaslaw.gr

Vasileios was born in Athens in 1980. He received his education at the Universities of Athens (2001, LL.B.), Munich, Ludwig Maximilian Universität, (LL.M, in German Law 2003; PhD in criminal Law 2005; "Habilitation" and Venia Legendi in Criminal Law, Criminal Procedure Law, European and International Criminal Law, Economic Criminal Law 2010) and Zurich (PhD in Capital Market Law 2008). He lectured at the University of Athens (2010-2017) and has been an appointed Lecturer of Criminal Law and Criminal Procedure at the Neapolis University Pafos in Cyprus.

Vasileios joined the Law Firm Ovvadias Namias in 2010 and has been a member of the Patras Bar Association since 2003.

Vasileios is fluent in German and English.

Hungary

Hogan Lovells Budapest, Partos & Noblet

Dr. András Multas

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Employers in Hungary are not obliged to create a whistleblowing system, but, if they choose to do so, the system is regulated by law. According to Act CLXV of 2013 on complaints and reports of public interest ("**Whistleblowing Act**"), investigators (the employer or a third party engaged by the employer) are obliged to keep confidential the content of a whistleblower report and information concerning the persons involved, in particular the identity of the complainant, until the investigation is completed or prosecution is initiated. Investigators are not allowed to share information with other employees or employee representatives. However, information on the content of the report must be disclosed to the person or entity that is the subject of the report.

In the context of private whistleblowing systems, employees are protected by the Labor Code of Hungary, which provides that an employee may not be terminated for lawfully exercising a right. While this is not absolute protection, if a termination is explicitly or implicitly based on the employee's whistleblower status, it will be deemed unlawful.

In addition to internal investigations, the Whistleblowing Act also sets out provisions in relation to complaints and reports of public interest, which individuals may file directly with government bodies and the local government. In the context of such complaints and reports, the Whistleblowing Act establishes that any measures detrimental to the complainant must be avoided, even if, under different circumstances, such measures could be considered lawful.

Employers are required to investigate internal whistleblowing reports. Complaints and reports of public interest to authorities must also be investigated. On the basis of a well-based complaint or report of public interest, the following must be done: a) restoring legality; b) stopping the causes of the errors discovered; c) remedies; and d) initiation of accountability procedures if needed.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) According to Section 262 of Act I of 2012 of the Labor Code, works councils monitor compliance with labor law provisions and employers are obliged to consult the works councils before adopting regulations – such as a whistleblowing reporting system – that affect a large number of employees. Section 15(2) of the Whistleblowing Act prohibits investigators from disclosing information to employee representatives until the investigation is completed or prosecution is initiated. However, if a whistleblower reporting system is operated by outside legal counsel, which is not yet common in Hungary, and a report is made, which concerns an act or omission of a company executive, outside legal counsel must immediately inform, among others, the supervisory board, which under Hungarian law can consist of employee representatives.

b) According to the General Data Protection Regulation ("**GDPR**") it is generally not mandatory to employ a data protection officer ("**DPO**"). The Whistleblowing Act does not contain any specific rules for notifying the DPO. However, the DPO can be a member of the investigation team, in which case they will be informed. There is no obligation under applicable law to notify the Hungarian data protection authority of the launch of an investigation.

c) Authorities have no right to be informed until the investigation is completed. After completion, the competent authorities may need to be informed, depending on the outcome of the investigation. If a criminal offense is confirmed, such an offense must be reported.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

The Labor Code provides that, as a general principle, employment relationships are governed by the principle of good faith and fair dealing. This may imply a duty to cooperate, as employees are not allowed to behave in a manner that violates the rights or legitimate interests of the employer.

An internal whistleblowing policy can establish a more concrete obligation for employees to cooperate. Breach of such an obligation can lead to disciplinary action if specified in the applicable collective bargaining agreement or in the employment contract. A disciplinary action can be a written warning, limited financial penalties, and/or the termination of the employment contract. Even if not specified in the collective bargaining agreement or employment contract, failure to comply with an internal policy can still result in the termination of the employment contract, depending on the seriousness of the breach.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

The employer's right to terminate an employee with immediate effect must be exercised within 15 days of discovery of the grounds for termination, but, in any case, must be exercised within one year after the misconduct occurred, or, in the case of a criminal offense, up to the expiration of the statute of limitations. Based on applicable case law, the 15-day deadline is triggered when the person or body entitled to issue the termination notice takes sufficient note of the facts to make the decision. In case of an ongoing investigation, the 15-day deadline does not start until the investigation is completed or at least at an advanced stage. The Whistleblowing Act provides that an investigation must be completed within 30 days after receipt of a report, which may be extended in exceptional cases, but, in any case, may not take longer than three months.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

When processing data concerning the interview, data privacy laws, in particular, the GDPR and Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information apply to the collection and processing of data.

b) Reviewing emails?

According to the Labor Code, an employer is obliged to inform employees in advance about possible access to, or monitoring of, their emails and devices. Moreover, pursuant to the GDPR, the employer is obliged to inform employees about all processing of personal data. This is usually accomplished with an internal policy. The distribution of the policy must be documented by the employer.

According to the GDPR, emails can only be accessed, stored, and monitored by the employer for a legally justified purpose, and access, storage, and monitoring must be limited to the review of necessary data. The Labor Code adds that monitoring must be limited to the employee's actions in relation to the employment relationship. The monitoring of private communications is prohibited. Hence, even where the employee uses office IT devices for private purposes, the employer cannot process private content and must delete it from backup copies. According to a decision of the Hungarian Data Protection Authority in an individual case, if the employee is allowed to store private information on the office computer's hard drive and use the office email address for private purposes, the employer must provide the employee time to remove this information before the monitoring starts. However, unless expressly permitted by the employer, it is prohibited to use corporate devices for personal purposes.

c) Collecting (electronic) documents and/or other information?

If the collection of documents and other information involves the monitoring of the employee's computer and/or other devices, the rules set out in section 5b apply.

d) Analyzing accounting and/or other mere business databases?

There are no rules under Hungarian law that would impede the use or review of accounting and business databases during an investigation.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

According to the Whistleblowing Act, on submission of their complaint to the employer, the whistleblower must be informed of procedural deadlines, the possibility that a personal interview may be necessary, the consequences of a report submitted in bad faith, and the possibility to submit anonymous reports. The subject of the report must be informed, in detail, of the report concerning them, their rights, and the rules of procedure at the beginning of the investigation. While the affected persons must be informed about their procedural rights, there is no obligation for the investigators to hand out written instructions to the whistleblower.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

In contrast to an individual's right to remain silent during interrogations by criminal authorities, there is no corresponding right for employee interviews as part of internal investigations.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no explicit legal obligation to provide an "Upjohn warning" under Hungarian law.

d) Be informed that they have the right that their lawyer attends?

According to Section 15(3) of the Whistleblowing Act, investigators must ensure that the subject of the whistleblower report has the opportunity to seek legal representation before giving a statement regarding

the report. This provision does not specify whether the legal representative may be present at the interview. However, Section 15(3) appears to imply a right to have a lawyer present.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

According to Section 15(2) of the Whistleblowing Act, investigators are not allowed to share information with employee representatives until the investigation is completed or criminal prosecution is initiated. The attendance of a member of the works council is therefore not be possible.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Employees should be informed of all details concerning the processing of their data, including the transfer of personal data within Hungary, within the European Union, or to a third country, such as the United States. It is advisable to explain this possibility in the whistleblowing policy, including all relevant details, such as the legal basis of the transfer (e.g. EU-U.S. Privacy Shield).

g) Sign a data privacy waiver?

Data privacy waivers do not exist under Hungarian law.

h) Be informed that the information gathered might be passed on to authorities?

According to the GDPR, the data subject must be informed of all relevant details concerning data processing. This includes details of data transmission to authorities. It is advisable to explain this possibility in the whistleblowing policy.

i) Be informed that written notes will be taken?

According to Hungarian law, there is no explicit legal obligation to inform the employee that written notes will be taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law governing document holds or retention notices, but internal policies may regulate the relevant processes. IT policies may also entitle employers to scrutinize employee devices and retain information directly from such devices.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

If the documents containing the results of the investigation have been prepared by outside counsel or are in the custody of outside counsel, they fall under the confidentiality rules set out in Act LXXVIII of 2017 on attorneys, and, therefore, are protected by attorney-client privilege.

According to Section 16(1a) of the Whistleblowing Act, an internal whistleblowing system may be operated by outside counsel. It is, therefore, advisable to engage outside counsel to operate the company's internal whistleblower system in order to have a stronger claim to attorney-client privilege. It may also be helpful to label privileged documents accordingly to prevent accidental access by investigators. However, labelling itself does not automatically guarantee privilege.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

There are no specific rules for confidentiality applicable to in-house counsel under Hungarian law.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Certain notification obligations may be found in the relevant insurance policies. However, notification cannot violate the law.

The investigators must keep the content of the notification and the information on the persons concerned in the case confidential until the investigation is completed or criminal prosecution is initiated. Investigators are not allowed to share information with third parties. Actions might be taken once the investigation is completed.

b) To business partners (e.g. banks and creditors)?

The investigators must keep the content of the notification and the information on the persons concerned in the case confidential until the investigation is completed or criminal prosecution is initiated. They are not allowed to share any information with third parties. Actions might be taken once the investigation is completed.

Certain reporting obligations can apply under the relevant agreement, which, however, may not violate the law.

c) To shareholders?

There are no specific rules under Hungarian law in this regard. However, according to Sections 55 to 60 of Act CXX of 2001 on the Capital Market, issuers of securities that have been offered to the public must disclose to the public without delay any information that concerns, directly or indirectly, the value or yield of their securities issue, and which may have any bearing on the reputation of the issuer. Issuers must, at the same time, file that information with the Hungarian National Bank as well.

d) To authorities?

Authorities have no right to be informed until the investigation is completed.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There are no explicit rules for immediate measures to be taken. However, an investigation should not disguise evidence or interfere with a public investigation. In the absence of any specific rules in this context, companies are obliged to act in accordance with the general principles of law and take measures in order to mitigate the damages caused by any potentially unlawful conduct and suspend any activity that could potentially qualify as a criminal offense. The nature of the actions to be performed by the affected company depends on the actual circumstances and should be assessed on a case-by-case basis.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Since the Whistleblowing Act covers internal investigations, such concerns should not arise as long as the investigation complies with applicable laws.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Search warrants are used in criminal proceedings and must comply with the formal and material requirements of the law. They must be issued by a court, the prosecutor, or the investigating authority, such as the police or the National Tax Authority. A search warrant may be issued if it can be reasonably presumed to lead to finding a criminal suspect, evidence of a crime, or property/items subject to confiscation. A search warrant must be issued in

writing and must describe what evidence or items are expected to be found. Evidence obtained improperly by a court, the public prosecutor, or the investigating authority may not be considered and used as evidence.

In addition to criminal proceedings, on the basis of authorization by the court, the Hungarian Competition Authority in antitrust matters, and, on the basis of authorization by the prosecutor, the Hungarian Tax Authority in tax matters, may carry out dawn raids.

The Hungarian Competition Authority is empowered to conduct "site searches" of any premise, vehicle, or data medium to find evidence connected to the infringement investigated. Investigators may enter premises without the consent of the owner or tenant and without anyone present. They may also open any sealed-off area, building, or premises during the search. The Hungarian Competition Authority is entitled to prepare forensic copies and seize objects. It may request police assistance where deemed necessary for the successful and safe conduct of the site search. A site search may only be carried out in possession of a prior court order. Furthermore, as of 1 January 2021, the Hungarian Competition Authority is empowered to use covert recordings as evidence, provided that such recording is not the only proof of the infringement. That being said, evidence unlawfully obtained by an authority (including the Hungarian Competition Authority) shall not be admissible as evidence during competition supervisory proceedings.

The Hungarian Tax Authority has similar authority to carry out dawn raids in tax matters.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

According to Act XC of 2017 on criminal procedure ("Criminal Procedure Code"), the prosecutor is entitled to dismiss a criminal complaint or suspend an investigation if the person involved in the criminal offense cooperates in the investigation by providing evidence and if the interests of national security or law enforcement take priority over the interest of the state to prosecute. Under Hungarian law, corporations cannot benefit from these deals, since the criminal offense itself is always committed by individuals.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Act CIV of 2001 provides criminal sanctions against legal entities for willful criminal offenses committed by their directors, representatives, supervisory board members, employees, or contractors. Sanctions such as dissolution, limitation of activity, or fines may be imposed on the legal entity, if the legal entity benefited from the criminal conduct or used a vehicle to carry out the offense.

The Criminal Procedure Code lays down specific rules for the criminal liability of executive officers and directors in relation to the misappropriation of company funds and passive corruption, i.e. the request, acceptance or receipt of an unlawful advantage. In both cases, the maximum term of imprisonment is three years. However, in case of passive corruption, if the perpetrator breaches his official duty in exchange for unlawful advantage or commits the offense with accomplices or on a commercial scale, he could face up to eight years' imprisonment.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

In competition matters, the Hungarian Competition Authority may reduce the penalty as follows.

For compliance programs implemented prior to the proceedings in antitrust matters, a reduction of up to 7 percent is subject to (i) the implementation of suitable compliance efforts; (ii) stopping the infringement after being detected internally; and (iii) substantiating that the infringement was stopped as a result of the compliance program. In addition, if the compliance program contributed to suitable evidence for a leniency application, a

further 3 percent reduction can be reached. The lack of involvement of high-level officials is required in both cases. In consumer protection proceedings, the reduction percentage is not specified by law.

For compliance programs implemented after the initiation of the proceedings in antitrust matters, the Hungarian Competition Authority may reduce the penalty by up to 5 percent if the implementation is undertaken in conjunction with a leniency application, a settlement or active measures to rectify the consequences of the infringement. In the event of a consumer protection infringement, the Hungarian Competition Authority may reduce the penalty by up to 20 percent subject to active reparation or the admission of the infringement, and up to 5 percent without such reparation or admission.

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The implementation of internal whistleblowing systems is not mandatory under Hungarian law and, thus, such internal systems are not widespread in Hungary. Whistleblowing policies are mainly implemented in Hungary by U.S.-based companies based on their legal obligation to do so under U.S. law. To comply with the Hungarian Whistleblowing Act, these policies need to be adjusted accordingly. This is a challenge for many international corporations operating in Hungary, which are subject to other laws and may wish to implement their whistleblowing system in a standardized manner across all jurisdictions.

CONTACT

Hogan Lovells Partos & Noblet

Gerbeaud House
Vörösmarty tér 7/8
Budapest 1051
Hungary

Tel.: +36 1 505 4480
Fax: +36 1 505 4485
www.hoganlovells.com

Dr. András Multas
Senior Associate
Hogan Lovells Budapest
T +36 1 505 4480
andras.multas@hoganlovells.co.hu

András is a member of the employment team in the Budapest office. András advises on various employment law areas including policy implementation and various compliance matters (including anti-bribery, whistleblowing etc.). András has also advised a number of clients on data protection and privacy matters.

Ireland

A&L Goodbody


Kenan Furlong


Kate Harnett


Deirdre Roddy


Bríd Nic Suibhne

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X		
No				X Only where specifically provided for (eg. Corruption legislation)	X Only in anti-corruption legislation

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Procedures must take account of the Protected Disclosures Act 2014, which provides protections for workers in Ireland who make "protected disclosures" of relevant information, which, in the worker's reasonable belief, tend to show one or more "relevant wrongdoings". A "relevant wrongdoing" is broadly defined and includes the commission of an offense, failure to comply with a legal obligation, miscarriage of justice, danger to the health and safety of any individual, damage to the environment, misuse of public funds or resources, gross mismanagement by a public official and destruction or concealment of information relating to any of the foregoing. Whistleblowers must be provided with protection from dismissal or penalization and protection of their identity (subject to certain exceptions).

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) There is no requirement for an employee representative body to be informed about an internal investigation before it commences.

b) There is no general requirement to notify the Data Protection Commissioner. However, this is likely to depend on the subject matter of the investigation.

c) If a criminal offense may potentially have been committed, then a mandatory reporting obligation to the Irish police could arise if the offense is included in a list of scheduled offenses enshrined in legislation. This

applies to a broad range of theft, fraud, company law, financial services law, and white collar type offenses. A company (or members of its senior management) may also have mandatory reporting obligations to the company's regulator(s).

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

A common law duty of mutual trust and confidence is generally implied in employment relationships. This would require the employee to answer questions in connection with their employment, honestly and truthfully. A duty to cooperate in such investigations often features in company policies. It would be usual for the disciplinary process to apply to employees who refuse to cooperate.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

No labor law deadlines are triggered by investigative actions. Similarly no rights to sanction employees are waived by investigative actions. However, where an investigation is being carried out without affording the employees involved the benefit of fair procedures, an employee could bring civil proceedings seeking injunctive relief to restrain the continuation of the investigation. Observing fair procedures is a crucial component of the investigative process in Ireland, and will reduce the likelihood of an employee obtaining injunctive relief. Employment injunctions are relatively more common than other types of injunctions. Usually, these orders are sought on an interim basis (i.e. pending a breach of contract claim), but some cases have seen injunctions granted that prevent action such as dismissal outright.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Data protection legislation (including the Data Protection Act 2018, General Data Protection Regulation Regulation (EU) 2016/679 ("**GDPR**"), and any amending legislation) applies to any processing of personal data.

The employer will be the data controller of personal data collected or used during interviews (whether it conducts the interview itself or delegates it to a third party). Thus it retains responsibility for the personal data and ensuring that it is processed in accordance with data privacy laws (in particular the obligation in relation to fair and transparent processing). The employer will therefore be responsible for ensuring that employees are adequately informed that their personal data may be processed for the purpose of these interviews; about the categories of personal data processed; and the legal basis which the employer is using to process such data. Employees must also be informed as to whom their personal data will be disclosed to; how long it will be retained and processed; whether it will be transferred to a non-EEA country (and if so the safeguards in place and means to obtain a copy of them), what their rights are in respect to their data (e.g. right of access, right of rectification, and right of erasure), their right to lodge a complaint with the competent supervisory authority, whether the provision of their personal data is a statutory or contractual requirement and the existence of any automated decision-making in relation to their data.

The employer will also need a lawful basis for carrying out such processing. If reliance is placed on legitimate business interests as the legal ground for processing, the employer must specifically outline what that legitimate business interest actually is. Consent is also a lawful basis for processing. However, due to the perceived imbalance of power in the employer/employee relationship, together with the much higher compliance threshold for relying on consent under GDPR, it is not advisable to rely on employee consent alone as a lawful basis for processing employee personal data.

If the interviews involve the processing of any sensitive personal data, the employer will need to ensure that one of the more limited legal bases for processing such sensitive personal data can be relied upon. Employers should seek to resist collecting or processing sensitive personal data wherever possible.

b) Reviewing emails?

The same obligations in relation to fair and transparent processing, and having a lawful basis to carry out the processing outlined above, equally apply to reviewing emails. The employer should have an email monitoring policy in place with employees, which is brought to employees' attention so that employees are on notice that their communications are not private and are monitored. Employers should only monitor employee emails where it is reasonably necessary in the interests of the business and without prejudice to the fundamental rights, freedoms, or legitimate interests of employees.

c) Collecting (electronic) documents and/or other information?

If the collection of documents includes personal data, the employer will need to ensure it meets its fair processing obligations (i.e. provides the individuals whose personal data is collected with information as to why their data is being collected, and for what purpose, as detailed in 5a above). This may be covered in a privacy policy or employment manual. There must also be a lawful basis for collecting such data, such as if it is required to comply with a legal obligation or for the legitimate business interests of the employer and where such interests do not outweigh the rights or freedoms of the employee.

d) Analyzing accounting and/or other mere business databases?

To the extent that business databases contain any personal data, the employer must ensure compliance with its fair processing obligations and have a lawful basis for collecting personal data as outlined above. Any investigation should take account of the Official Secrets Act 1963, which prevents disclosure, without authorisation, of "official information" of public office holders and confidential contractual information.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

Where possible it is generally considered best practice, in advance of any interview, to communicate in writing the investigation terms of reference to the employee. This should be done where the investigation could lead to findings, which may have an adverse impact on the employee in question**.** However, there is no legal requirement to state this in writing.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

Irish law recognizes a "privilege against self-incrimination". There is no statutory obligation to advise an employee of this, though there is a requirement to ensure that fair procedures and natural justice are applied in the course of the investigation. If there is an allegation of criminal wrongdoing involving the employee, fair procedures and natural justice are interpreted as requiring the employee to be notified of their entitlement to seek independent legal advice from their own lawyer.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

In accordance with fair procedures, it should be made clear to the interviewee that any lawyers present are acting for the company, and not the employee, who may in some cases have their own legal representation.

d) Be informed that they have the right that their lawyer attends?

This depends on the type of investigation. There is no right to (and therefore no right to be informed about) representation if the investigation is a fact-gathering exercise, prior to a separate disciplinary hearing that will decide if the allegations are proven or not. However, where the investigator appointed will reach formal findings, the principles of fair procedures and natural justice will apply, which can include in certain cases, the right to legal representation and the right to cross examine one's accuser.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

As mentioned above with respect to the right to legal counsel, the right to representation depends on the type of investigation, in particular, whether the investigator will reach formal findings against the employee.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Employees must be informed of all processing activity carried out on their personal data, including where the data is to be transferred to a country outside the EEA, such as to the United States.

g) Sign a data privacy waiver?

Signing a data privacy waiver is not necessary and, in fact, it would not be advisable to rely on consent of employees for processing their personal data. As outlined above, there are alternative lawful grounds available to employers to process personal data.

h) Be informed that the information gathered might be passed on to authorities?

In order for the employer to meet its fair and transparent processing obligations, interviewees must be informed that their personal data may be passed on to authorities. The employer would need to have a lawful basis for sharing the data with the authorities, such as compliance with a legal obligation.

The disclosure of personal data to authorities would also be lawful to the extent that such disclosure is necessary for the purpose of preventing, detecting, investigating, or prosecuting criminal offenses or preventing a threat to national security, defense, or public security.

i) Be informed that written notes will be taken?

It is best practice to inform employees that notes will be taken. It is advisable to share draft notes with the employee following the interview and afford the employee an opportunity to respond to the content, in particular where the investigator can make formal findings against the employee. While this is not a strict requirement under Irish law, failure to adhere to principles of fair procedures and transparency may compromise an investigation.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Such notices should generally be issued as a matter of good practice to "custodians" of material potentially relevant to the investigation in order to secure and ensure the safekeeping of the material.

It is also advisable to suspend routine/automatic document or data destruction processes for any records or materials which may be potentially relevant to the matters under investigation, to ensure that relevant material is not unwittingly destroyed.

There is no specific form such notices must follow. Typically they should be issued as soon as possible to persons (or "custodians") who are likely to hold potentially relevant records or materials, in order to make the recipient fully aware of their obligations to preserve all relevant records and materials.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege may be claimed over the findings of the internal investigation if it can be established that either "legal advice privilege" or "litigation privilege" applies. Legal advice privilege protects communications between lawyers and their clients, the dominant purpose of which is seeking or providing legal advice. Litigation privilege protects confidential communications between a client and their lawyers and third parties, where the dominant purpose is to prepare for actual or reasonably apprehended litigation. The Irish courts have held that litigation privilege can apply in relation to materials generated in contemplation of a regulatory or criminal investigation.

Protection of privilege in an internal investigation requires advance planning and regular review. In order to maximize a claim to privilege it is generally advisable (among other things) to: (i) involve external lawyers at an early stage; (ii) where appropriate, label documents created in relation to an investigation with an appropriate "privilege" tag; (iii) limit the dissemination of legal advice, privileged work, and other sensitive documents to a small group and to what is strictly necessary in the circumstances; and (iv) ensure that material relating to the investigation is stored separately.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

In-house counsel is entitled to be treated in the same way as external legal counsel in respect of legal privilege in Ireland. The principal exception to this is in relation to European Commission competition investigations, where the European Court of Justice has held that communications with in-house lawyers are not legally privileged.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

It is generally advisable to check the insurance policy early on. Where required, a precautionary notification to insurance companies should be made as soon as possible, to avoid any subsequent refusal of cover on the basis that the matter was not notified on a timely basis.

b) To business partners (e.g. banks and creditors)?

Early notification to business partners will depend on the nature and subject matter of the investigation. Assessment on a case-by-case basis will be required.

c) To shareholders?

Directors typically owe duties to the company, rather than to shareholders. There may, however, be special circumstances where a duty could be owed to the shareholders, such that disclosure is required. For publicly listed companies, the Rules of the Irish Stock Exchange ("**ISE**") require that companies must, without delay, provide to it any information considered appropriate to protect investors. The ISE may, at any time, require such information to be published to protect investors, or to ensure the smooth operation of the market.

d) To authorities?

This will depend on the nature of, and subject matter of, the investigation. The company (or its senior management, including, in particular, any persons in "Pre-Approved Controlled Functions") may have specific mandatory reporting obligations to relevant regulator(s), including for example, to the Central Bank of Ireland, the Director of Corporate Enforcement, the Data Protection Commissioner, and/or the Competition and Consumer Protection Commissioner.

Where the investigation relates to a matter potentially involving certain fraud, corruption and/or company law offenses, a report to the Irish police under Section 19 of the Criminal Justice Act 2011 may be required.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Consideration should be given to whether any mandatory reporting requirements arise and steps should be taken to ensure the preservation of all relevant materials. Consideration should also be given to taking appropriate mitigation steps while the investigation is ongoing, including any necessary notification to any impacted third parties, e.g. to customers who are potentially impacted by an employee fraud.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Where an internal investigation and regulatory investigation are operating in tandem, it is generally advisable to maintain regular contact with the regulator to ensure that they are on board with the approach being taken in the internal investigation.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

In most cases, the Irish police will require a search warrant before searching premises, although there are statutory exceptions to this. Generally, search warrants are issued by District Court Judges.

The legal prerequisites which apply to regulators will depend on the statutory provisions under which they are appointed. Some regulators have statutory powers to conduct searches and "dawn raids" on business premises on foot of their warrant of appointment alone (without needing to apply to court for a specific permission to do so). However, a search warrant (granted by a court) may be required in certain circumstances, e.g. to search a private dwelling, seize original documents, and/or use reasonable force in connection with statutory search and seizure powers. A recent Irish Supreme Court decision held that the regulator must exercise its search powers in an appropriate and proportionate manner to ensure that, insofar as possible, only relevant material is seized for review and that where irrelevant material is seized, it should not be reviewed.

There is judicial discretion over whether to admit improperly gathered evidence. The Irish Supreme Court has held that evidence obtained unconstitutionally may still be admissible if the prosecution can establish that any breach of constitutional rights was due to inadvertence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

There is currently no general system for "non-prosecution agreements" or "deferred prosecution agreements" ("**DPAs**") in Ireland. A Cartel Immunity Program operates under Irish competition law, which has some of the features of DPAs. There is also no formal plea or bargaining system in Ireland, although plea bargaining does operate informally in practice.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

The range of penalties will depend on the specific conduct, but can potentially include fines and/or imprisonment following a successful criminal prosecution. Companies convicted of an offense may also be excluded from participating in public tenders. Compensation orders and adverse publicity orders can be made in some situations. Some regulators may also have civil enforcement powers, which they can deploy as an alternative to prosecution. Such powers may include requesting undertakings or issuing compliance notices.

In certain cases, where it is proved that an offense committed by a company has been committed with the "consent or connivance of", or was "attributable to any neglect" on the part of a director or officer of the company, the latter can also be found guilty, and subjected to the relevant applicable penalties. Directors can also potentially face "restriction" and/or "disqualification" for a set period of time and can be made personally liable for the debts of a company, in certain circumstances.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

The compliance system in place is likely be a relevant factor in mitigation of any penalty imposed on a company, its directors, officers, or employees. There is one instance where it could constitute a complete defense for a company: the Criminal Justice (Corruption Offenses) Act 2018 holds companies accountable by providing that a company may be liable to prosecution for corrupt acts by its director, manager, employee, agent, or subsidiary. The only defense available is for a company to show it "took all reasonable steps" and "exercised all due diligence" to prevent the corruption. The proposed Criminal Justice (Theft and Fraud Offenses) Amendment Bill provides for a new corporate offense of fraud affecting the financial interests of the European Union on similar terms regarding corporate liability and the available defense.

In the case of a corruption offense above, the defense would only apply where the efficient compliance system was implemented prior to the misconduct. Otherwise, it is likely that the Courts/Regulator would view the implementation of an effective compliance system as a mitigating factor, although greater weight is likely to be attached to one implemented prior to the misconduct.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

There is a general trend of increased regulatory activity and investigations in Ireland, which is, in turn, leading to an increase in internal investigations. In light of increased regulatory activities, it is expected that the Irish courts will continue to see applications for injunctions restraining investigative processes.

An apparent trend includes some agencies conducting initial interviews "under caution", i.e. the interviewee is cautioned that anything they say may be used in evidence against them, even where their status – whether a witness, subject, or a suspect – remains unclear.

Ireland adopted new anti-corruption legislation in mid-2018, which has made it much easier for the authorities to prosecute and secure convictions for corruption offenses. In early 2018, the government published a general scheme of draft legislation to establish the Office of the Director of Corporate Enforcement (which is currently within the Department of Business, Enterprise and Innovation) as a stand-alone commission structure to be called the "Corporate Enforcement Authority" with increased independence as well as new investigative tools to enforce company law.

In line with European legislation, the focus of regulators and law enforcement on money laundering and terrorist financing has grown in the past few years.

CONTACTS

A&L Goodbody

28 N Wall Quay, North Wall
Dublin 1
Ireland

Tel.: +353 1 649 2000
www.algoodbody.com

A&L Goodbody is a leading Irish corporate law firm with a dedicated and specialist Fraud and White Collar Crime team. We advise on managing relationships with regulators, corporate fraud & asset tracing, fraud investigations and the defense of criminal prosecutions. Our clients include Irish and international corporates, financial institutions and public bodies. We also represent boards, senior management and employees caught up in regulatory investigations. At all times, we strive to protect our clients from the reputational consequences that can flow from a criminal investigation.

We have extensive experience in dealing with regulators both in Ireland and abroad. In Ireland, we deal with all regulators including the Office of the Director of Corporate Enforcement (ODCE), the Data Protection Commissioner (DPC), the Environmental Protection Agency (EPA), the Garda National Economic Crime Bureau (GNECB), the Central Bank, the Competition Authority, the Revenue Commissioners and the Criminal Assets Bureau (CAB).

We regularly work with international law firms and other advisors in dealing with claims from regulators such as the Serious Fraud Office (SFO) in the United Kingdom, and in the United States, the Federal Bureau of Investigation (FBI), the Food & Drugs Administration (FDA) and the Department of Justice. We also have experience of dealing with various other regulatory authorities in a range of EU jurisdictions, Australia and Russia.

Kenan Furlong
Partner
A&L Goodbody
T +353 1 649 2260
kfurlong@algoodbody.com

Kenan Furlong is a partner in A&L Goodbody's Litigation and Dispute Resolution Department and is co-Head of the Fraud & White Collar Crime Unit. He advises clients on internal investigations, whistleblowing issues, dawn raids, and money laundering issues. He also advises clients on managing their relationships with various Irish regulators and the Garda National Economic Crime Bureau (GNECB). In addition he assists with investigations by foreign regulators such as the SFO, the IRS and the SEC.

Kate Harnett
Associate
A&L Goodbody
T +353 1 649 2128
kmharnett@algoodbody.com

Kate Harnett is an Associate in A&L Goodbody's Dispute Resolution Department and Fraud and White Collar team. Kate is an experienced criminal defense practitioner and also previously worked as a prosecutor in the Office of the Director of Public Prosecutions. Kate advises domestic and international clients in relation to compliance matters, various issues arising out of regulatory investigations and on managing their relationships and engagements with regulators.

Deirdre Roddy
Associate
A&L Goodbody
T +353 1 649 2568
droddy@algoodbody.com

Deirdre Roddy is an Associate in A&L Goodbody's IP & Technology Group. Deirdre has extensive experience in advising both domestic and international clients in relation to a variety of data protection issues, including data privacy policies, vetting, employee monitoring, direct marketing, data transfers, data protection audits, managing data access requests, consent, preparing for and responding to cyber-security incidents.

Bríd Nic Suibhne
Associate
A&L Goodbody
T +353 1 649 2274
bnicsuibhne@algoodbody.com

Bríd Nic Suibhne is an Associate in the firm's Employment Department. Brid advises a wide range of clients across a variety of business and industry sectors on all aspects of contentious, advisory and corporate employment matters. In particular, Brid is experienced in advising on employment disputes, workplace change, restructuring and industrial relations. Brid has worked on a number of high profile internal and external employee investigations for large organizations, as well as having represented clients in the Workplace Relations Commission, the Labor Court, the Circuit Court and the High Court.

Italy

Hogan Lovells Studio Legale

Francesca Rolla

Alessandro Borrello

Vincenzo Donadio

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X Administrative liability of companies.	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Italian law offers whistleblower protection both for individuals employed by public entities and private companies, providing that retaliatory and discriminatory measures against the whistleblower, including employment termination, are null and void.

Under the whistleblowing law (Law No. 179/2017), private companies' compliance plans, provided by Legislative Decree No. 231/2001 on corporate administrative liability ("**Decree 231**"), must include one or more channels enabling the detailed reporting of misconduct learned by employees at the workplace. These channels must shield the whistleblower's identity. Although there is no legal duty to follow-up on the whistleblower report with an internal audit, it is advisable to consider starting an investigation, especially in cases of serious misconduct.

If an employee submits a groundless report either intentional or grossly negligent, the company is entitled to sanction the relevant whistleblower.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Under Italian law, there is no obligation to inform and/or involve employee representative bodies before an internal investigation is initiated. In other words, the employer is free to launch an audit and investigation process at its discretion and within limits set by law.

b) According to the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), which entered into force on 25 May 2018, the Data Protection Officer ("**DPO**") shall be involved, properly and in a timely manner, in all issues which relate to the protection of personal data, therefore also when commencing internal investigations.

In principle, internal investigations do not have to be reported to the Italian Data Protection Authority ("**DPA**").

c) There is no obligation to inform and/or involve government authorities at the start of an internal investigation.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

There is no specific obligation for employees to participate in interviews. However, due to the general duties of diligence, obedience, and loyalty that apply to the employment relationship, the employee is expected to cooperate as part of their job duties. If the employee refuses to participate in the investigation, their refusal may be considered a breach of their obligations, which may justify the beginning of disciplinary procedures (which may end with a disciplinary sanction if the relevant requirements are met).

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Employers should initiate an investigation as soon as they become aware of any potential misconduct and/or wrongdoing. If an employee's misconduct emerges from the internal investigation, the employer must immediately start disciplinary procedures in compliance with the so-called promptness principle for disciplinary actions. The timing may vary depending on, among other factors, the severity of the conduct and the number of people involved. At the end of the disciplinary procedure, the employer may impose sanctions, including dismissal for just cause.

Italian law does not provide any specific guidance with regard to the upper limit of the promptness principle. What is crucial is that the disciplinary action is started as soon as the employer has been made aware of the employee's misconduct and has collected sufficient evidence to start a disciplinary procedure. In some cases, disciplinary proceedings began six months after the start of an investigation were held by courts to comply with the promptness principle, as the time was deemed necessary to investigate and ascertain the employee's misconduct.

Moreover, once a disciplinary procedure has been commenced and the employee has exercised their right to be heard, the relevant sanction (if any) must be imposed within the strict deadline set out by the applicable Collective Bargaining agreement.

If the employer does not act promptly, there is a concrete risk – where the employee challenges the sanction – that a judge might identify such delay as tacit acceptance of the employee's conduct and declare the sanction unlawful.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

The Privacy Laws (Legislative Decree No. 196 of 30 June 2003 "**Privacy Code**", as amended following the entry into force of the GDPR, and the GDPR itself) apply to any processing of personal data. If the interview requires the collection of and/or any other processing of personal data, such as the preparation of reports and/or notes, it is advisable to assess how these activities are carried out in this respect (including issuing privacy notices to the relevant employees, etc.).

In any case, when performing internal investigations, companies must comply with the general principles of data processing set out in Article 5 of the GDPR (i.e. lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality).

b) Reviewing emails?

Private communication is protected by the Italian Constitution. The unauthorized and unlawful review of private communication constitutes a criminal offense punishable by up to four years' imprisonment (up to five years' for offenses committed against a public authority system).

In the employment relationship, however, the review of emails is allowed under Article 4 of Law 300 of 20 May 1970, provided that the email use is related to the employment relationship. According to the DPA, it is therefore advisable to explicitly mention the lack of confidentiality of communications within internal policies. If there are no specific policies in this context, the employee and/or third parties may reasonably expect certain types of communication to be treated as confidential.

Review of emails must, in any case, be carried out without being excessive. The process must be proportionate, in accordance with data protection principles. In addition, employees may exercise their rights under the Privacy Laws, including, for example, the right of access, rectification, and, subject to specific conditions, the right to object and erasure. In specific circumstances set forth by the Privacy Laws, the abovementioned rights may be limited.

c) Collecting (electronic) documents and/or other information?

The collection of documents and other information related to the employment relationship, whether for legal or organizational reasons, is not subject to any particular restriction. The collection, however, cannot exceed the purposes related to the employment relationship and must comply with an obligation imposed by law or regulation. Such information shall be gathered and treated in compliance with the provisions of the Privacy Laws. In this context, it is worth mentioning a recent decision issued by the DPA against a company that – instead of deactivating a terminated employee's corporate email account - used an email received by the employee on the deactivated account one year after the termination as evidence in court proceedings. The DPA found the procedures adopted by the company to be unlawful because they did not comply with data protection principles, which require the employer to protect the confidentiality of a former employee as well.

Finally, the Privacy Laws apply to any document containing personal data of the employee. With respect to the processing of such documents, employees may exercise the rights granted by the Privacy Laws, as mentioned above in 5b.

d) Analyzing accounting and/or other mere business databases?

If such accounting and/or business database include personal data, the Privacy Laws shall apply.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

As long as the interview is conducted in compliance with applicable employment and privacy law provisions (e.g. the employee has received a privacy notice illustrating their rights under the Privacy Laws), there is no legal obligation to inform the employee about the legal circumstances. However, providing information on the subject matter and a brief description of the investigation may be ethically necessary and advisable. For documentation purposes, it is advisable to provide these instructions in writing to be signed by the interviewee.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

This is not mandatory under Italian law. If the interview is designed to collect facts and not to challenge wrongdoings (meaning that the purpose of the interview is merely gathering facts and not accusing the interviewee), the employee is free to make any statements that they deems relevant for this purpose. If the employer learns of any misconduct during the interview, this must be dealt with by way of a dedicated disciplinary procedure.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

If the interview is conducted and/or attended by a third party (e.g. a lawyer), the employer should explain to the employee the role of that third party, in compliance with the general principle of good faith and fairness. Therefore, if a lawyer takes part in the interview, the company should disclose their role.

d) Be informed that they have the right that their lawyer attends?

As mentioned above, the purpose of the interview is to collect facts. The employee's participation in the interview thus falls within their job duties. Accordingly, there is no strict obligation to allow the employee to be accompanied by a lawyer. However, if the company is assisted by a lawyer, and the employee asks for the same right to be granted, the company could evaluate whether such participation would allow for a fair set-up and avoid an unbalanced situation.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Similarly, there is no provision for the employee to be accompanied by a representative of the works council or another representative body. Representatives of works councils or trade unions can only assist employees in disciplinary proceedings.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

According to the Privacy Laws, the interviewee needs to be informed about any transfer of personal data as well as the legal basis for such transfers. Consent to a cross-border transfer is not required if the transfer is legally covered. In particular, the Privacy Laws allow the transfer of personal data outside the European Union if the transfer is necessary to defend a legal claim or if the company has taken appropriate security precautions to protect the transferred data, e.g. Binding Corporate Rules, Standard Contractual Clauses, Privacy Shield (for the United States only), or an adequacy decision issued by the European Commission for a specific country.

g) Sign a data privacy waiver?

Data subjects must be informed about the methods and purposes of the data processing, including their rights. In certain cases, employees must give informed, voluntarily, and specific consent.

h) Be informed that the information gathered might be passed on to authorities?

According to the Privacy Laws, data subjects (i.e. employees) should be provided in the privacy notice with information regarding potential recipients or categories of recipients of their personal data.

i) Be informed that written notes will be taken?

For reasons of transparency, it is advisable to inform the employee that written notes will be taken. Furthermore, if such written notes involve the processing of personal data (e.g. the notes mention the names of interviewed employees), the Privacy Laws and all related principles apply to these notes (e.g. the data retention period, which is determined by the company in light of the purposes for which such data was originally collected).

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Document hold notices and retention policies are allowed in Italy, although there is no specific rule that must be observed.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

There is no general concept of legal privilege in Italy. However, according to civil and criminal law and the code of conduct of the Italian Bar, lawyers who are members of the Bar are obliged to maintain professional secrecy about

any information they receive during their work for their clients. If criminal proceedings are pending, greater privilege protection can be achieved by appointing legal counsel in accordance with the rules of the Criminal Procedure Code.

In these cases, to ensure the highest privilege protection, investigation reports and legal memos should be prepared by the appointed outside legal counsel, kept at their office, and labelled as "*Legally privileged and confidential*". Investigation reports and documents collected during an internal investigation, if kept at the company's premises, could be seized by enforcement authorities (e.g. the public prosecutor), as in-house counsel cannot assert legal privilege.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

In-house counsel do not benefit from the attorney-client privilege.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There are no legal provisions requiring early notification to insurance companies. This should, however, be assessed in accordance with the provisions of the insurance contract. Notification may be appropriate under certain circumstances, for instance, if the D&O policy covers internal investigations.

b) To business partners (e.g. banks and creditors)?

There is no explicit requirement to inform business partners about internal investigations. However, there is a general obligation under Italian law to perform contracts in good faith. The initiation of an internal investigation could constitute relevant information for the other party with regard to the purpose of the contract. Therefore, the possibility of notifying business partners should be assessed on a case-by-case basis.

c) To shareholders?

Although there is no legal duty to inform shareholders that an internal investigation is starting, the decision to provide early notification should be assessed on a case-by-case basis and depends on the seriousness of the alleged misconduct.

d) To authorities?

There is no general obligation to inform public authorities.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

A company should minimize the damage and try to avoid committing other offenses similar to those committed by its employees. Accordingly, when significant misconduct is discovered, the company should also consider reviewing and amending its compliance plan and taking all necessary and specific measures.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Prosecutors are, generally, not informed about internal investigations and, therefore, do not ask for specific steps to be observed.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Both search warrants and dawn raids in criminal proceedings must comply with the formal and material requirements of the Italian Criminal Procedure Code. They can only be carried out if there is a concrete reason to believe that specific things relevant to the alleged criminal offense can be retrieved.

Search warrants can only be executed by order of the Public Prosecutor and in accordance with the conditions of the Italian Criminal Code. In exceptional cases, where it is necessary and urgent, the police can take provisional measures to seize items, which are sent to the judge for confirmation within 48 hours. If this confirmation is not given within 48 hours, the provisional measures shall be revoked and considered null and void.

Evidence gathered in violation of relevant rules set forth by the Italian Criminal Code may not be used in the criminal trial, except when such evidence amounts to the *corpus delicti*.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Italian law does not provide for non-prosecution or deferred prosecution agreements for individuals or corporations. Under Italian law, however, the prosecutor and the defendant (including corporations) can enter into a plea bargain, even during preliminary investigations.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Decree 231 introduced corporate administrative liability for offenses listed in Decree 231 and committed by leadership in the interest, or for the benefit of, the company.

If a company is held liable under Decree 231, it may be fined according to the seriousness of the offense (up to around €1.5 million) and/or be subject to interdictory sanctions (such as debarment from exercising activity and disqualification from contracting with the public administration), confiscation, and publication of the court's decision.

The penalties for individuals vary depending on the type of offense committed and can include imprisonment, monetary fines, and interdictory sanctions.

Furthermore, both companies and their employees can be held liable for damages under civil law by those who have been injured by the misconduct.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

According to Decree 231, the company is exempted from liability if it has implemented – prior to the perpetration of the alleged misconduct contemplated by Decree 231 – a compliance plan under Decree 231 (a "**231 Plan**") which includes, among other things, the appointment of an *ad hoc* Surveillance Body ("**SB**"). The SB is an autonomous, independent body that oversees the implementation and updating of the 231 Plan.

Moreover, the company can mitigate its potential liability if it demonstrates that – following the perpetration of the relevant offense contemplated by Decree 231 – it has implemented an appropriate 231 Plan in order to prevent that the committed offense is perpetrated again. Accordingly, failure to take action following a compliance breach could prevent the company from relying on this defense.

Implementation of an efficient 231 Plan does not *per se* entail suspension or reduction of penalties for the relevant company's directors, officers, or employees. In this context, it cannot be excluded that failure by the members of the board of directors, officers, or employees to take action in light of suspected compliance failures may lead to

personal civil and/or criminal liability for those individuals (e.g. because the directors could be deemed to have failed to discharge their duties to the company).

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

By decision no. 11626 of 7 April 2020, the Italian Supreme Court of Cassation – following the principle established by lower courts – ruled that even foreign companies whose registered office is located outside Italy are subject to Italian jurisdiction and can be held liable under Decree 231 for offenses committed in Italy by their directors, officers, or employees in the interest, or for the benefit, of the foreign company. Therefore, the establishment of compliance systems pursuant to the laws of the country where the company has its registered office might no longer be sufficient to avoid corporate administrative liability under Decree 231 in Italy.

Foreign companies operating in Italy (even if only occasionally or through branches) should thus consider to adopt a 231 Plan or implement their current compliance policies and procedures in order to ensure their adequacy to prevent that crimes listed in Decree 231 are performed in Italy.

In July 2020, the Italian Government issued the Legislative Decree no. 75/2020, implementing Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law. The Decree introduced a new set of tax crimes that can lead to corporate administrative liability under Decree 231.

CONTACTS

Via Santa Maria alla Porta, 2
20123 Milan
Italy

Tel.: +39 02 7202521
Fax: +39 02 72025252
www.hoganlovells.com

Francesca Rolla
Partner
Hogan Lovells Milan
T +39 02 7202521
francesca.rolla@hoganlovells.com

Francesca Rolla is a Partner at Hogan Lovells, founder of the Italian Litigation practice and head of the Investigations White Collar Crimes and Fraud team in Italy. With almost 30 years of experience as a litigator, Francesca represents international and Italian clients in product liability and tort disputes and advises on product safety and compliance issues, as well as on internal investigations. In respect of Investigations and White Collar Crime, she leads a team specifically dedicated to advising clients on how to avoid the legal, commercial and reputational risks posed by investigations and prosecutions. Francesca assists in handling internal investigations and investigations by criminal or other public authorities, coordinating the work of criminal counsels and external experts.

Alessandro Borrello
Senior Associate
Hogan Lovells Milan
T +39 02 7202521
alessandro.borrello@hoganlovells.com

Alessandro Borrello is a Senior Associate in the Italian Litigation, Arbitration and Investigations practice at Hogan Lovells. His work is mainly focused on domestic and cross-border litigation and internal investigations, across various industry sectors.

Being a key member of the Investigations, White Collar Crimes & Fraud group in Italy, he regularly works as project manager in the context of internal investigations and provides targeted advice to clients on solutions to mitigate legal, commercial, and reputational risks posed by investigations and prosecutions.

Vincenzo Donadio
Associate
Hogan Lovells Milan
T +39 02 7202521
vincenzo.donadio@hoganlovells.com

Vincenzo Donadio in an Associate in the Italian Litigation, Arbitration and Investigations practice at Hogan Lovells. His work is mainly focused on commercial litigation, product liability and internal investigations, assisting international and domestic clients operating in various industry sectors such as technology and life sciences.

Being a member of the Investigations, White Collar and Fraud group in Italy, he regularly assists clients in the context of internal investigations providing advice to mitigate legal, commercial and reputational risks posed by investigations and prosecutions.

Latvia

Ellex Klavins

Irina Kostina

Edvijs Zandars

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes		X	X	X	X
No	X No criminal liability of legal persons, but "coercive measures" (e.g. liquidation) possible in case of criminal conduct by employees. Administrative liability of corporations is possible.				

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

The Whistleblower Act came into effect on 1st May 2019. It states that business entities that have more than 50 employees must create an internal whistleblowing system prescribing procedures for how employees and contractors can report on possible breaches and how the reports of whistleblowers are handled.

The Whistleblower Act states that it is an obligation of the employer to guarantee protection of a whistleblower, as well as their relatives, for example, protection of identity, protection against adverse effects caused due to whistleblowing, etc.

The Labor Act prohibits employers from punishing or otherwise, directly or indirectly, subjecting employees to negative consequences, should employees report suspicions about criminal offenses or administrative violations at the workplace to competent authorities or officials.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Employee representative bodies do not have a legal right to be informed about or participate in internal investigations. However, the employer may, in its discretion, choose to inform such bodies. In practice, if there is a works council in a company, it is often recommended to inform it about an investigation, although there is no formal process for this.

b) Although a data protection officer should be well informed about personal data processing in the company, there is no statutory requirement to involve or inform them about an investigation, although it may be recommended to avoid possible unjustified intrusion in data subject's private life.

c) There is no legal requirement to inform local authorities about the start of an internal investigation. However, if, in accordance with the law, a serious (e.g. intentional serious bodily injury) or especially serious crime (e.g. death following such injury) had to be reported to the competent authorities, but a person has failed to do so, the Criminal Act provides for liability for failure to comply with this duty. There are also special provisions that provide a duty to report certain conduct to authorities (e.g. environmental pollution, money laundering).

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees do not have a duty to support an investigation and, therefore, cannot be disciplined for failure to cooperate. However, there is a duty of an employee to perform their employment duties. An employee is required, if asked, to provide the employer with information regarding the performance of job duties. Nevertheless, it is not possible to force the employee to provide information about other employees.

The employer may impose disciplinary measures on the employee if the employee has failed to perform their duties or has not provided complete information about the performance of the job duties.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

No, Labor Act deadlines are initiated or employee sanctioning rights waived by investigation actions.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

General data protection rules arising from the General Data Protection Regulation ("**GDPR**") should be taken into account before conducting interviews, including the obligation of the data controller (i.e. the person who organizes the investigation, most commonly the employer) to ensure that personal data of all parties are processed strictly for the purpose of the investigation, are proportional and that only duly authorized persons have access to such personal data. Information must also be provided to employees concerning the purpose of the data processing.

b) Reviewing emails?

General data protection rules should be taken into account before reviewing emails.

c) Collecting (electronic) documents and/or other information?

General data protection rules apply to the collection of any documents that may contain personal data. In addition, please note that Latvia does not have a blocking statute regime.

d) Analyzing accounting and/or other mere business databases?

General data protection rules apply. If there is no personal data involved, the data processing rules do not apply.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no legal obligation to provide the employee with written instructions. However, a company's internal whistleblowing policy could provide such an obligation.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

Employees do not have an obligation to answer questions during an internal interview. It is advisable to remind the employee that they have no obligation to give any information that could be self-incriminating.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no legal obligation to provide the employee with such a warning and the Whistleblower Protection Act is silent on this matter. However, the employer should inform the employee who will participate in the interview and the basis for their participation.

d) Be informed that they have the right that their lawyer attends?

There is no legal obligation to inform the employee of the right to counsel and the Whistleblower Protection Act is silent on this matter. However, it is advisable to inform the employee of their right to legal assistance and in any case the employee has a right to invite their attorney-at-law (the qualified lawyer admitted to the Latvian Bar Association).

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is no legal obligation to inform the employee of the right to have an employee representative attend the interview. As the employee has the right to ask an employee representative to attend the interview, it is advisable to inform the employee accordingly.

The Whistleblower Protection Act only states that the representatives of employees have the right to provide support to the whistleblower. The Labor Act provides general rights for employee representatives to obtain information and consult with the employer before the employer takes decisions which may affect the interests of employees. Consequently, the employee representative would, in general, be entitled to participate at such meetings.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

General data protection rules should be taken into account in regard to the cross-border transfer of personal data. Article 13 and 14 of the GDPR stipulates what information must be provided to the data subject before the processing of personal data has commenced. Among other information, the data subject must be informed of data recipients and of the fact that the data controller intends to transfer personal data to a third country (outside the European Economic Area) together with an indication of appropriate safeguards used.

g) Sign a data privacy waiver?

Based on general data protection rules, in employment relationships it is difficult to ensure that consent of the employee is given freely, thus consent should not be used as a legal basis for personal data processing. Instead, other legal bases e.g. to perform agreement, to comply with legal obligations or if processing is necessary for the purposes of legitimate interests pursued by the employer, should be used.

h) Be informed that the information gathered might be passed on to authorities?

Except when disclosure is requested by authorities according to law, individuals must be informed about recipients of the data, including that information may be passed on to authorities, if the information is acquired from the respective employee. In case the information gathered has not been obtained from the respective employee, Article 14 of the GDPR allows not to inform the data subject if provision of such information could impair the achievement of the objectives of the data processing e.g. the investigation.

i) Be informed that written notes will be taken?

There is no legal obligation to specifically inform the employee that written notes will be taken during the interview (as long as the employee is informed of the data processing itself). However, notes or minutes of an interview may only serve as valid evidence if all participants sign the notes or minutes, confirming the accuracy of the information contained therein.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no law establishing the admissibility of document hold or retention notices in Latvia. Therefore, document hold notices in private relations are admissible and are regulated by the company's internal policies.

The Act on Accounting, the Archives Act, and other laws set mandatory retention periods for certain types of documents, while the GDPR requires that personal data be retained no longer than necessary for the specific purpose. Since there are no specific retention periods indicated for information collected during an investigation, such information must be retained no longer than necessary for the purpose for which it was collected.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege applies exclusively to information provided by the client to the attorney-at-law. The attorney-at-law may not disclose the secrets of their client, even after the case is closed or the attorney-at-law has been released from handling the case. A report prepared by an attorney-at-law for the client in connection with an internal investigation led by the attorney-at-law would be protected from disclosure by the attorney-client privilege. Nevertheless, the client may be obliged to inform the authorities of potential criminal conduct uncovered by the report, without disclosing the report itself. It is generally advisable to involve outside counsel (attorney-at-law) in internal investigations to ensure investigation findings are protected by the attorney-client privilege.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

The attorney-client privilege does not apply to in-house counsel. An attorney is understood to be a person who is an attorney-at-law or attorney-at-law assistant and has been admitted to the Latvian Bar Association or who has a right to practice in Latvia in accordance with EU laws.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Early notification to the insurance company on starting of investigation is only necessary if required by the insurance policy.

b) To business partners (e.g. banks and creditors)?

There is no statutory obligation to inform business partners about the start of an investigation. However, credit and financial institutions have an obligation to report unusual and suspicious transactions in accordance with the requirements of the Act on Prevention of Legalization of Proceeds from Crime and Terrorism Financing and Proliferation Financing.

c) To shareholders?

There is no legal obligation to inform shareholders about the start of an investigation, but the company's internal policies may provide such an obligation. Article 194 of the Commercial Act provides shareholders the right to be informed regarding the activities of the company and to become acquainted with all of the company's documents.

d) To authorities?

There is no legal obligation to inform the authorities of the start of an investigation. In certain cases, everyone has a duty to report criminal offenses or administrative violations.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

As there is no law governing the conduct of internal investigations, there are no specific measures that legally must be taken once an investigation has started, other than the observance of the Whistleblower Act and data protection laws. Moreover, if a breach of law is detected, the company must take measures to stop the misconduct and to either prevent or minimize potential liability.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Internal investigations are outside the scope of competence of prosecutors, who are only concerned with criminal matters in the context of criminal investigations. However, it is crucial that the company does not destroy any potential evidence during the course of its internal investigation. Furthermore, if a serious or especially serious crime is detected, the company should report it.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Typically, a valid criminal search warrant requires initiation of a criminal procedure and court approval. In emergency cases where, due to a delay, objects or documents may be destroyed, hidden, or damaged, a search may be performed with the decision of the person directing the proceedings or, in case the decision is taken by the investigator, with the consent of a public prosecutor. If the prerequisites are not fulfilled (in criminal liability matters) the gathered evidence may not be admissible.

As regards to administrative liability, "dawn raids" may be initiated by various authorities with slightly different prerequisites. For example, in order to carry out a dawn raid, the Competition Council must obtain a court order where the subject and purpose of the inspection; the assets, information, and documents to be searched for; and the timeframe for performing procedural actions are specified.

By contrast, the police and similar authorities must initiate an administrative violation procedure and either obtain the consent of the property owner or a court order (or the consent of the prosecutor) in order to perform an on-site inspection. The presence of the property owner (or its representative) or a representative of the municipality is required. If the prerequisites are not fulfilled (in administrative liability matters) the gathered evidence may not be admissible, unless the deviation from the requirements was minor.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Although a corporation may face so-called "coercive measures" when its employees have engaged in criminal conduct, legal persons are not subject to criminal liability under the Criminal Procedure Code. Legal persons may,

however, be liable for violations of the Latvian Administrative Violations Code. Settlements with regulators in administrative cases are common for corporations.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

The Criminal Act provides for the following "coercive measures", which can be taken against a legal entity when its employees have engaged in criminal conduct: liquidation, limitation of rights, confiscation of property, and levy. Penalties under the Criminal Act for natural persons depend on the crime committed. For instance, an employee acting as an intermediary for bribery could face up to five years' imprisonment, community service or a fine. Certain criminal offenses, e.g. engagement in a prohibited business, may lead to a prohibition of business activity and a ban on holding certain offices.

The most common type of penalty for administrative violations is a fine. For example, members of the management board of a legal entity may be fined for tax debts to the company. Members of the management board of a legal entity may also be held criminally liable, for instance, for evasion of tax payments. Pursuant to the Criminal Act, in such cases fine or even imprisonment could be applied.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

A reduction of penalties is unlikely, as the authority may assume that, if there is a compliance system in place at the company and a director, officer, or an employee, nevertheless, has perpetrated any misconduct, this system does not work properly. The fact that there is the compliance system in the company which was not observed and despite of which the misconduct was perpetrated, might be considered to be an aggravating factor to some extent.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The Whistleblower Act came into effect on 1st May 2019 which is a new development for providing an effective compliance system for the companies. The companies which have more than 50 employees have a duty to organize an internal whistleblowing system at the company and provide a clear regulation on how whistleblowers' reports have to be reviewed, timelines for such review, and which persons may participate in the investigation etc. Of course, companies with fewer employees also are encouraged to create such a system.

This is definitely something new for the companies and since the Act has been in force for less than a year it is difficult to predict how effective it would be, nevertheless, it is observed on the market, and the companies pay more and more attention to the corporate compliance issues. Therefore, it is likely that the proper internal investigations also will become an integral part of the internal compliance systems.

CONTACTS

K.Valdemara 62
1013 Riga
Latvia

Tel.: +371 67814848
Fax: +371 67814849
www.ellex.lv

Irina Kostina
Associate Partner
Head of Employment Law Practice
Ellex Klavins
T +371 67814862
irina.kostina@ellex.lv

Irina Kostina is the Head of Employment Law Practice. She has more than 15 years of legal experience specializing in various employment and dispute resolution matters. Irina is an expert on sensitive management and key employee termination and complex multi-jurisdictional transfer of undertakings issues. Irina represents corporate clients in the court proceedings in disputes with their former or current employees and in front of the supervisory state institutions, as well as advices clients. Irina has extensive experience on consulting clients regarding the inspections performed by controlling institutions, initiated administrative cases and appeals on its decisions in court. Irina's experience includes also representation of numerous clients in civil and administrative cases in local courts and in arbitration on different contractual and corporate matters. She also advises and represents clients in relation to recognition and enforcement of foreign court rulings and arbitral awards, assists in collection of evidence and cooperates with state bailiffs in the execution stage.

Edvijs Zandars
Senior Associate
Ellex Klavins
T +371 67350550
edvijs.zandars@ellex.lv

Edvijs Zandars specializes in Competition Law, Information Technology, Intellectual Property and Data Protection. He regularly advises clients in all product life cycle stages and has broad experience in introducing various software products, telecommunications equipment and consumer goods to the local market. Edvijs is also proficient in data protection matters and provides assistance to data controllers and processors in fulfillment of requirements by the Latvian and EU Law. He also has significant experience in advising international and local clients on protection and enforcement of intellectual property rights and other regulatory matters.

Liechtenstein

Gasser Partner Rechtsanwälte

M.A. HSG Thomas Nigg, LL.M.

Mag. iur. Johannes Sander

Overview

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X See § 63 *et seq*. of the StGB.	X
No					

Question List

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Although there is still no specific whistleblower protection law in Liechtenstein, the Financial Market Authority ("**FMA**") created an external platform based on Articles 4 and 5 of the Financial Market Authority Act. The whistleblower platform serves as protection for whistleblowers, who report potential or actual violations, in order to effectively combat abuse and better protect clients of Liechtenstein's financial center (cf. also Article 28a of the Due Diligence Act, the "**DDA**"). The platform was set up in order to bring Liechtenstein in compliance with European financial market regulations.

These reports can be made to the FMA either online or via post and may be anonymous. After reviewing the report, the FMA may contact the whistleblower to obtain additional information if necessary and provided that the identity is known. Reports that do not fall within the scope of the FMA's legal competences are forwarded to the competent authority (e.g. allegations of criminal conduct are forwarded to the prosecutor's office).

With respect to internal whistleblowing, Article 28a(3) of the DDA states, for instance, that companies subject to the DDA with more than 100 employees must establish an internal, anonymous reporting procedure for whistleblower complaints. However, the law does not provide guidance on the content of the internal process. A duty to investigate such internal reports will usually be included in internal compliance guidelines and is incumbent upon the management of a company. However, a whistleblower does not have to be informed of the outcome of the investigation.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

First of all, one must clarify that a specific (legal) concept of internal investigations, which may perhaps exist in other countries, does not exist in Liechtenstein. Potential internal wrongdoings are investigated based on internal guidelines.

a) Public and private labor law provides for employee representatives/employee representative bodies. These mainly deal with abusive wage payments, health protection issues, or mass redundancies (see Article 45 of the Labor Law). The law does not require that an employee representative body be advised of internal (whistleblower) investigations.

b) According to Article 13a of the Data Protection Ordinance ("**DSV**"), the data protection officer ("**DPO**") must have access to all information necessary to fulfill their duties, which includes monitoring the use of personal data and remedying data privacy violations. In addition, the DPO must maintain a data collection list and provide it to the data protection authority or persons concerned upon request. Therefore, the company, in general, has to inform the DPO about all data privacy related procedures, including process of an internal investigation.

c) With respect to internal investigations, local authorities do not have a specific right to be informed. However, in some cases it might be useful to involve them on a voluntary basis.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

There are no explicit provisions concerning the participation of employees in internal investigations. However, according to labor laws, employees have to act in the employer's interest, which may – based on a case-by-case basis – include the duty to cooperate in and/or contribute to internal investigations to the extent it concerns their profession and/or area of work. If the employee refuses to participate in the investigation, their behavior potentially qualifies as professional misconduct and may provide ground for the termination of the employment.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

If an employer obtains knowledge of relevant facts which could lead to an immediate dismissal, the employer must immediately dismiss the employee without notice otherwise the employer forfeits the right to do so. There is no specific deadline, but in principle, the terminating party must declare the termination as soon as the reason for termination has come to his knowledge. An appropriate period for consideration is usually two to three working days and, in exceptional cases, one week. A "serious" suspicion of professional misconduct satisfies the knowledge prerequisite. Therefore, it is critical to know at which point during an investigation a suspicion becomes "serious". Except for cases of immediate dismissal, no other labor law deadlines are triggered or rights waived by investigative actions.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

By Resolution of 10 July 2018, the General Data Protection Regulation ("**GDPR**") was adopted to the general acquis of the European Economic Area. Since 20 July 2018, it is applicable in Liechtenstein. The GDPR governs any processing of personal data wholly or partly by automated means and any other processing of personal data which form or are intended to form part of a filing system (cf. Article 2 GDPR). Labor law allows for the processing of employment related information if it is necessary to fulfill the employer's duties. This naturally includes protocols of employee interviews. However, processing and sharing data within the company and/or company group is only allowed within the boundaries of the GDPR.

b) Reviewing emails?

The Department for Economics (*Amt für Volkswirtschaft*) released guidelines for the surveillance of employees. However, the latest version is dated February 2018 and therefore does not include the GDPR. According to Article 88 GDPR and Article 1173a § 28a Liechtenstein Civil Code, the processing of employee's data is admissible in order to conduct and fulfill the employment contract. Whether the general surveillance of employees is admissible, especially having regard to the principle of proportionality and reasonableness, has not been tested in court. Further, it depends on the facts of each case. For example, as German literature suggests, it may make a difference whether the employee is allowed to use their email for private purposes also.

c) Collecting (electronic) documents and/or other information?

In principle, the same applies to collecting (electronic) documents and/or information. However, since (electronic) documents usually do not contain "private by-catch information", the issue is probably less of a practical concern. Provided that the employer and/or employee can demonstrate a justified interest in collecting documents, it may be admissible according to the GDPR. In our opinion, collecting data that assist in uncovering an infringement or violation of legal duties should be justified as the GDPR does not intend to cover-up professional misconduct.

d) Analyzing accounting and/or other mere business databases?

Analyzing accounting and business databases may be regarded as "processing" under GDPR. However, the GDPR only protects personal data of natural persons. Analyzing accounting and business databases is, therefore, not covered by the GDPR regime.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no legal obligation to give written instructions to employees before internal interviews.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

Under the Criminal Procedure Act of Liechtenstein, a suspect has the right to remain silent during interrogations by criminal authorities and in criminal proceedings in general. However, there is no corresponding "right" or "duty" with regard to employee interviews as part of an internal investigation.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

In Liechtenstein, there is no legal obligation to give an employee an Upjohn warning. However, the warning is, in practice, commonly given. According to the Liechtenstein Bar Association, lawyers are not allowed to represent more than one client in the same matter. Although they are not obliged to inform the employees of this fact, it is generally good practice to do so.

d) Be informed that they have the right that their lawyer attends?

There are no explicit provisions concerning the duty to inform an employee of their right to have a lawyer present during an internal interview.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

As already mentioned, there is no law in Liechtenstein regarding internal investigations. Such internal investigations are subject to and follow internal guidelines. Hence, internal guidelines must be checked to see if the employee has a right to have a works council representative attend the interview.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Since the GDPR is applicable, its provisions on sharing and transferring data cross-border need to be considered. Transferring data falls within the term "processing data", which is why the general preconditions for processing data must be fulfilled (Article 6 GDPR). Provided that processing data, including the transfer to third countries according to Chapter V GDPR is admissible, the employee does not have to be informed specifically.

g) Sign a data privacy waiver?

As outlined at question 5b, we are of the opinion that collecting data for whistleblower purposes and/or for uncovering illegal activities within the boundaries of proportionality and reasonableness is admissible irrespective of the consent of the individual. The GDPR does not serve to cover illegal misconduct. As a consequence, we are of the opinion that a privacy waiver is neither necessary, nor is it necessary to inform the employee about a privacy waiver. However, this has not been subject to a decision by the Data Protection Authority or a court in Liechtenstein. Therefore, these remarks merely represent the view of the authors. Due to the lack of case law or decision of the Data Protection Authority, there is no claim to completeness.

h) Be informed that the information gathered might be passed on to authorities?

There is no legal obligation to inform the interviewee that the information gathered might be passed on to authorities. However, it is advisable to inform about the possibility.

i) Be informed that written notes will be taken?

There is no legal obligation to inform employees that written notes will be taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

With respect to this matter, there are no statutory provisions concerning document hold notices or document-retention notices in Liechtenstein nor is there any published case law in this regard.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

According to Article 15 of the Lawyers Act ("**RAG**"), attorneys-at-law are bound to secrecy concerning all issues related to their profession that are of interest for their clients. The right of an attorney-at-law to secrecy may not be circumvented by judicial or other official measures and attorney-client privilege is not waived, even if a privileged correspondence is found outside of the attorney-at-law's custody (Article 15 (2) and (3) RAG).

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Provisions regarding attorney-client privilege are only applicable to attorneys-at-law. Correspondence and documents of in-house counsel are not included in the scope of RAG. Nonetheless, in-house counsel bears a duty of confidentiality, resulting from the general duty of trust and loyalty to an employer. According to case law, the seizure of records of attorneys-at-law is forbidden, but this does not include documents written, gathered or possessed by an in-house counsel. In order to ensure privilege protection, it is therefore recommended to involve outside counsel (attorneys-at-law).

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Possible reporting obligations may only arise from the insurance policy itself or general contractual duties of care and loyalty.

b) To business partners (e.g. banks and creditors)?

Information duties may only arise from contractual obligations between the company and the business partner.

c) To shareholders?

Internal investigations, depending on their subject matter and scope, may relate to insider information that could possibly influence stock prices. According to Article 5a of the Market Abuse Act, an issuer of financial instruments has to disclose to the public insider information that may affect the price of such instruments as soon as possible. Therefore, it is important to evaluate on a case-by-case basis if there is an obligation to report to the shareholders.

d) To authorities?

There is no general legal obligation to inform authorities about an internal investigation. However, taking into account one's own potential liability (e.g. omission or assistance), certain criminal offenses should be reported to the public prosecutor and other statues require that government/supervisory authorities be notified of certain circumstances.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Although there are no statutory obligations on companies with respect to internal investigations, a company should stop any criminal conduct of employees as soon as it becomes aware of the conduct and take steps to minimize damages. If employees are affected, this will be of the utmost importance for the company.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutors do not generally play a role in internal investigations. However, it is important that a company does not destroy any relevant information or evidence during an internal investigation. This could become relevant if certain criminal offenses are later reported to the public prosecutor.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

There are formal and material prerequisites set forth in the Criminal Procedure Act ("**StPO**"), which have to be met in order to have a valid search warrant or to conduct a legitimate dawn raid.

A search warrant is usually initiated upon motion of the public prosecutor and ordered by a court. A search warrant must be based on exigent circumstances or a reasonable suspicion that a person suspected of a crime, or an item used for committing a crime, can be found (see Article 91a and 98 *et seq*. of the StPO).

Competent supervisory authorities may carry out extraordinary on-site visits within the framework of the DDA (see Article 28(1)(c)).

According to the judgment of the Austrian Supreme Court, illegally gathered evidence may still be used in court proceedings, unless expressly prohibited by law. According to the Liechtenstein State Court, the same applies in Liechtenstein.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Only under certain circumstances set forth in the StPO may deals and non-prosecution agreements between the court or the public prosecutor's office and a corporation be reached in association criminal proceedings (*Verbandsstrafverfahren*).

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

The liability of legal entities is regulated under Article 74a *et seq*. of StPO. Legal entities are responsible for the offenses and crimes committed by managers and directors, which are culpably committed in the performance of business activities. However, a legal person should only be responsible for the offenses of regular (i.e. non-managerial) employees, even if the offense was not culpably committed, where the commission of the offense was made possible or substantially facilitated by the failure of the managers to take necessary and reasonable measures to prevent such offenses.

Typical criminal penalties that result from misconduct of individuals are fines, disgorgement of proceeds or, in the case of executives, imprisonment. Depending on the nature of the business or profession, individuals may be further punished during disciplinary proceeding with disbarment from their profession or fines.

If a legal entity is held responsible for an offense, it shall be subject to a "corporate monetary penalty" (*Verbandsgeldstrafe*). The corporate monetary penalty is to be calculated in daily rates (*Tagessätze*) and can be conditionally suspended in whole or in part. The daily rate shall be assessed in accordance with the income situation of the legal person, taking account of its economic ability apart from the income situation, as well as the seriousness of the offense and any remedial measures taken by the entity after the offense. The daily rate typically corresponds to 1/360 of annual corporate revenue, but must be at least 100 Swiss francs and at most 15,000 Swiss francs.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Where the corporate monetary penalty imposed on a legal person is conditionally suspended in whole or in part, the court may issue instructions imposing technical, organizational, or personnel measures on the legal person to deter further offenses for which the legal person is liable. The legal person shall, in any event, be instructed to rectify the damage arising from the act to the best of its ability, to the extent that this has not already occurred.

As a general principle, the implementation of a compliance system may also be taken into account when it comes to determining the level of guilt, which necessarily has consequences on the level of fines.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The recent creation of the FMA mechanism for handling whistleblower complaints is the most noteworthy trend. The topic is very relevant and areas of conflict with various elements of criminal law, data protection, professional secrecy, and fiduciary duties must be considered.

CONTACTS

GASSER PARTNER

Wuhrstrasse 6
9490 Vaduz
Liechtenstein

Tel.: +423 236 30 80
www.gasserpartner.com

M.A. HSG Thomas Nigg, LL.M.
Senior Partner
GASSER PARTNER
T +423 236 30 80
thomas.nigg@gasserpartner.com

Thomas Nigg is Senior Partner at GASSER PARTNER Attorneys at Law, currently practising in Vaduz. He studied law at the University of St. Gallen (Switzerland), where he obtained his Master of Arts in Legal Studies HSG (M.A. HSG) in 2008. In 2007 he began practising as a lawyer in Liechtenstein and was admitted to the Liechtenstein Bar in 2010. In 2016 he was appointed a Senior Partner of GASSER PARTNER Attorneys at Law. The greater part of his work involves representing clients, mostly corporations or high-net-worth individuals, before courts in civil, criminal, and administrative matters, and assisting clients in commercial, corporate, and criminal law, plus banking and regulatory issues pertaining to both national and international affairs.

Mag. iur. Johannes Sander
Partner
GASSER PARTNER
T +423 236 30 80
johannes.sander@gasserpartner.com

Johannes Sander is a partner with GASSER PARTNER Attorneys at Law, currently practising in Vaduz. He studied law at the University of Innsbruck, where he earned his Master's degree in law (Mag. iur.) in 2011. In 2012, he began practising as an associate in Austria and passed the Austrian bar exam in 2015. After that, he joined GASSER PARTNER Attorneys at Law. His main areas of practice include civil law, criminal law, corporate law, and litigation.

Lithuania

COBALT

Dr. Dalia Foigt-Norvaišienė

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X			X
No			X	X	

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

The Law of the Republic of Lithuania on Whistleblowers' Protection that came into force starting from 1 January 2019 does not provide for any specific procedures. However, every company must maintain internal channels for whistleblowers reports and keep the information on whistleblowers strictly confidential. In addition, in accordance with the Law on Whistleblowers' Protection, the whistleblower must be notified within five business days about starting an investigation.

According to paragraph 1 of Article 39 of the Labor Code of the Republic of Lithuania (hereinafter – the "**Labor Code**") an employee cannot be held liable for a breach of the confidentiality agreement if the employee informs the authorities about illegal behavior in order to fulfill their legal obligations. There are no specific rules how the company must behave in this situation due to the fact that it should be regulated under the internal rules of the company.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) The Labor Code and/or other Lithuanian legislation do not provide for an obligation to inform any employee representatives about an internal investigation.

b) According to the Lithuanian Law on Legal Protection of Personal data (hereinafter – the "**LPPD**"), there is no obligation to inform a data protection officer ("**DPO**") or a data privacy authority about an internal investigation. However, if a DPO is appointed, general GDPR principles apply. For example, any employee may inquire about their data privacy rights (including information provided in the whistleblower report) and

the DPO shall be entitled to obtain the necessary information to respond to the query. In addition, the DPO has data processing monitoring duties. Thus, the company will generally have to inform the DPO about all data privacy related procedures and processes of an investigation.

c) Lithuanian legislation does not oblige the employer to inform the prosecution authorities about an internal investigation. However, the authorities need to be informed immediately if, during an internal investigation, the employer discovers signs of a current or future potential breach of criminal law.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

The Labor Code does not specify the duty of the employee to support the investigation. However, according to paragraph 1 of Article 24 of the Labor Code, employers and employees must act honestly, cooperatively and must not abuse the law in performance of their labor law rights and duties. This means that the employee has to participate in the investigation by answering questions related to their employment duties truthfully and completely.

In case the employee is required to participate in the investigation, the employee's refusal may be regarded as misconduct. Such misconduct may justify a dismissal if the employee had already received a formal warning for the same or similar misconduct before.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

According to paragraph 3 of Article 49 of the Labor Code, the employer can remove the employee from their work for up to 30 calendar days during the investigation of circumstances on the possible breach of employment duties by the employee. During this time the employer has to pay the employee their average salary.

Further, under Article 58 paragraph 6 of the Labor Code, an employer shall take the decision to terminate the employment contract for its violation within one month from the disclosure of the violation and no later than within six months from the date of the violation. The latter period might be extended to two years if the violation committed by an employee results from an audit, inventory or inspection of an activity.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

The LPPD provides certain specific local requirements. However, these requirements do not deal with employment-related investigations. Thus, the general GDPR principles of transparency, fairness, and lawfulness apply. Thus, employees have to be informed that (i) in case of any suspicion or a claim, an internal investigation shall be carried out by the impartial local investigation team, (ii) whether anonymous claims are accepted, (iii) how long the data obtained during the investigation is stored, (iv) who shall have access to it, etc.

b) Reviewing emails?

General GDPR principles of transparency, fairness, and lawfulness apply. It is very important that employees are informed about the situations in which their emails or other electronic communication can be monitored. The Lithuanian supervisory authority has provided a public opinion about the monitoring of employees' emails and other communication. According to this opinion, an overall monitoring of emails is prohibited. There has to be a valid reason for such monitoring, for example, suspicion of fraud, long absence, and suspicion of unethical behavior or breach of internal company rules. If emails are monitored, it is highly recommended that a representative of employees is present in order not to jeopardize any evidence.

Moreover, if an email is clearly marked as "personal" or "private", it should generally not be opened. In order to properly inform the employee, it is recommended to inform the employee in line with the internal policies of the company governing the monitoring of electronic communication at the workplace.

c) Collecting (electronic) documents and/or other information?

All documents and data both in written and electronic form are the employer's property which means that there is no prohibition to collect and/or review this information. If a folder is marked "Personal" or "Private" it should generally not be collected unless there is reliable evidence that the file has been named "personal" in deceit.

d) Analyzing accounting and/or other mere business databases?

Analyzing of accounting and/or other mere business databases is not legally restricted.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no general and statutory obligation to instruct an employee about the legal circumstances and their rights before the interview.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

The right to remain silent to prevent self-accusation only applies if a person is interrogated by local authorities under the suspicion that the person may have committed a crime. This right is in no way connected to interviewing an employee during an internal investigation.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no explicit obligation to inform the employee that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee.

d) Be informed that they have the right that their lawyer attends?

If the whistleblower is recognized by the competent authority as whistleblower they have a right to the legal aid.

The employee's general right to have a lawyer present during the interview is not governed by any Lithuanian law. However, companies often allow this kind of legal attendance in order to have a fair set-up or if the employee is suspected of having committed an offense.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

According to Lithuanian legislation, the employee does not have a strict legal right to be attended by a representative of the work council.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Yes, employees must be informed about their data transfer to countries outside the EU/EEA. In addition, such countries must be disclosed and applicable security measures must be indicated. The data transfer to third countries is performed according to the GDPR standards. There are currently no local regulations or guidelines on this topic.

g) Sign a data privacy waiver?

The wording of applicable laws does not explicitly provide for the possibility of a privacy waiver. Moreover, in employment relationships, there is high risk that such employee privacy waiver would be considered as forced due to subordination. Therefore, we have not witnessed such waivers in practice.

h) Be informed that the information gathered might be passed on to authorities?

In accordance with the GDPR, an employee must be informed about all potential recipients to whom the employee's personal data may be transferred to.

i) Be informed that written notes will be taken?

The content of the information to be provided to the data subjects is provided in Article 13-14 of the GDPR. The mentioned provisions do not contain an explicit requirement to inform about interview notes being taken. However, in order to be transparent, the employer may provide as much information as they consider necessary.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law governing this question, however, issuing of such notices is a common procedure.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The results of the internal investigation may not be revealed due to client secrecy. By the mentioned way, attorney-client confidentiality may be applied.

In accordance with the Law of the Bar Association of the Republic of Lithuania, an attorney-at-law cannot be summoned as a witness or provide explanations about circumstances, which he gained knowledge about by providing legal service. This is because of his professional duties. It is also generally prohibited to inspect, check or withdraw attorney at law's documents (in any form) related to his activity. Therefore, the search or examination of the attorney at law in his work place, living place, vehicle, etc. can be performed only with the participation of the member of the Executive Board of the Bar Association.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

The Labor Code does not specifically regulate attorney-client privilege in case of in-house counsel. Documents in the custody of in-house counsel can therefore in general be seized by the authorities.

However, under Lithuanian case law in-house counsel have to inform authorities in case they become aware of a potentially committed crime within their company.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

As far as circumstances arise which could cause claims against the insurance company, the policy holder should make a notification of circumstances to the insurer. However, there are no Lithuanian legal statutes which govern such explicit obligation.

b) To business partners (e.g. banks and creditors)?

Lithuanian legislation does not govern such an obligation. However, the duty to inform a business partner may arise from contractual obligations between the parties. It depends on the individual case whether and when the business partner needs to be notified.

c) To shareholders?

Lithuanian laws do not govern explicit obligations to inform shareholders about the internal investigation.

d) To authorities?

There is no duty to inform the prosecutor about the internal investigation or potential misconduct within the company. There may only be exceptions for very significant crimes, for instance, murder, serious health impairment, etc. However, a cooperative approach with the local prosecutor may prevent adverse and unexpected measures by the authorities, such as dawn raids.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

In accordance with paragraph 2 of Article 205 of the Labor Code, the employer has the duty to inform and to consult employees about all questions of particular importance. Starting an internal investigation may be considered as such an event.

Further, if the company becomes aware of ongoing criminal conduct within the company, it may be advisable to conduct disciplinary measures to stop such misconduct. There are two ways to make sure that an individual's behavior is stopped:

- In accordance with paragraph 3 of Article 49 of the Labor Code, an employer may, while examining the circumstances in which an employee may be subjected to the breach of their duties, waive the employee until 30 calendar days paying them their average salary.
- Under Article 58 paragraph 2, subparagraphs 5 and 6 of the Labor Code there is a possibility to terminate the employment contract with the employee in case of the following circumstances:
    - material damage done deliberately to the employer or an attempt to intentionally cause him material (property) damage;
    - a criminal offense was committed during the work time or at the work place.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices generally appreciate internal investigations through external investigators, such as law firms. Early involvement, communication and coordination may be helpful for good cooperation with local prosecutors. In this regard, it is crucial that the company does not destroy any potential evidence or convey the impression that evidence is or will be destroyed. Therefore, data retention orders should be communicated at the earliest stage possible.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Under Article 145 of the Code of Criminal Procedure of the Republic of Lithuania, in cases where there are grounds for assuming that there are, in some premises or in any other place or in the possession of some person, instruments of a crime, tangible objects and valuables that were obtained or acquired in a criminal offense, a pre-trial investigation officer or a prosecutor may conduct a search for the purposes of discovering and seizing them.

The search is carried out on the basis of a reasoned judgment issued by the pre-trial investigation judge. This judgment must specify the objects to be searched for (possession of a person, instruments of a crime, tangible objects and valuables that were obtained or acquired in a criminal way, or certain items or documents which might be relevant to the investigation of the criminal offense). In cases of utmost urgency, the search may be carried out pursuant to the resolution of a pre-trial investigation officer or a prosecutor. However, in such cases a pre-trial investigation judge has to confirm the legitimacy of such a search within three days after the search was conducted. If such confirmation of a pre-trial judge is not received within the specified period, all objects, valuables and documents seized during the search must be returned to the persons from whom these objects, valuables or documents had been taken. Further, the results of such a search may not be used as evidence in further proceedings. The latter also applies if other requirements for the search are not met.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Deals and non-prosecution agreements are not provided for corporations under Lithuanian law.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

In accordance with the Penal Code of the Republic of Lithuania (hereinafter – the "**Penal Code**"), there is no special provision on misconduct between companies or their directors, officers or employees. However, if one of the mentioned subjects commits a crime against another subject, penalties can generally include fines, public work, arrests or even imprisonment. The type of penalty depends on the committed crime.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Lithuanian law does not provide for such possibility. However Lithuanian courts might consider on a case-by-case basis the possibility to reduce penalties in case the efficient compliance system has already been implemented prior to the alleged misconduct.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

We are not aware of post-GDPR case law regarding internal work-related investigations. However, as mentioned in 5b above, the Lithuanian supervisory authority has provided a public opinion about the monitoring of employees' emails and other communication. In essence, this public opinion sets certain trends regarding data processing of employees, such as a prohibition of overall monitoring. In practice, it is also highly recommended that any extraction of evidence is performed in the presence of the employee representatives.

CONTACT

Lvovo 25
Vilnius 09320
Lithuania

Tel.: +370 5250 0800
www.cobalt.legal

Dr. Dalia Foigt-Norvaišienė
Legal Counsel
COBALT
T +370 5250 0800
dalia.foigt@cobalt.legal

Dr. Dalia Foigt-Norvaišienė chairs the Employment, Immigration and Labor Law Pratice Group at COBALT Lithuania. She has an extensive over 24 years of experience in advising clients on Employment, Corporate Law issues and is a recognised expert on international and domestic arbitration. She provides both day-to-day counselling, as well as assists clients in more extensive projects and cross-border transactions. She has assisted numerous local and international clients upon choosing the best solution for establishing a business in Lithuania and upon setting up and operating these businesses including but not limited to employment matters. Dalia is frequently invited to share her experience and knowledge in international publications, conferences, seminars and trainings.

Before starting a private practice Dalia gained her PhD in the area of Environment law and continued her career as Senior Researcher and Associated Professor of Vilnius University. Dalia has also taken part in legislative work in Lithuania in the areas of Environment and Litigation.

Dalia is active member of business community and maintains good contacts with municipal and central government institutions while representing business community and seeking to improve business environment. Dalia is an honourable member of Business Women Association, Member of European Business Network, Member of France-Lithuanian Chamber of Commerce, Member of the Board of Lithuanian Lawyers Association, Member of International Bar Association, Member of Lithuanian Bar and member of its Council and its Employment Law Committee.

Luxembourg

Lutgen + Associés

André Lutgen

Pierre Hurt

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Whistleblowers are protected against retaliation from their employer by labor law, where acts of bribery, trading in influence, taking illegal advantage, or sexual harassment are reported. Although no procedure expressly protects a whistleblower's identity during an internal investigation (except in cases of market abuse), it is nevertheless recommended to provide such protection to avoid the risk of a whistleblower suffering any negative consequences as a result of the report. If a whistleblower experiences negative consequences, the employer may be liable for mishandling the whistleblower's identity.

The only legal obligation to investigate relates to anti-money laundering ("**AML**") matters. This is inferred from the obligation to report any suspicious information about a client, which may include internal whistleblower complaints.

However, whistleblowers' protection will be strengthened with the transposition of the Directive (UE) 2019/1937 of the European Parliament and the Council of 23 October 2019 on the protection of persons who report breaches of Union law. Member States shall comply with this Directive by 17 December 2021.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Except for sexual harassment investigations, there is no law concerning the notification or participation of employee representative bodies in internal investigations. This may, however, be required by certain industry collective agreements.

b) The employee's right to privacy in the workplace is protected under Luxembourg law. Infringement thereof may constitute a criminal offense. Under the General Data Protection Regulation ("**GDPR**"), companies

operating in Luxembourg need to appoint data protection officers ("**DPO**"). If an investigation requires the processing of sensitive personal data, the DPO must be consulted in order to assess the impact of such processing.

Under the GDPR, if the DPO determined that the processing involves a high risk, the Commission Nationale de la Protection des Données ("**CNPD**") must be consulted. If the investigation relates to a data breach, the CNPD must be notified.

c) Given that Luxembourg is an important financial center, the necessity to inform a supervisory body, namely the Commission de Surveillance du Secteur Financier ("**CSSF**") or the Commissariat Aux Assurances ("**CAA**"), should be carefully taken into consideration.

Ongoing criminal behavior revealed in the course of an investigation should be reported to the public prosecutor. In cases relating to AML, the public prosecutor's financial intelligence unit – Cellule de Renseignement Financier ("**CRF**") – must be notified.

Entities, board members, or employees with ties to the public sector have an obligation to report any misdemeanor or crime to the public prosecutor's office.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

An employee's duty to support an internal investigation is inferred from the employee's general duty of loyalty to his employer, i.e.the duty to act in the employer's best interests. Disciplinary measures, including dismissal, can be taken against an uncooperative employee, where the lack of cooperation constitutes misconduct and has a negative impact on the employer. Employers should be careful in assessing the gravity of an employee's uncooperative behavior, as sanctions must be proportionate.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

From the moment an employer has knowledge of severe misconduct, which could justify immediate dismissal, the employer has one month to proceed with the dismissal. The employer is presumed to have knowledge of severe misconduct, when the employee with the authority to dismiss has sufficient knowledge of the misconduct. Such knowledge may be obtained through the investigation.

If the employer decides to simply sanction an employee for misconduct, the same misconduct cannot be used at a later stage as grounds for dismissal.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

The GDPR applies in Luxembourg since 25 May 2018 and is complemented by the law « *Loi du 1er août 2018 portant organization de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* ».

In very limited cases, the protection of state secrecy should be taken into account (*according to the loi modifiée du 5 juillet 2016 portant réorganization du service de renseignement de l'État (SRE)*).

a) Conducting interviews?

Data privacy laws apply to any processing of data. This includes securing, collecting, and reviewing data, as well as the creation of work products, such as interview file notes and final reports. Therefore, it is very important to perform an early assessment of the applicable data privacy laws with the DPO, where applicable, and to document the steps taken.

b) Reviewing emails?

Private communication is highly protected under Luxembourg law. The employer has a general obligation to respect the privacy of non-professional electronic communications of employees. Therefore, a thorough analysis of legal exposure should always be performed before email review is initiated.

c) Collecting (electronic) documents and/or other information?

The request of a legal authority or a legal obligation will often be a sufficient justification for gathering and using data. However, the mere communication with authorities can, in some instances, trigger the applicability of data protection laws. In critical cases, it may be advisable not to produce data on a voluntary basis, but to await a written formal request from the authority.

d) Analyzing accounting and/or other mere business databases?

No law in Luxembourg restricts the analysis of accounting and/or other mere business databases.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no legal obligation to provide written instructions to employees. It is nevertheless recommended that employees be informed of the general context of the investigation and of the rights of the employee during the investigation. Such information should be provided in writing, with a copy to be signed by the employee.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

Although an individual has the right to remain silent during interrogations by criminal authorities, there is no corresponding right with regard to employee interviews as part of internal investigations. However, per the ethical rules of the Luxembourg Bar Association, an interviewer should avoid pressuring an interviewee to make a self-incriminating statement.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

A so-called Upjohn warning must be provided to the interviewee under the ethical rules of the Luxembourg Bar Association.

d) Be informed that they have the right that their lawyer attends?

It is unclear from the case law whether an employee has a right to have personal counsel attend the interview. However, companies often allow such attendance to have a fair set-up or if the employee is suspected of having committed criminal offenses.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

The right to be assisted by a representative from the works council or from a nationally representative union is only provided for by labor law in case of a preliminary interview for dismissal in companies with at least 150 employees. Prior notice of the possibility of dismissal must be provided.

If there are any concerns that an interview could lead to a dismissal, and hence amount to a preliminary interview for dismissal, it is advised that the interview be treated as such.

Even when not legally required, a company may choose to allow a representative to assist the employee, especially if the company is itself assisted by a lawyer, so as to preserve "equality of arms". As this is not based on any legal obligation, a company should assess if the presence of such a representative is compatible with the preservation of confidentiality and/or professional secrecy obligations.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The employee should be informed that data may be transferred and processed outside of the European Union. The basis for the transfer must satisfy the provisions of the GDPR, be it consent, model clauses, binding corporate rules, or the like.

g) Sign a data privacy waiver?

It is advisable to offer the employee a data privacy waiver to sign. The employer should, however, still independently assess the legitimacy and proportionality of the subsequent use of the data, as the courts may review the adequacy of the employer's data privacy assessment, even in instances when an employee signed a waiver.

h) Be informed that the information gathered might be passed on to authorities?

Even though there is no legal obligation in Luxembourg to inform the employee that information may be passed on to authorities, it is common practice to add this caution to the interview instructions. An interviewee should, in particular, be informed if the data may be transferred to non-EU authorities.

i) Be informed that written notes will be taken?

There is no legal obligation under Luxembourg law to inform the interviewee that notes will be taken. However, in the interest of transparency, the potential future use of information provided by the employee (e.g. for reports and potentially for disclosure) should be explained.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law or practice governing this question in Luxembourg.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The only findings covered by privilege are those made by experts retained by counsel (an *avocat*). For the findings of the internal investigation to be covered by attorney-client privilege, the employer has to mandate a lawyer to proceed with the investigation. Said lawyer can then require the assistance of experts if necessary (e.g. the forensic department of a consulting or accounting firm), whose work, by being integrated in the lawyer's investigation, would be covered by attorney-client privilege.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Attorney-client privilege does not apply to in-house counsel in Luxembourg. However, any exchange with a law firm, including one between in-house and outside counsel, is protected by the attorney-client privilege, even if the communication is in the custody of in-house counsel.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Notification to insurance companies when starting an investigation is highly advisable. In this regard, the relevant insurance contracts should be checked.

b) To business partners (e.g. banks and creditors)?

Information duties may arise from contractual obligations between the company and the business partner. Even if there is no explicit provision in the contract, there may nonetheless be an obligation in cases where the internal investigation concerns information that is highly important for the other party and relevant to the purpose of the agreement. These interests of the business partner need to be evaluated against the legitimate interests of the company. Therefore, it depends on the individual case whether and when the business partner needs to be notified. In any circumstance, the situation in regard to legal privilege must be carefully examined.

c) To shareholders?

Duties to inform shareholders only exist for publicly listed companies and may be at odds with the desire to maintain confidentiality or professional secrecy duties. The company must evaluate on a case-by-case basis if there is an *ad hoc* duty to report to shareholders.

Under current market abuse legislation, knowledge of an internal investigation may be seen as insider information that could influence stock prices. An obligation to disclose may arise if the internal investigation may affect stock prices significantly and fulfills different criteria (e.g. risk of the internal investigation, scope, involved suspects). In case of a violation of the reporting duties, the company may be liable for damages and may eventually be exposed to criminal and administrative sanctions.

d) To authorities?

Depending on the area of activity of the company or on the type of incident that is investigated, various authorities and supervising bodies may need to be notified:

– The CSSF, in relation to market abuse, AML, and fraud;

– The CAA, in particular in relation to AML matters; and

– The CRF, in relation to AML matters.

Moreover, ongoing criminal behavior revealed in the course of an investigation should be reported to the public prosecutor and to the supervisory authority.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

A company is expected to show diligence in identifying the damage caused by the alleged misconduct, mitigating its effects, and preventing further damage (e.g. by strengthening processes or reinforcing its compliance system). It is also recommended that a company proportionately sanction misconduct to discourage further cases.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

The need to report the facts leading to an internal investigation or the results of such an investigation to the public prosecutor's office is to be evaluated by the company (except where there is a legal obligation to report). Should the prosecutor's office open its own criminal investigation, the authorities will typically take complete control of the investigation and any parallel internal investigation will have to be coordinated with them.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

A search of company premises may only take place by order of a judge and cannot begin before 6.30 a.m. or after midnight. Furthermore, a search of company premises cannot devolve into a so-called "fishing expedition" to discover infringements. The search can only be used for the purpose of finding evidence to strengthen an existing investigation of identified infringements. All types of communication between a lawyer and the client are protected by legal professional privilege and cannot be seized, except if the lawyer is suspected of having committed a crime. Searches executed in breach of the legal prerequisites can be annulled, rendering seized evidence unusable, but companies should be mindful of the short statute of limitations to lodge an annulment claim.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Deals may be closed with the public prosecutor's office by corporations in cases of offenses with a fixed sentence of up to five years of imprisonment and/or a fine of a minimum of €500. The maximum fine depends on the nature of the offense and could reach millions of euros. Such deals are mainly used in cases of minor offenses and tax fraud. A deal may be entered into as long as the trial judge has not yet decided on the guilt of the defendant or whether the offense is still prosecutable. It is, therefore, recommended to begin negotiations with the prosecutor's office as early as possible, if this step is considered an option.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

The prosecution of a company does not preclude the prosecution of the individual(s) involved in the commission of the offense.

Four types of penalties are applicable to companies: fines (ranging from €500 to €3.75 million, depending on the offense); asset seizure; exclusion of participation in public procurement; and winding up.

As to natural persons, the main applicable sanctions are fines (ranging from €251 to €2.5 million, depending on the offense); imprisonment; and asset seizure. For some regulated professions, a criminal sentence may cause an individual to be barred from that profession.

Although prison sentences for the most common offenses can reach up to 10 years, infringements committed in the context of the company, meaning where an employee/manager/director has used his position and function within the company to defraud, are generally sanctioned with a fine and sentence of several months on probation, if any.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Criminal courts must consider mitigating circumstances to reduce the sentence pronounced. There is no list of circumstances that may be taken into account. It is up to the judge to determine which element is relevant for determining the sentence. In addition, according to the principle of the individualization of the sentence, criminal courts must ensure that every sentence is adjusted to the person convicted.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Luxembourg is currently evaluated by the Financial Action Task Force ("**FATF**"). The FATF sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. FAFT inspectors conduct on-site inspections to verify the proper application of AML rules. They control Luxembourg's financial regulator, the CSSF, and a representative sampling of companies in banking, funds, insurance, etc.

The European Directive on the European Investigation Order ("**EIO**") in criminal matters (Directive 2014/41/EU) has been implemented in Luxembourg (*Loi du 1er août 2018 portant transposition de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale*). Aimed at strengthening European cooperation in criminal matters, the Directive creates a single investigation order on the European level to facilitate the gathering of evidence. In this respect, while one may still be able to challenge an EIO, the grounds for such challenges are limited.

The CSSF has set up a complex independent whistleblowing entity for the financial sector. Moreover, a July 2015 law granted the CSSF the power to impose administrative sanctions of up to 10 percent of a company's annual revenue and up to €5 million on natural persons. The CSSF has imposed sanctions of more than €3 million,

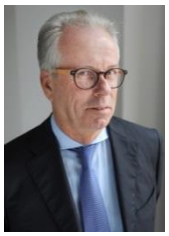
€4 million and €8.9 million on two banks for non-compliance with AML rules. Very recently, sanctions of €2.2 million have been imposed on eight entities for non-compliance with AML procedures.

CONTACTS

LUTGEN + ASSOCIES

10, rue Sainte Zithe
2763 Luxembourg
Luxembourg

Tel.: +352 27 35 27
Fax: +352 27 35 27 35
www.lutgen-associes.com



André Lutgen
Partner
Lutgen + Associés
T +352 27 35 27
al@lutgen-associes.com

During my long experience in defending company directors in criminal proceedings, I have found that behind each business manager there is an individual with his own feelings and awareness. We need to accompany him, acting as a legal professional throughout proceedings, which are often much too long, while supporting him during the personal upheaval that marks this period, which is often perceived as a life-changing experience.

In business litigation, listening is the only means of understanding what is the real problem confronting us, which enables the identification of the appropriate remedy. The solution of the problem, as envisaged by the client, is frequently inappropriate, and my professional ethics forbid me from acting as a "procedures merchant".

Pierre Hurt
Partner
Lutgen + Associés
T +352 27 35 27
ph@lutgen-associes.com

Following my doctorate thesis and after several years teaching at the Universities of Paris 1 Panthéon Sorbonne and Paris 5 René Descartes, I continued my academic activities at the University of Luxembourg, whist at the same time becoming a lawyer. I am convinced that a demanding professional practice does not in any way preclude a high level of theoretical competence – just the opposite. After having specialized in civil law and civil proceedings during my years at university, and my initial years at the bar, I have progressively built up a fund of knowledge in criminal law and criminal proceedings since joining Lutgen + Associés.

Malta

Camilleri Preziosi Advocates

Henri Mizzi Diane Bugeja

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X		X
No				X	

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

The Protection of the Whistleblower Act (Chapter 527 of the Laws of Malta), provides procedures, which allow employees in both the private and public sectors to disclose information regarding the improper conduct of their employers or colleagues. In addition, it ensures the protection of such employees from detrimental actions. Prior to the promulgation of this Act, the Employment and Industrial Relations Act (Chapter 452 of the Laws of Malta) also protected whistleblowers, prohibiting retaliation against employees for having made a complaint to the lawful authorities or for having disclosed information to a public regulating body regarding any alleged illegal or corrupt activities. Further, both the Public Administration Act (Chapter 595 of the Laws of Malta) and the Public Service Management Code oblige public employees and officers respectively, to report any unethical behavior or wrongdoing by another employee or officer to a senior employee or officer.

Under the Protection of the Whistleblower Act, a disclosure is deemed to constitute a "protected disclosure" if:

- It is made in good faith; and
- At the time of making the disclosure, the whistleblower reasonably believes that the information disclosed and any allegation contained in it are substantially true and that the information disclosed tends to show an improper practice being committed by their employer, another employee of their employer or by persons acting in the employer's name and interests, based on the information they have at that moment.

With regard to internal whistleblowing procedures, the Protection of the Whistleblower Act provides that all employers to whom the Act applies (including the public administration, private sector organizations and voluntary organizations meeting the thresholds laid down in the Second Schedule), must have internal whistleblowing procedures in place. These regulate the collection of such information; the notification to the whistleblower of the status of the improper practice so disclosed; and any other related matters. The law does not specify the content of such internal procedures. Notwithstanding the foregoing, in case of organizations where no such obligation exists and no such internal procedures are in place, the whistleblower is still protected when an internal disclosure is made to the head or deputy head of the organization. Thus, the Protection of the Whistleblower Act places an obligation on each employer to establish appropriate procedures for internal investigation of whistleblower reports while leaving the practical execution at the employer's discretion.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) There is no reference to trade unions in the Protection of the Whistleblower Act. However, in practice, the employer would inform the employee of their right to consult the union which he is a member of.

b) The Maltese legal framework does not impose an obligation to inform data protection officers or data privacy authorities of an investigation, nor does it provide for their participation in an internal investigation. However, it may be advisable to inform the data protection officer about all data privacy related procedures, including those related to an employee investigation according to the Data Protection Act (Chapter 586 of the Laws of Malta), as well as the forthcoming European General Data Protection Regulation, Regulation (EU) 2016/679, ("**GDPR**"), since the data protection officer must, *inter alia*, safeguard employees' data privacy rights and fulfill his data protection monitoring duties more generally. In particular, the data protection officer would be consulted by the employer to ensure that the lawful basis being relied upon for the processing of personal data in the context of the investigation is appropriate and whether the balance between an employee's right to privacy at work and other legitimate rights and interests of the employee would be violated as a result of this investigation

c) The Protection of the Whistleblower Act requires the appointment of a 'whistleblowing reporting officer', which is defined as the person identified within an organization to whom a protected disclosure may be made. Where the disclosure leads to the detection of a crime or contravention under any applicable law, the said officer may refer the report to the police for investigation. An authority to whom a protected disclosure is made may disclose such information to another authority within 30 days where it feels that the matter can be better investigated by another authority.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Generally speaking, Maltese law does not make any reference to the necessary procedure to be adopted in such investigations and does not place any such obligation on employees. Investigations are to be carried out in accordance with the internal procedure adopted by the employer subject to other applicable laws (including those regulating employment and data protection, amongst others). Additional obligations may be expected in case the employee has management responsibility due to potential supervisory duties.

The Protection of the Whistleblower Act further provides that the existence of the internal procedures and adequate information on how to use the procedures must be published widely within the organization. Generally speaking, such procedures would provide that all employees should cooperate with any external or internal investigations carried out. With particular reference to external investigations, where the company in question is a regulated entity or is otherwise subject to anti-money laundering laws, all employees are required by law to be fully cooperative and transparent in any investigations or inquiries conducted by competent authorities.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

There are generally no labor law related deadlines linked to investigative actions. In particular, there is no formal deadline within which an employer must terminate the employment of an employee found to be in breach of the employment contract. The applicable law specifies that an employer may dismiss the employee without notice and without liability when there is good and sufficient cause to do so. Moreover, accepted practice favors employers who

set up internal disciplinary structures, *inter alia* to oversee fair disciplinary proceedings. Such fair proceedings include granting employees the chance to defend themselves with the aid of trade union and/or legal representatives (if required) against the charges levied against the employee. This should be done prior to a decision being taken by the employer leading to dismissal. To not prejudice its rights, it would always be advisable for an employer to dismiss the employee as soon as an informed conclusion on the proper cause for a dismissal is reached.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Personal data must be processed in accordance with the requirements of the GDPR and the Data Protection Act (which is largely based on the GDPR), which *inter alia* includes that the processing has to be fair and lawful as well as be conducted in accordance with good practice. Furthermore, the "processing" of personal data is attributed a very broad definition by the GDPR and as such, "processing" covers any operation or set of operations which is performed on personal data or sets of personal data. Accordingly, interviews conducted in pursuance of an ongoing investigation must comply with the requirements of the GDPR and the Data Protection Act.

b) Reviewing emails?

Emails generally contain personal data and as a result generally fall within the scope of the requirements of the GDPR and the Data Protection Act for processing of personal data. Thus, data subjects need to be informed of any reviews of emails or other electronic communications. Further, it should be noted that the Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 586.01) provide that no person other than the user, may listen, tap, store or undertake any other form of interception of any electronic communication, inclusive of emails, without the consent of the user concerned.

c) Collecting (electronic) documents and/or other information?

The collection of documents, including electronic documents, or other information, which contain personal data, may only be undertaken if said collection is lawful under the GDPR and the Data Protection Act.

d) Analyzing accounting and/or other mere business databases?

Accounting and business databases fall within the remit of the GDPR and the Data Protection Act only if and to the extent that such databases contain personal data. Generally speaking, these databases would typically contain data that relates to the activities of the employer and its business rather than personal data.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

Maltese law does not specifically place any obligations on the employer to instruct the employee about his rights in relation to the investigation or any specifications on the conducting of the investigation itself.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

Both Maltese and European Union law provide an individual's right to remain silent in case of self-incrimination. Maltese criminal courts have interpreted this right to mean that a suspect does not need to reply to incriminating questions during an interrogation. Although not expressly mentioned in the Protection of the Whistleblower Act, it would still be good practice to grant the employee the option to have their attorney present during the interview.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

The Upjohn warning does not currently feature in Maltese law. In fact, there is no law providing guidelines on the procedure to follow when the lawyer in attendance is the lawyer of the company or an independent lawyer appointed by the interviewee.

d) Be informed that they have the right that their lawyer attends?

Prior to recent legislative amendments, one had a right to speak to a lawyer only before an interrogation. However, the lawyer did not have the right to be present during the interrogation, notwithstanding numerous rulings from the European Court of Human Rights pointing toward the need to strengthen the right to legal assistance during such interrogation.

Recent legislative amendments now generally grant the right of access to a lawyer. These amendments were *inter alia* enacted to transpose the European Directive 2013/48/EU, which deals with "the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings", amongst other correlated rights.

Notwithstanding the above, these legislative amendments apply only to official proceedings of investigating authorities and do not extend to internal investigations of a company operating in the private sector. Moreover, the accepted practice in private organizations suggests that in disciplinary proceedings, the attendance of a lawyer qua representative of the employee under investigation is allowed and at times encouraged to ensure as fair a process as possible.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

In practice, the interviewee should be allowed to seek advice from a trade union in relation to a potential or ongoing investigation and to consult with the trade union. Although there is no legal obligation to inform the employee, it is highly recommended that employers inform employees of such right before carrying out an interview.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

According to the GDPR, the transferring of any personal data which is undergoing processing or is intended to be processed to a third country (including the United States) is also subject to the requirements and protection afforded by law. Further, the data may only be transferred to a third country which ensures an adequate level of protection in terms of the Data Protection Act and the GDPR. The United States are not considered to be such a country. So any transfer to the United States would make additional justifications necessary which have to be assessed in each individual case.

g) Sign a data privacy waiver?

There is no requirement for the interviewee to sign a data privacy waiver. However, should the company determine that the applicable lawful basis of processing the personal data for the purpose of the interview is the data subject's consent, the company would need to ensure that the data subject's consent is appropriately collected in accordance with the provisions of the GDPR, particularly Article 7 therein. That being said, in the event that consent is deemed to be the appropriate lawful basis of processing, consent provided in this context would not be considered to be a waiver as such.

h) Be informed that the information gathered might be passed on to authorities?

The employee must be informed and their consent should be requested unless the respective employer is under a legal obligation to report the individual to the authorities.

i) Be informed that written notes will be taken?

There is currently no obligation under Maltese law to inform the interviewee that written notes will be taken during the interview which is largely unregulated by Maltese law.

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Document retention would normally be tackled in a data processing policy. Such an internal policy regulates the procurement, processing, and retention of different data sets depending on the laws applicable to the individual data sets. However, there is no specific regulation relating to document hold/retention notices *per se*. The retention of documents generated as a result of a report made under the Protection of the Whistleblower Act would largely depend on the internal procedures established by the employer pursuant to the requirement of the Protection of the Whistleblower Act as well as the legally accepted standards for document retention in terms of data protection law.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

In Malta, the legal attorney-client privilege is sacrosanct and predominantly exists in the context of civil and criminal litigation as well as in criminal proceedings and any investigations by the competition authority. Lawyers and their clients are granted protection with regards to confidentiality by the Code of Ethics, issued by the Maltese Chamber of Advocates.

In order to ensure privilege protection, external legal counsel should generally be involved. Further, claims of privilege are more likely to be upheld where the company can demonstrate that the advice provided by members of the legal professional was given in relation to a potential investigation by the authorities or otherwise where litigation is reasonably in prospect.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Maltese law on legal professional privilege fails to distinguish between independent lawyers and in-house counsel. Therefore it is safe to assume that the obligation of professional secrecy and confidentiality applies equally to both independent lawyers and in-house counsel. However, it may be more difficult to ascertain privilege on documents prepared by in-house counsel.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

The law does not specifically list any obligation of the employer. However, certain obligations with regards to precarious potential and ongoing investigations may arise from the terms and conditions of the insurance policy.

b) To business partners (e.g. banks and creditors)?

Certain notification duties may arise from any contracts or agreements entered into by the employer and any third parties where a potential or ongoing investigation may prejudice the position of any creditors with regards to the collection of any outstanding debts. Therefore any obligations in this respect are to be considered under the agreement itself and possibly any statutory law governing the relationship between the said partners.

c) To shareholders?

The directors of a company are responsible for the day-to-day running of the affairs of the company and thus act as the fiduciaries of the company. The directors of a company have certain reporting obligations to the shareholders especially where a potentially precarious situations risks diminishing the value of their shares.

d) To authorities?

Generally speaking, there is no obligation on the part of the company to inform the authorities about any internal investigation whether it is ongoing or not. However, this depends on the gravity of the wrongdoing and whether it affects public interest. Further, where the company is a regulated entity, the applicable laws

may, in certain instances, require the company to inform the competent authorities with immediate effect of any significant events affecting their business, including any significant internal investigations.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There are no general legal provisions in this respect although, with reference to regulated entities, these are required to take all reasonable measures in order to remediate any misconduct at the earliest whilst also establishing internal systems and controls to mitigate and manage the risk of such misconduct happening again in the future.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

The Protection of the Whistleblower Act requires every employer to have internal procedures in force, as described above. However, the Act fails to specify what exactly these internal procedures should cover and therefore it is safe to assume that it very much remains within the discretion of the employer. Wherever the disclosure involves an improper practice which constitutes a crime or contravention under any law, the whistleblowing reporting officer may pass on the report to the police for investigation thereof. The Protection of the Whistleblower Act is a relatively new introduction to the local legislative framework and, as such, there is little evidence, if any, on how local prosecutors are likely to react to internal investigations. There are no official or formal procedures which employers are expected to follow when conducting internal investigations (other than their own internal procedures which are required to be established pursuant to the Act). Consequently, the approach to be taken by local prosecutors, including their treatment of the conclusions arising from internal investigations and the procedure that has been followed is likely to depend on the facts of the case at hand.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Except in certain delineated cases expressly stated in the Criminal Code (Chapter 9 of the Laws of Malta), a police officer may not enter any private premises for the purpose of affecting a search within the said premises unless he is in possession of a warrant issued by a Magistrate. Apart from the police, raids may also be carried out by the Financial Intelligence Analysis Unit ("**FIAU**") where the criminal activity falls within the remit of the Prevention of Money Laundering Act (Chapter 373) and the Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01). Raids are carried out on the basis of an 'investigation order' which is issued by the Criminal Court upon application by the Attorney General. The FIAU's powers include the authority to enter any property and confiscate material related to the investigation without warning. Any search, whether carried out by the police or the FIAU cannot, however, extend to legal privilege for e.g. any communication between the suspect and his legal representative or to any excluded material. The search warrant or investigation order shall always be applied within the parameters for which it was issued. Once on the premises, the police or FIAU officer carrying out the search may seize anything if they have reasonable cause to believe that the object has been obtained in consequence of an offense or if it is evidence in relation to an offense. Under Maltese law, illegally obtained evidence may still be admissible.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

As from 2002 Maltese criminal law provides the option of sentence bargaining which means that the Attorney General, appearing on behalf of the prosecution and the accused through his legal counsel, can discuss and

predetermine what punishment and consequences arising from the finding of the guilt can be imposed by the court, in case of a guilty plea. The Maltese Criminal Code does not specifically mention whether corporations can avail themselves of this provision.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

The liability of the company falls on the directors of the company, as under Maltese law companies are not subject to criminal responsibility. However, the company may be subject to certain administrative fines and penalties in certain specified cases. The nature and amount of the penalties vary depending on the industry or sector in question and the laws applicable thereto. This notwithstanding, a company may face administrative fines of up to €20,000,000 or in the case of an undertaking, 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. Such administrative fines may be imposed onto a company by a supervisory authority where the company has processed personal data in reliance on a lawful basis which is deemed not to be the most appropriate lawful basis under Article 6 of the GDPR. An example of this may arise where the company relies on consent as its lawful basis of processing personal data for a particular purpose, but it transpires that consent would not be applicable as the consent collected does not satisfy the requirements of Article 7 of the GDPR.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Section 2 of The Protection of the Whistleblower Act provides that employers fulfilling certain criteria must have internal procedures in place for receiving and dealing with protected information but does not specify in detail how such mechanisms are to be designed and/or implemented. The Act does not lay down any penalties for non-compliance with this section nor does it provide for any aggravation and/or mitigation of other offenses and penalties under the Act or any other law in cases where organizations implement efficient compliance systems or *vice versa*. However, in practice, penalties could be mitigated in case the organization or its representatives have done their utmost to implement proper internal mechanisms prior to or following the alleged misconduct.

In the case of regulated entities, the Maltese financial services rulebook provides for a reduction or suspension in penalties where effective compliance systems have been introduced, where the company and its officials cooperate with the relevant authorities, and/or where other mitigating measures would have been introduced. From a criminal law perspective, particularly in the case of corporate criminal liability, the company may, in its defense, argue that it had taken all reasonable measures to prevent the misconduct from taking place and, if this argument is upheld by the Courts, then it may lead to a reduction or suspension of any applicable penalties.

From a data protection perspective, the fact that a company implemented an efficient compliance system may be taken into account when a supervisory authority has decided to implement an administrative fine in the event of a personal data breach or other infringements of the GDPR.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The Malta Financial Services Authority ("**MFSA**") and the Financial Intelligence Analysis Unit ("**FIAU**") have been particularly active in the financial services space in recent years. More specifically, they have upped their on-site inspections and have also levied numerous penalties for breach of the relevant rules and regulations. Any such penalties or other regulatory measures taken by regulators are made public on the respective websites. The entities subject to such measures have the right to appeal against the imposition of certain penalties or other administrative measures.

The Office for Competition ("**OC**") has similarly made a concerted effort to concentrate its resources on decreasing the number of pending cases and has closed a relatively high number of cases. The sectors involved covered the carriage of passengers, food services, fuel sales, car parking rates, and yacht marinas.

The authorities are expected to maintain their momentum insofar as on-site inspections and investigations are concerned, although no legislative changes are expected.

While the Information and Data Protection Commissioner's Office (the "**IDPC**", the relevant supervisory authority in Malta for data protection) does not publish its decisions, it did publish statistics on notified data breaches in October 2019. This document states that the IDPC received 109 data breach notifications between January 2019 and October 2019. The IDPC issued a total of five fines in the private sector, amounting to €4,500 in total and one fine in the public sector of €5,000.

CONTACTS

CAMILLERI PREZIOSI
ADVOCATES

Level 3, Valletta Buildings
South Street
Valletta 1103
Malta

Tel.: +356 21238989
www.camilleripreziosi.com

Henri Mizzi
Partner
Camilleri Preziosi
T +356 21238989
henri.mizzi@camilleripreziosi.com

Henri heads the EU, Competition and Regulatory Practice Group within Camilleri Preziosi and is directly responsible for main commercial and corporate litigation, including regulatory disputes between licensed entities and regulators. The Practice Group is actively involved in communications, media, IT & IP, data protection, employment and industrial relations, energy, infrastructure and environment as well as transport and related industries.

Diane Bugeja
Senior Associate
Camilleri Preziosi
T +356 21238989
diane.bugeja@camilleripreziosi.com

Diane is a Senior Associate in the Corporate Finance Practice Group at Camilleri Preziosi. She practices primarily in financial services law, financial regulation and anti-money laundering regulation, providing advice to local and overseas clients on the impact of the current and forthcoming regulatory regime on their business models. Diane also advises clients on the regulatory aspects of a wide range of transactions, including licensing-related matters, capital markets initiatives and ongoing liaison with regulatory authorities more broadly. Prior to joining the firm, Diane was a risk and regulatory consultant at a Big Four audit firm, working in Malta and in London, and subsequently joined the enforcement departments of the UK and Maltese financial services regulators.

The Netherlands

Hogan Lovells International LLP


Manon Cordewener


Jessica Booij


Joke Bodewits


Maria Benbrahim

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X		X
No				X	

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

As of 2016 the House for Whistleblowers Act (the "Whistleblowers Act") requires employers with at least 50 employees to draft and implement an internal whistleblower regulation. An internal whistleblower regulation should outline the following:

a. How and to whom to report abuses;

b. Types of abuse which can be reported;

c. The obligation of the employer to deal with reports confidentially, should the employee request confidentiality; and

d. The possibility for an employee to seek counsel to discuss the suspicion of abuse.

In addition, the employer must explain to the employee under what circumstances abuse may be reported externally and the legal protections afforded to whistleblowers. The employee is generally only allowed to report the abuse externally after a reasonable time has passed and the company has failed to eliminate the abuse.

An employee may file a request with the House of Whistleblowers in order to initiate an external investigation. The House of Whistleblowers is an independent governmental institution responsible for investigating abuses reported by employees. The House of Whistleblowers assesses reports on a case-by-case basis to determine whether it will initiate an external investigation.

If an internal report is made, the company should do everything to eliminate the suspicion of abuse. If the company fails to do so within a reasonable time and the employee makes an external report to the Investigation Department of the House of Whistleblowers, the employer and employee will be obliged to appear before the Department. The Investigation Department will issue a research report, which will contain recommendations to eliminate the abuse or to prevent a recurrence of the abuse. The report is not binding for any of the parties, but the employer has the duty to inform the House about the way it has addressed and/or implemented the recommendations. If the employer does not comply with the recommendations, it is obliged to give the reason for the non-compliance.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) The works council has no right to be informed about an internal investigation, although it must consent to the internal whistleblower regulation proposed by the employer. This is the case upon establishment, change, or withdraw of the whistleblower regulation. Furthermore, any changes to policies on complaints or whistleblowing are also subject to the prior right of consent of the works council.

b) The General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") and the Dutch Implementation Act of the GDPR (the "**DIA GDPR**") do not explicitly require notifying a data protection officer ("**DPO**") about an internal investigation. However, a DPO should be involved in all issues which relate to the protection of personal data based on the GDPR. Further to this general requirement, and based on Guidelines for Data Protection Officers, issued by the Dutch Data Protection Authority ("**DDPA**") and the European Data Protection Board, it is advisable to inform the DPO on investigations.

Furthermore, where the processing activity is likely to result in a high risk to the rights and freedoms of natural persons a data protection impact assessment ("**DPIA**") has to be carried out, in which case the GDPR requires seeking the advice of the DPO. Such DPIA should contain (i) a description of the envisaged processing operations and the purposes for processing, (ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes, (iii) an assessment of the risks to the rights and freedoms of the data subjects, and (iv) the measures envisaged to address the risks. In case the DPIA indicates that there is a high risk in the absence of measures taken to mitigate the risk, the DDPA has to be consulted.

In addition to the aforementioned requirement to inform the DDPA in case of a high risk (after conducting a DPIA), the GDPR and the DIA GDPR do not require informing the DDPA about an internal investigation.

Consequences in case of non-compliance

The maximum administrative fine for not involving a DPO or not performing a DPIA when required is €10,000,000 or 2 percent of the annual turnover. The DDPA has issued guidelines for imposing administrative fines. Based on these guidelines, the default fine for non-compliance with the said requirements is €310,000.

c) There is no statutory obligation to inform local authorities. However, a company's internal whistleblower regulation could provide this obligation.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees are obliged to cooperate with investigators of the House of Whistleblowers (i.e. to provide complete and truthful responses to requests). However, non-compliance is not sanctioned in the Whistleblowers Act. The House of Whistleblowers is not legally obliged to continue the investigation if the employee requesting the investigation does not cooperate adequately.

If an investigation is not conducted by the House of Whistleblowers, there is no specific rule that requires an employee to cooperate. However, on the basis of the general principle that employees should act as "good employees", it is expected that an employee will support and cooperate with an internal investigation. If an employee refuses to cooperate, an assessment could be made to determine what disciplinary measures, if any, should be imposed. Circumstances to consider include, but are not limited to, the personal circumstances of the employee, the length of the employment, and the seriousness of the suspected misconduct.

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Dutch law does not provide for explicit rules for internal investigations initiated by an employer, in a sense that there is no particular statute or codified regulations.

However, employers should be aware of the following:

a. It is only possible to dismiss an employee with immediate effect if the dismissal is prompt (onverwijld). This means that an investigation (after suspicion has been raised) should be carried out with minimum delay and the employer should dismiss the employee immediately once the culpability has been sufficiently established. Whether a dismissal was carried out quickly enough to be valid depends on the circumstances of the case.

b. The employer has a duty to act as a good employer. This means that an investigation should be conducted in a fair and reasonable way. If an employee was, for example, pressured or threatened during the investigation, this might hinder the employer's ability to take disciplinary measures. Moreover, if the employer engages in serious misconduct during an investigation, employees might try to claim damages or high severance payments.

In addition, there are various regulatory frameworks that govern internal investigations, such as the principles of duty of care, based on the principles of proper governance (*beginselen van behoorlijk bestuur*) and the principles of good employer ship (*goed werkgeverschap*).

The main principles that must be taken into account by an employer who plans an investigation are the principles of:

- **Duty of care**: this entails the requirement of careful consideration of relevant interests and the related principles of transparency, proportionality and subsidiarity;
- **Independence/neutrality**: the investigation team should not be involved in any way in the (alleged) irregularity and/or have a significant relationship with the individuals (allegedly) involved;
- **Fair play**: classical fair play principles are the duty to give reasons, to manage legitimate expectations, and to adhere to proportionality, subsidiarity and equality. It follows from Dutch case law that an employee should be allowed to be accompanied by any third person including a lawyer in the context of a (potential) dispute with the employer. Dutch legal literature reflects that legal assistance should be allowed and even encouraged by the employer once a particular step in an internal investigation may have consequences for the employee's legal position. In this respect, the nature of business activities, type of incident, the extent of the breach and the person of the employee are relevant factors.
- **Détournement de pouvoir**: the information obtained may not be used for other purposes than investigating the irregularity encountered;
- **Substantiation**: notes of interviews should be taken and presented for correction and/or confirmation by the relevant employee.
- **Honesty**: the employee should be able to rely on the statements of the employer throughout the process;
- **Equality**: equal cases will be treated equally;
- **Presumed innocence**: it is important not to make any accusations pending the investigation but rather confront the employee with facts and ask explanatory questions (address assumptions).

These principles should be taken into account through all (possible further) phases of the investigation process, i.e. when preparing, conducting and reporting on the investigation.

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Under Dutch data protection law, a legal basis for the processing of personal data is required. A legal basis cannot be found in the consent given by the employee, as employee consent is not considered freely given in an employment relationship, especially when it concerns investigations. Generally, a legal basis for conducting an internal investigation, including an employee interview, exists when the controller (in this case, the employer) has a legitimate business interest to investigate suspicions of misconduct, provided that the data subject has no overriding interest in the protection of their private life, and (i) the interview is relevant to the investigation; (ii) the same purpose cannot be achieved using less intrusive means (e.g. only document review); and (iii) the controller has implemented measures to protect the rights of the data subject (e.g. restricting access to interview data).

In case of an investigation by the DDPA, the controller will be required to demonstrate to the DDPA that it has taken into account the conditions above. When personal data is processed relating to criminal convictions and offenses or well-founded suspicions thereof, or related security measures, the DIA GDPR requires an exception to apply, such as for the protection of the controller's interests, insofar as it concerns criminal acts that are (expected to be) committed against the controller or its employees.

Furthermore, where the processing activity is likely to result in a high risk to the rights and freedoms of natural persons a DPIA has to be carried out (see section 2b).

Data subjects should be informed about the purposes and means of the processing prior to the commencement of processing. An employee should be informed before the interview is conducted. An exception to this rule applies where there is a substantial risk that such notification would jeopardize the ability of the controller to investigate a matter properly or gather the necessary evidence or where notification may lead to the destruction of data. In such cases, the notification to the data subjects may be delayed as long as such a risk exists, which should be determined on a case-by-case basis.

b) Reviewing emails?

As with conducting interviews, there must be a legal basis for the email review. The legal basis is typically derived from the legitimate business interest of the controller provided that (i) the email review is relevant to the investigation (e.g. non-relevant, private emails are excluded); (ii) the same purpose cannot be achieved using less intrusive means; and (iii) the controller has implemented measures to protect the rights of the data subject, including the right to privacy in the workplace (e.g. by engaging a third party to conduct the review, using an algorithm to search for emails, and restricting access to emails to a dedicated team subject to confidentiality obligations). In case personal data is processed relating to criminal convictions and offenses or well-founded suspicions thereof, or related security measures, the DIA GDPR requires an exception to apply. Furthermore, as described above, a DPIA may have to be carried out and data subjects may have to be informed in advance unless an exception applies.

c) Collecting (electronic) documents and/or other information?

As with conducting interviews and reviewing emails, a legal basis for collecting documents must exist, which is assessed using the factors described above. Also, as described above, a DPIA may have to be carried out and data subjects may have to be informed.

d) Analyzing accounting and/or other mere business databases?

Dutch data protection law does not protect the processing of non-personal data, e.g. statistics or accounting information.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no statutory obligation to provide an interviewee with written instructions; however, a company's internal whistleblower regulation could provide this obligation. Moreover, from the perspective of good

employer ship it may be required to communicate in writing on potential irregularities or investigations allowing the employee to understand the context and seek legal assistance.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no statutory obligation to inform the interviewee about the right to be free from self-incrimination; however, a company's internal whistleblower regulation could provide this obligation. Moreover, it is required to inform the employee on the possible legal consequences of the investigation so that the employee understands themself that self-incrimination may be at stake.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no statutory obligation to provide an Upjohn warning; however, a company's internal whistleblower regulation could provide this obligation. At the same time, from the perspective of good employer ship it is required to inform the employee thoroughly on the context and setting of the interview. The process should be fair and not misleading.

d) Be informed that they have the right that their lawyer attends?

If the interview is conducted by the police, where the employee is a suspect in a criminal investigation, then the interviewee should be informed that they have the right that their lawyer attends. If the interview is not conducted by the police, there is no such right or corresponding information obligation. However, a company's internal whistleblower regulation could provide this obligation. If the interview is not conducted by the police, a similar obligation can be assumed.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

The employee has no right to have a works council representative attend the interview; however, a company's internal whistleblower regulation could provide this right and corresponding information obligation. Moreover, the employee is free to have anyone he wishes to be present during the interview. This could be a relative, colleague, trust person, lawyer, or friend.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

As a rule of thumb, personal data may not be transferred to countries outside of the European Economic Area, unless the data recipient offers an adequate level of protection. Data subjects must be informed about the recipients or categories of recipients of their personal data and the transfer of data to a third country or international organization. Moreover, the GDPR requires that the data subject be informed of the safeguards implemented to legitimize the international transfer, for instance by reference to model clauses approved by the European Commission or Binding Corporate Rules (BCR) approved by the DDPA, and be informed of the means to obtain a copy of the safeguards or where they have been made available.

g) Sign a data privacy waiver?

Under Dutch data protection law, employee consent does not qualify as valid consent for investigations. As a result, a signed data privacy waiver has no legal effect.

h) Be informed that the information gathered might be passed on to authorities?

There is no statutory obligation to inform the interviewee that information might be passed on to authorities; however, the internal whistleblower regulation could provide this obligation.

i) Be informed that written notes will be taken?

There is no statutory obligation to inform the interviewee that written notes will be taken; however, the internal whistleblower regulation could provide this obligation. At the same time, from the perspective of good employer ship it is required to inform the employee beforehand that their feedback will be recorded in writing. The process should be fair and not misleading.

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Pursuant to the GDPR, personal data may not be kept longer than required for the purpose for which the data has been collected. Data subjects have to be informed about retention periods or the criteria used to determine the retention period. After the storage period has passed and the company no longer needs the data, the company must destroy it. An exception to the disposal of documents after the maximum retention period has lapsed can be established by issuing a document hold notice, which suspends the retention policy. Such a legal or tax hold notice prevents the disposal of relevant documents in case of any expected litigation or investigations.

In case personal data will be retained after an initial retention period, further to a hold notice, the data subject has to be informed about this new purpose and (criteria used to determine the) retention period, unless there is a substantial risk that such notification would jeopardize the ability of the controller to investigate a matter properly or gather the necessary evidence or where notification may lead to the destruction of data.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

In the Netherlands, the scope and extent of the attorney-client privilege (verschoningsrecht) is currently a topic of discussion.

In principle, the attorney-client privilege applies to the oral and written information received, drafted, and sent by the attorney in relation to his client or case. This privilege protection applies to legal advice and the documents used as the basis for such legal advice.

However, in 2015, a Dutch District Court ruled that the attorney-client privilege does not apply to a report composed by an attorney entailing merely factual findings of an internal investigation. The District Court held that the attorney-client privilege did not apply due to the absence of any legal findings, legal qualifications, or legal conclusions. In addition, the District Court noted that the investigation conducted by the law firm was to be called "independent". For this reason, the District Court did not consider the report to be internal, advisory, or confidential in relation to the client's legal position. This judgment has been extensively criticized.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Attorney-client privilege (verschoningsrecht) applies to attorneys-at-law registered with the Dutch bar (Nederlandse orde van Advocaten). Hence, an attorney-at-law working for a company, who is registered with the Dutch bar, may benefit from privilege protection. The Supreme Court confirmed in 2013 that attorney-client privilege also applies to attorneys-at-law employed by a company (*Cohen-advocaten*).

In-house counsel, not registered with the Dutch bar, do not have attorney-client privilege. Depending on their education, in-house counsel can be admitted to the Bar, provided they meet all requirements to become an attorney-at-law. In that case, the attorney and its company must enter into an agreement that safeguards the independent professional practice of the attorney.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

The requirement to notify an insurance company of the start of an investigation depends on the terms and conditions of the individual insurance policy.

b) To business partners (e.g. banks and creditors)?

In general, there is no requirement to notify business partners of the start of an investigation. However, certain finance and similar agreements may stipulate an obligation to notify the bank.

c) To shareholders?

The obligation to notify shareholders of the start of an investigation may arise from the articles of association, internal whistleblower regulation, and/or shareholders' agreement. In general, according to the Dutch Civil Code, the board has to provide shareholders with information they require, absent a weighty interest of the company. The board may only reject the request for information in exceptional cases, e.g. if a competitive position will be harmed.

Publicly-traded companies have to substantiate the weighty reason(s) for not providing the shareholders with the required information on the basis of the Dutch Corporate Governance Code. In addition, publicly traded companies have to immediately disclose any price-sensitive information to the public, unless the company has a legitimate interest to not disclose.

d) To authorities?

In general, there is no duty to inform the prosecutor about an internal investigation or potential misconduct within the company.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There is no statutory provision that prescribes immediate measures that have to be taken upon the start of an investigation. However, the company must stop potential, ongoing breaches of the law as soon as possible. Failure to do so may be attributed to the company in the context of civil, administrative, or criminal proceedings.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Whether a local prosecutor has concerns about an internal investigation depends on the specifics of the case.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Generally speaking, a search warrant or dawn raid can only be exercised upon approval by the relevant authorities, such as the Netherlands Authority for Consumers & Markets or the Public Prosecution Service.

In administrative proceedings, supervisory officers are allowed to search all locations, except homes, when needed to fulfill their supervisory duties. No warrant or court order is needed. Houses may only be entered after a court order from the investigative judge. During a dawn raid, the authorities gather evidence. The authorities are obliged to inform the company of the purpose and scope of the investigation at the start of a dawn raid. In general, a written description of the purpose is provided to the company. Fishing expeditions, where the authorities excessively search for evidence without defining the purpose and scope of the investigation, are not permitted.

In administrative proceedings – in principle – unlawfully obtained evidence does not have to be disregarded.

In criminal investigations, the public prosecutor is allowed to enter and search the premises of a company suspected of a crime. In that case, no court order is required. If the company is not a suspect the search or seizure can only be conducted by the investigative judge. The search can be requested by the public prosecutor. This request must be detailed and show that all the legal requirements are met. The investigative judge and the (assistant) public prosecutor are also required to be present during the search or dawn raid.

In the event evidence has been unlawfully obtained in criminal proceedings, the court has the discretion to exclude the evidence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

It is possible to enter into a deal with the public prosecutor. Such a deal could consist of a penal order that is accepted by the accused corporation. Therefore, the case will not be presented to the court. It is also possible to agree to the confidentiality of such deals. However, third parties may request a (redacted) version of the non-prosecution agreement on the basis of the Government Information (Public Access) Act.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

A company can be held criminally liable for the misconduct of its employees. The public prosecutor or specific supervisory authorities are able to impose fines on the company for breaches of statutory provisions. A fine of up to 10 percent of the annual revenue of the company in the prior financial year may be imposed.

Employees may also be held individually criminally liable. This could lead to a fine or even imprisonment. An individual convicted of public bribery, for example, may face up to six years in prison or a fine of up to €87,000.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

As explained in question 1 above, the Whistleblowers Act requires employers with at least 50 employees to implement an internal whistleblowers regulation. According to the Money Laundering and Terrorist Financing (Prevention) Act, some financial institutions are obliged to appoint a compliance officer. For other companies no such obligation exists.

In the Netherlands, no specific sentencing guidelines exist that provide for a reduction or suspension of penalties in case a company implemented an efficient compliance system. However, when determining the punishment, the judge will consider all circumstances of the case. It is possible that the judge will take into account whether the company has implemented an efficient compliance system. Also, in negotiations about a possible deal with the prosecutor, such circumstances can be of importance.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

In October 2019, the Court of Rotterdam issued a judgment on attorney-client privilege of 15 in-house lawyers. 15 foreign lawyers were working in the Netherlands for a Dutch company. The in-house lawyers concerned each took the view that they had a right to refuse to give evidence, based on their registration at the bar in the country of origin. These lawyers and the employer did not sign a professional statute safeguarding their independence. The court held that the independence of the lawyers was not sufficiently guaranteed so that they could not be classified as holders of confidential information. As a result, they did not have an independent right to refuse to give evidence.

CONTACTS

Atrium, North Tower
Strawinskylaan 4129
1077 ZX Amsterdam
The Netherlands

Tel.: +31 20 55 33 600
Fax: +31 20 55 33 777
www.hoganlovells.com

Manon Cordewener
Partner
Hogan Lovells Amsterdam
T +31 20 55 33 691
manon.cordewener@hoganlovells.com

As head of the Litigation practice in Amsterdam, Manon brings a wealth of knowledge and extensive experience in contract disputes, shareholders disputes, antitrust litigation, product litigation and professional liability disputes. Industry sectors in which she is active are as diverse as automotive, energy and natural resources, financial institutions and consumer.

Jessica Booij
Associate
Hogan Lovells Amsterdam
T +31 20 55 33 615
jessica.booij@hoganlovells.com

As an associate in the Amsterdam Litigation team, Jessica Booij focuses her practice on commercial, product liability and collective actions/group litigation. Jessica is engaged in (international) disputes regarding commercial contracts, cartel damages, class actions and torts in various industries. She also regularly advises clients on (EU) regulatory matters.

Joke Bodewits
Partner
Hogan Lovells Amsterdam
T +31 20 55 33 645
joke.bodewits@hoganlovells.com

As Head of the European Cybersecurity practice of Hogan Lovells in Amsterdam, Joke Bodewits counsels clients in global cybersecurity matters at all levels of an organization. Joke brings to her practice years of experience advising companies and boards on cyber and data risk management and data governance, breach preparations and response, and global data strategies. Joke has counselled many clients during enforcement actions following cyber incidents.

Maria Benbrahim

Counsel
Hogan Lovells Amsterdam
T +31 20 55 33 622
maria.benbrahim@hoganlovells.com

As Counsel of the Employment Team, Maria focuses, *inter alia*, on "strategic" corporate/employment law matters, such as the employment law aspects and consequences of restructurings, outsourcings and M&A transactions, employee consultation related matters, negotiations with works councils and trade unions. Clients turn to Maria Benbrahim for a sharp and focused lawyer, with not only a deep understanding of employment/corporate law, but also a down to earth and practical mind-set. Maria is a pragmatic, effective and bold negotiator and litigator.

Norway

Hjort Law Office DA

Henrik Boehlke

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

According to the Employment Protection Act, all companies employing more than five employees are obliged to draw up and incorporate written guidelines for internal whistleblowing. Companies employing five employees or fewer shall also have such guidelines if deemed necessary. The guidelines, which shall be drawn up in cooperation between the employer and representatives of the employees, shall, as a minimum:

- Encourage employees to report on blameworthy behavior or conditions;
- Describe how reports shall be made; and
- Indicate how reports shall be handled and followed up.

Employees filing reports according to these guidelines are protected against sanctions from the employer, and reports shall be handled according to these guidelines.

The Employment Protection Act's regulations regarding whistleblowing were amended and updated with effect from 1 January 2020.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) The General Data Protection Regulation (EU) 2016/679 ("**GDPR**") is incorporated as Norwegian legislation as a part of the Personal Data Protection Act. In general, inquiries as part of an internal investigation shall be conducted in accordance with the regulations in the Personal Data Protection Act, including the GDPR. In addition, the company's written guidelines described under question 1 shall be observed. According to the Data Protection Act, employees shall, as far as possible, be informed and have the opportunity to give a

statement before the employer reviews emails in the employee's mailbox made available for the employee by the employer.

b) Before reviewing the emails of employee, the Data Protection Officer (if any) of the company shall be informed and have the opportunity to provide a statement. The employer also has to consider if the conditions for such review are met, including if there are sufficient reasons for reviewing the emails.

c) The prosecution authorities do not have the right to be informed before a company initiates an internal investigation. However, depending on the circumstances, a voluntary notice to the prosecution authorities may be advisable. If the internal investigation reveals criminal offenses, and the prosecuting authority is made aware of the facts at a late stage, the company can be criticized for not having informed the authority at an earlier stage. This can have impact on a possible criminal sanction.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

In general, the assumption is made that an employee has the labor law duty to cooperate as far as the facts to be investigated relate to activities conducted or perceptions made as part of their work life. They must answer work-related questions truthfully and completely and produce relevant documentation to the investigator. If unrelated to work, a balancing of interests test is required to determine if a duty to cooperate exists. A relevant factor may for example be the employee's position in the company. A supervisory function may lead to greater cooperation duties. A balancing of interests also has to be performed in case the employee would be subject to self-incrimination. However, even then, the duty to cooperate generally applies. Thus, refusal may be regarded as violation of obligations under the employment contract. Such misconduct may justify sanctions according to the Employment Protection Act against the employee.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

There is no Norwegian legislation directly initiating deadlines or waiving of employee sanction rights by investigative actions. As mentioned under question 1, internal whistleblower reports shall be handled in accordance with the written guidelines. These guidelines might have regulations limiting the employer's right of actions as long as the investigation is ongoing. Whistleblowing itself shall not be a reason for sanctions against an employee.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

The Personal Data Protection Act, including the GDPR, as a main rule applies to any processing of personal data. This includes securing, collecting and reviewing personal data, as well as the creation of work products such as interview file notes and final reports. Therefore, it is very important to perform an early assessment of the applicable data privacy laws and to document the steps taken.

b) Reviewing emails?

Private communication is highly protected under Norwegian law. If the regulations in the Personal Data Protection Act are not met, e.g. when reviewing employee’s emailboxes, a fine for violation may be issued. Therefore, before conducting such a review, a thorough analysis of legal exposure should always be performed.

c) Collecting (electronic) documents and/or other information?

Norwegian legislation does not have a blocking statute regime. The Personal Data Protection Act incorporates Regulation (EU) 2016/679 (GDPR).

d) Analyzing accounting and/or other mere business databases?

The rules for protection of private communication and private information in the Personal Data Protection Act will normally not apply when analyzing accounting and/or other mere business databases.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no general and statutory obligation to instruct an employee about the legal circumstances and his rights. Nevertheless, it should normally be considered advisable and an ethical duty either to inform an employee about their legal rights, or to offer them free legal assistance before and under the interview. As a minimum, the employee should have a brief description on the background of the investigation and the subject matter. For documentation purposes, it is advisable to provide these instructions in written form and to have them countersigned by the interviewee.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

In contrast to an individual's right to remain silent in case of self-accusation during interrogations of criminal authorities, there is no corresponding right with regard to employee interviews as part of internal investigations. However, there are non-binding provisions of the Norwegian Bar Association recommending private investigators to be aware of the risk and the consequences of any self-incrimination during the investigation process.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

An Upjohn warning should be conducted if relations to U.S. law exist. Besides, giving an Upjohn warning is an accepted best practice in Norway, too. However, there is no explicit legal obligation to do so under Norwegian law.

d) Be informed that they have the right that their lawyer attends?

There is no specific Norwegian law granting an employee a right to attendance of an own counsel during interviews under an internal investigation. However, it is considered to be best practice to allow such attendance to have a fair set-up or if the employee is suspected of having committed criminal offenses. At least under the comprehensive internal investigations conducted by some of the biggest companies in Norway during the recent years, the companies have offered to pay for independent legal assistance to employees being interviewed as a part of the investigation.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

The employee does not have a strict legal right to be attended by a representative of the works council. However, to reduce risks of escalation with the works council and to ensure "equality of arms", companies can allow such attendance.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Regulation (EU) 2016/679 (GDPR) applies to cross-border transfers of personal data. This implies a duty to give information on cross-border transfer of personal data, conf. Chapter III, Section 2, Article 13. It is the responsibility of the data controllers and the data processors to ensure data security according to the Personal Data Protection Act and GDPR in cases of cross-border transfer of personal data.

g) Sign a data privacy waiver?

According to Regulation (EU) 2016/679 (GDPR) Chapter II, Article 6, the employee needs to approve all handling of personal data, as far as no permitting exception of the Regulation applies. In case that personal data of the interviewee might be used for other purposes in the future, such as in later court proceedings, a data privacy waiver of the interviewee can be helpful.

h) Be informed that the information gathered might be passed on to authorities?

According to Regulation (EU) 2016/679 (GDPR) Chapter III, Article 13, information regarding the recipients or categories of recipients of the personal data shall be given.

i) Be informed that written notes will be taken?

It is advisable to inform the employee that notes will be taken during the interview. It can also be advisable to give the employee the opportunity to read and sign the minutes of the meeting, in order to indicate acceptance of and/or agreement with the content.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law governing this question, but issuing such notices is a well-known procedure. Such notices should be clear, be sent to all potentially relevant addressees and be issued as early as possible.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

In Norway, attorney-client privilege rules are more liberal than in many other European countries. Privilege protection can be invoked both in relations with external lawyers and in relations with in-house lawyers.

Privilege protection only applies for regular legal work and advice done and given by lawyers. Thus, when initiating an internal investigation, it is advisable to ensure that the purpose of the investigation is confirmed in an engagement letter, and that the purpose is not limited only to fact finding, but also to give legal advice based on the facts found.

Norwegian attorney-client privilege rules do not only apply for documents in the possession of the lawyer, but among other, also for documents prepared by the client or third party to be used by the lawyer, and advice given by the lawyer to the client.

Even though the Norwegian privilege rules can be considered liberal, several Norwegian companies have found it difficult not to reveal the findings and the basis for the findings of an internal investigation to the authorities if it is publicly known that an internal investigation has been conducted.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

So far, privilege protection applies to legal advice of in-house lawyers. At the moment, there is an ongoing discussion if this practice shall be upheld.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

In general, the policy holder should notify the insurance company as soon as a situation that can trigger or has triggered an insurance event, occurs.

b) To business partners (e.g. banks and creditors)?

Information duties may arise from contractual obligations between the company and the business partner. Even if there is no explicit provision in the contract, there may be an obligation in case of starting an internal investigation if it is highly important information for the other party and relevant with regard to the purpose of the agreement. These interests of the business partner need to be evaluated against the legitimate interests of the company. Therefore, it depends on the individual case whether and when a business partner needs to be notified.

c) To shareholders?

Potential reporting duties towards shareholders compete with the company's intention to maintain (business) confidentiality. Internal investigations are highly important aspects and could be seen as insider information that may possibly influence the stock price. The corporation has to evaluate case by case if there is an *ad hoc* duty to report to the shareholders. If the internal investigation affects the market price significantly and fulfills different criteria (e.g. risk of the internal investigation, scope, involved suspects) an obligation to disclose can exit. In case of a violation of the reporting duties, the company may be held liable to corporate penalty and to pay damages for economic losses.

d) To authorities?

In general, there is no duty to inform the prosecutor about an internal investigation or potential misconduct within the company. There may only be exceptions for very significant crimes. However, a cooperative approach with the local prosecutor may prevent adverse and unexpected measures by the authorities, such as dawn raids.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

The company has to minimize damages and try to prevent new damage to fulfill its supervisory duties. In addition, the company has a duty to stop any ongoing breach of law. Additionally, the company may have to re-evaluate its compliance system in order to eliminate potential deficits and to improve its existing system. Further, the company may impose sanctions on the concerned employees to show that misconduct is not tolerated inside the company.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices generally appreciate internal investigations through external investigators e.g. law firms. Early involvement, communication and coordination may be helpful for a good cooperation with local prosecutors. In this regard, it is crucial that the company does not destroy any potential evidence or convey the impression that evidence is or will be destroyed. Therefore, data retention orders should be communicated at the earliest stage possible.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Both search warrants and dawn raids must fulfill formal and material requirements stipulated by law.
The search warrant in general has to be issued by a district court, or – in case of imminent danger – by the prosecutor. As a main rule, the search warrant should be written and signed. Further, it has to describe the alleged facts and the offense that the individual is being accused of. To issue a search warrant, there must be a reasonable suspicion that an offense was committed. In addition, the search warrant, but also the dawn raid itself, has to be based on reasonable balancing of interest decisions.

When computers and other data carriers are seized, the relevant persons are under obligation to give information about passwords etc. necessary to access the data carriers. The police may also force a person to open data carriers protected by biometric authentication (such as fingerprints).

As a main rule, the involved persons and companies have the right to be informed when a search warrant is executed. If the reason for a search warrant is suspicion of gross crime, including gross corruption, the police can, by approval of the court, execute the search warrant without prior information to the involved persons and companies.

In case these legal requirements are not fulfilled, generally, the seized evidence may still be used in court proceedings. Only in severe cases of illegally obtained evidence, the evidence may not be used in court. This may be the case if there was no reasonable suspicion of a criminal offense or if the decision was made without balancing the interests of the searched person/company with the state's interest to prosecute. Formal legal requirements, such as a missing signature, will generally not lead to a prohibition of use of the seized evidence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

In Norway, there are no statutory rules for plea-bargaining or non-prosecution agreements. However, it is well known that the prosecuting authority, including the National Authority for Investigation and Prosecution of Economic and Environmental Crime ("**ØKOKRIM**"), in numerous of cases has been in dialog with the accused companies before the final indictments have been made. Such dialog can be established to evaluate whether the case can be settled by a fine accepted by the company or if the case has to be brought to court.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

In Norway, companies may be subject to criminal liability based on legal offenses made by the company's employee(s), or by other persons acting on behalf of the company. For a company, the penalty will always be a fine.

Natural persons will never be subject to criminal liability solely based on legal offenses made by other persons. To be subject to criminal liability for legal offenses committed by others, it is a prerequisite that the individual can be held liable as a consenting party. To be held criminally liable as a consenting party, it is generally a prerequisite that the individual physically or psychically supported the principal in his criminal offense and that they were aware of the principal's criminal intentions. For natural persons several different types of penalties are relevant, including fines, imprisonment, and loss of rights.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

If the prosecuting authority and the court find that a natural person has committed a crime and that all other conditions for penalty are fulfilled, the main rule is that a penalty will be applied. If the company at the time of the crime had a compliance system in place suitable for preventing the crime, this can be an argument for a stricter reaction against the natural person who managed to commit the crime anyway.

If a natural person on behalf of a company commits a crime, it depends on a broader assessment if a penalty will be applied against the company. For this decision, it is relevant if the company’s compliance system at the time of the crime was suitable for preventing the crime.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

After "metoo", the most obvious new investigation trend is the increased focus on the employer’s duty to secure a healthy psychosocial work environment and to take measures to avoid sexual harassment. Whistleblowing reports regarding the work environment cause a significant number of internal investigations.

When it comes to financial crimes, an increased focus on anti-money laundering and "know your customers" can be expected.

CONTACT

HJORT

Akersgaten 51
0105 Oslo
Norway

Tel.: +47 22 47 18 00
Fax: +47 22 47 18 18
www.hjort.no

Henrik Boehlke
Partner
Hjort
Admitted to the Supreme Court
T +47 9011 9020
hb@hjort.no

Henrik Boehlke advises primarily on dispute resolution (including arbitration), criminal cases and inquiries. He has extensive litigation experience from both civil commercial disputes and criminal cases (including cases brought by Økokrim – the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime). Henrik is engaged as regular defense attorney by Oslo district court and the Borgarting appeal court. Henrik also advises on commercial law, the law of damages, real estate law and reindeer management law.

Poland

Hogan Lovells (Warszawa) LLP


Agnieszka Majka Celina Bujalska

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

In Poland, specific procedures that need to be considered when a case is reported by a whistleblower apply currently only to financial institutions such as banks and investments firms operating in Poland, as well as certain entities set out in the Polish Act on the Prevention of Money Laundering and Terrorist Financing.

The above entities are legally required to adopt procedures for anonymous reporting of infringements of law, and in case of banks and investment firms, also infringements of internal procedures, and ethical standards. In particular, as part of the procedures, they must ensure that employees who report violations are protected against acts of a repressive nature, discrimination, or other types of unfair treatment.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Under Polish law there is no legal obligation to notify any specific persons or bodies about an internal investigation that a company is about to, or is currently, conducting. There is also no statutory obligation to ensure the participation of employee representative bodies in the investigation.

Nevertheless, if an individual employee requests that a union or work council representative take part in the interview, the employer might want to consider allowing his presence. Moreover, employee representative bodies have to be consulted in connection with certain post-investigation actions involving employees that are members of trade unions, e.g. in case of termination of an employment contract (consultations with company trade union organizations) or changes of an organizational nature (consultations with work councils) as a result of the investigation.

b) There is no statutory obligation to notify the data protection officer about an investigation. However, under Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, (repealing Directive 95/46/EC (General Data Protection Regulation)) (the "**GDPR**"), the Data Protection Officer's ("DPO") general obligation is to monitor compliance of personal data processing with personal data protection regulations. We, therefore. believe, that the DPO should be informed about any investigation, in particular as investigations, as a rule, carry an increased risk to the rights and freedoms of data subjects.

The Data Protection Authority ("DPA") does not have the right to be informed of or participate in, any particular investigation. The DPA may, however, carry out inspections in order to check the compliance of the processing of personal data, under personal data protection regulations.

c) There is no obligation to inform any other local authorities or officials about a pending investigation. Although, parallel cooperation with the prosecution authorities can, under certain conditions, be advantageous.

As the above notifications are not mandatory, no sanctions are imposed in case of non-compliance.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Under Polish employment law, an employee is obliged to care for their employer's interests. There is no other explicit duty for employees to support an investigation. However, as long as an employee's support for an investigation aims at safeguarding the company's interest, the employer can legitimately expect its employees to cooperate within the limits of their employment relationship. Therefore, a refusal to cooperate can, under certain circumstances, be treated as a material breach of the employee's fundamental duties. This would then justify disciplinary measures. The expectation to cooperate should not breach the employee's fundamental rights, including their right to privacy, their right to a defense, or their right to a fair trial.

The question of whether the scope of support corresponds to the employee's tasks must be assessed on a case-by-case basis.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

As a rule, the termination of an employment contract without notice due to the fault of the employee (disciplinary dismissal) cannot come into effect later than one month after the employer learned about the circumstance justifying the termination.

The disciplinary dismissal must be based on credible grounds. According to one of the Supreme Court's recent judgments, the beginning of the above-described time-limit can be calculated from the moment the employer learned of the comprehensive grounds for dismissal after the completion of the internal investigation.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) **Conducting interviews?**
b) **Reviewing emails?**
c) **Collecting (electronic) documents and/or other information?**
d) **Analyzing accounting and/or other mere business databases?**

There are no specific legal boundaries under Polish law that would limit the way an interview is conducted. However, it is advisable that the interview is carried out with an awareness of the employee's fundamental rights, which include, in particular, human dignity, the right to defense, the right to privacy, and the right to a fair trial.

In addition, it would be legitimately expected that an employee will not bear any negative consequences in connection with their participation in the interview. This includes, but is not limited to:

- Confidentiality of their involvement to protect the employee from any social disadvantage in their workplace;
- No extension of working hours by the hours spent in the interview; or
- No requirement to answer questions in a foreign language that the employee does not usually speak during their normal conduct of work.

The interview is also subject to limitations based on the GDPR, or the Act on Classified Information Protection ("**CIP**") if it has been established that the entity where the investigation is taking place, or the relevant persons involved, are authorized to access classified information.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no general or legal obligation to provide the interviewees with any written or oral instructions or inform them about their legal position. It is, however, advisable to, at least, briefly inform the employee about the nature, purpose of, and reason for the interview, as well as to instruct the employee that the interview is confidential. If the employee is expected to cooperate during an investigation, it should be made clear that participation in the interview will not exceed the scope of their employment duties or their knowledge acquired during their employment. In particular, it should be communicated that the employee would not be expected to share any information from the employee's, or another person's private life.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no general or statutory duty to inform the interviewee about their rights, corresponding in nature to a warning by authorities during a criminal investigation in Poland. It is, however, advisable to explain the role of the employee during the interview and that they have the right to avoid answering questions that could incriminate them. The employee will usually feel under pressure, to tell the truth to their superiors, although it could, to some extent, cause serious implications for themself.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

The company will usually be represented at interviews by lawyers whose role should, for the avoidance of any unnecessary doubt or confusion, be explained to the employee. The company is not required to provide an Upjohn warning, however, maintaining clarity during the interview is highly recommended.

d) Be informed that they have the right that their lawyer attends?

There is no obligation to inform an employee of their right to have a lawyer attend the meeting. Whether or not a lawyer can even attend is controversial and should be assessed in each individual case.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

As an employee cannot effectively expect the attendance of such bodies, there is also no obligation to inform the employee of this right.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The interviewee must be provided with information required under Articles 13 or 14 GDPR, in particular informed that data could be transferred cross-border.

g) Sign a data privacy waiver?

Under Polish privacy laws, the interviewee is not required to sign a data privacy waiver. However, the information on the processing of personal data, required under Articles 13 or 14 GDPR, respectively, should be provided to the interviewee. For evidentiary purposes, it is advisable to obtain a signed confirmation that the interviewee received the relevant information.

h) Be informed that the information gathered might be passed on to authorities?

There is no legal obligation to inform the interviewee that the data might be passed on to authorities. However, it is advisable to warn the employee of this possibility.

i) Be informed that written notes will be taken?

If one of the people attending the interview is taking notes, it is advisable to explain the role of this person, along with the purpose for which the notes are being taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no formal requirement for issuing document hold notices, or other specifics to be observed under Polish law. However, these documents are allowed and recommended.

The above rule does not apply to public and local government institutions that, in connection with their activity, become aware of an offense to be prosecuted *ex officio*. These entities are not only obliged to immediately report an offense to the authorities and undertake the necessary actions but also to prevent the loss of traces or evidence.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege can be claimed over the findings of an internal investigation if these have been elaborated by the attorneys and/or communicated to the client within the scope of the legal assistance that they provide to the company.

In order to ensure privilege protection, communication with attorneys and attorney-client work products should be labeled as privileged and confidential (Polish: Objęte tajemnicą adwokacką/radcowską). It is recommended that all documents or advice are communicated to the company via external servers where documents are uploaded and accessible only to designated persons.

During dawn raids, the company's employees or outside counsel should inform the enforcement authorities which documents and data are privileged, making sure that they are left unread and that the investigators place them in sealed packages. Information about the seizure of privileged documents should be documented in the dawn raid protocol. Privileged documents or data can be used as evidence only if it is indispensable for justice, and if a particular fact cannot be established otherwise. Using privileged documents as evidence is only possible on the basis of a court decision. However, documents that cover circumstances related to the performance of a defense counsel's function can never be used as evidence in criminal proceedings. If an external advisor (e.g. forensic services) is involved, sub-contracting should take place through an outside legal counsel in order to safeguard legal privilege.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Yes, as long as the in-house counsel acts in its capacity as an attorney (Polish: radca prawny) and provides legal assistance to the company.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Although the commencement of an investigation does not necessarily mean that any irregularity in fact existed, there may be a company's obligation to notify the insurance company. This will usually depend on the terms of the insurance agreement.

b) To business partners (e.g. banks and creditors)?

This is usually not required unless the agreements between the parties expressly state so.

c) To shareholders?

There is generally no formal requirement to notify the shareholders of an investigation, unless the investigation or the underlying facts have the potential to have significant impact on the financial situation of the company. In practice, the decision should be made on a case-by-case basis depending on the shareholder structure and the effect of the case upon the business.

d) To authorities?

Under Polish law, there are no specific notifications required when starting an investigation. Only the findings of an investigation or the irregularities that triggered the investigation, in certain cases, need to be notified to the relevant authorities.

As a rule, anyone who becomes aware of an offense that is prosecuted *ex officio* has a social duty, rather than a legal obligation, to notify the public prosecutor.

This does not apply to public and local government institutions, which are obliged to immediately report offenses to the authorities if they became aware of an offense prosecuted *ex officio* in connection with their activity.

A legal obligation to notify the authorities rests upon anyone who has reliable information about certain most serious criminal offenses (e.g. terrorist offenses, offenses against humanity, or homicide). Moreover, under the Polish Act on the Prevention of Money Laundering and Terrorist Financing, the obliged institutions are required to notify the General Inspector of suspicions of money laundering or terrorist financing.

Depending on the type of irregularity revealed in connection with an investigation, certain other notification requirements might apply. This includes, but is not limited to, product safety issues, which need to be notified to the product surveillance authorities together with the information as to which actions have been taken to prevent possible threats posed to consumers.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There are no specific measures that a company would be expected to undertake. However, it is advisable to consider the potentially required actions at every milestone of the investigation, and to seek advice from an external counsel.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

It is very rare that criminal authorities become involved in an internal investigation of a company in any way. However, it is possible that, at the same time, a related investigation is pending at the prosecutor's office. In this case, it is highly advisable to cooperate with the authorities. However, every interaction should be undertaken in close cooperation with external counsel.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

A dawn raid can be conducted by the public prosecutor, by the police, or another authorized agency (e.g. the Central Anti-Corruption Bureau, or the Internal Security Agency) acting upon an order from the court or the public prosecutor. Prior to the actual searching process, the person or entity must be summoned to voluntarily hand over the requested documents/devices. As a rule, a person whose premises are to be searched should be provided with a search warrant issued by the court or the public prosecutor. The documents to be seized should be covered by the scope of the search warrant. However, in urgent cases, the search can take place upon an order from the head of its

unit, or even upon the official identity card of the official. The court or public prosecutor's decision approving the search must be requested in the search protocol and delivered within seven days from the day of searching.

Specific rules apply to documents containing classified information, information constituting a professional secret, other legally protected secrets, or containing private information. If any of these documents are seized, the company should alert the investigators about the potential breach of secrecy. The investigators should then refrain from reading them and refer the documents to the prosecutor or court in a sealed package. Subsequently, to use the documents containing classified information or information constituting a professional secret as evidence, the court or the prosecutor has to issue a decision in this respect. Attorney documents for the purposes of criminal defense can never be used as evidence in criminal proceedings.

Using evidence gathered by public officials (e.g. police officers, or prosecutors) in breach of these rules is inadmissible.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Deals, non-prosecution agreements, or deferred prosecution agreements are not available for corporations under Polish law.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Under the Polish Criminal Corporate Liability Act, a company can be found criminally liable and sanctioned for the misconduct of individuals of the company. The company can be fined with a financial penalty of up to 3 percent of their revenue earned in the business year in which the offense was committed. Forfeiture or various prohibitions or loss of benefits are also potential sanctions as well as publication of the judgment which can be severely detrimental to the company's reputation.

Polish criminal law does generally not stipulate criminal liability for individuals for the acts or omissions of third parties. Under limited circumstances, directors, officers, or employees can be subject to fines because of acts or omission of others, for example, if they failed to observe supervisory or monitoring duties and therefore allowed misconduct by a person or body.

The above offenses create individual criminal liability of individuals for their own failure to observe their duties and do not create liability for offenses committed by someone else.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

The Criminal Corporate Liability Act does not provide for any explicit reduction or suspension of penalties in case the company implemented an efficient compliance system. Nevertheless, the functioning of the compliance system could be taken into account by the court during the assessment of the company's liability and/or determination of the amount of penalty.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

In January 2019 the Ministry of Justice submitted to the Polish Parliament a bill of the Criminal Corporate Liability Act. The bill was aimed at entirely changing the rules of corporate criminal liability in Poland. It introduced concepts such as (i) corporate criminal liability becoming independent of a physical person's liability, (ii) significant

increases in financial penalties, and (iii) the introduction of general whistleblower protection under Polish law. The bill was said to be one of the top priorities of the government.

After its submission, however, no reading of the bill has been held in the former Parliament. Although the same party won the parliamentary elections in October 2019, it is unclear whether the bill will be subject to consideration by the current Parliament.

CONTACTS

Pl. Trzech Krzyży 10/14
00-499 Warsaw
Poland

Tel.: +48 22 529 29 00
Fax: +48 22 529 29 01
www.hoganlovells.com

Portugal

Uría Menéndez Abogados, S.L.P.

Nuno Salazar Casanova

Melissa Pereira Filgueira

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

The treatment of whistleblowers and their corresponding reports is laid down in various specific laws in Portugal.

(i) Corruption and Economic and Financial Crime Law ("**Law 19/2008**")

Pursuant to Law 19/2008, a whistleblower who reports any infraction, the knowledge of which results from the performance of their professional duties, must not in no manner be hampered. Furthermore, the imposition of any disciplinary penalties on the whistleblower within a one-year period following the communication of the infraction is presumed to be unfair.

Additionally, whistleblowers are entitled to:

- Anonymity until the pressing of charges;
- Be transferred following the pressing of charges; and
- Benefit from the witness protection program within criminal proceedings. Under the program, the whistleblower will remain anonymous upon the verification of specific circumstances.

(ii) Money Laundering and Terrorism Financing Law ("**Law 83/2017**")

Law 83/2017, as amended, sets forth the legal framework to prevent, detect and effectively combat money laundering and terrorism financing. Law 83/2017 applies to financial entities and legal or natural persons acting in the exercise of their professional activities (e.g. auditors and lawyers) (collectively, "**Obliged Entities**").

Pursuant to Article 20 of Law 83/2017, individuals who learn of any breach by virtue of their professional duties must report those breaches to the company's supervisory or management bodies. As a result, the Obliged Entities must refrain from threatening or taking hostile action against the whistleblower and, in particular, from any unfair treatment within the workplace. Specifically, the report cannot be used as a ground for disciplinary, civil or criminal action against the whistleblower (unless the communication is deliberately and manifestly unjustified).

Article 108 of Law 83/2017 also sets forth the right to report any breaches — or evidence of breaches — to the sectoral authority.

(iii) Legal Framework of Credit Institutions and Financial Companies ("**RGICSF**")

Under Portuguese law, credit institutions must implement internal-reporting mechanisms that must guarantee the confidentiality of the information received and the protection of the personal data of the persons reporting the breaches as well that of the persons charged. Pursuant to Article 116-AA of RGICSF, the persons who, as a result of the duties performed in a credit institution, become aware of

- any serious irregularities in the management, accounting procedures or internal control of the credit institution; or
- evidence of breach of the duties set out in the RGICSF which may cause any financial imbalance

must communicate those circumstances to the company's supervisory body. Those communications cannot, *per se*, be used as grounds for disciplinary, criminal or civil liability actions brought by the credit institution against the whistleblower.

Moreover, Article 116-AB of RGICSF establishes that any person who is aware of compelling evidence of a breach of the statutory duties may report it to the Bank of Portugal. Such communications cannot, *per se*, be used as grounds for disciplinary, criminal or civil liability actions brought by the credit institution against the whistleblower, except if the report is manifestly unfounded.

The Bank of Portugal must ensure adequate protection of the person who has reported the breach as well as of the person accused of breaching the applicable duties. It must also guarantee confidentiality of the identity of the persons who have reported breaches at any given time.

(iv) Portuguese Securities Code ("**CVM**")

Article 382 of the CVM establishes that financial intermediaries with registered office, head office or branches in Portugal that, within the performance of—and due to—their activity or position, become aware of facts that qualify as crimes against the securities market or against the market of other financial instruments, must immediately inform the board of directors of the Portuguese Securities Market Commission ("**CMVM**").

Additionally, pursuant to Article 368-A of CVM, any person aware of facts, evidence or information regarding administrative offenses under the Portuguese Securities Code or its supplementary regulations, may report them to the CMVM either anonymously or including the whistleblower's identity. The disclosure of the whistleblower's identity, as well as that of their employer, is optional. If the report identifies the whistleblower, their identity cannot be disclosed, unless specifically authorized by the whistleblower, by an express provision of law or by the determination of a court.

Although the CVM allows for the possibility of submitting an anonymous communication, this approach is not supported by the Portuguese Data Privacy Authority ("**CNPD**"). The CNPD takes the more conservative stance that anonymity should be rejected in order to prevent false accusations.

In any case, such communications may not, *per se*, be used as grounds for disciplinary, criminal or civil liability action brought against the whistleblower. Nor may such communications be used to demote the employee.

Pursuant to Article 368-E of the CVM, the CMVM must cooperate with other authorities within the scope of administrative or judicial proceedings in order to protect the employees against employer discrimination, retaliation or any other form of unfair treatment by the employer, that may be linked to the communication to the CMVM. The whistleblower must be entitled to benefit from the witness-protection program in the event of the individual's participation in criminal or administrative-offense proceedings related to the communication to the CMVM.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Employee-representative bodies are not entitled to be informed about or to participate in the investigation before an internal investigation has started. The works council is only entitled to participate in disciplinary proceedings after a formal accusation has been made against the employee.

b) The Data Protection Officer ("**DPO**") must be involved in all issues relating to the protection of personal data. As such, it is generally recommendable to inform the DPO of the internal investigation prior to its commencement and to involve the DPO throughout the course of the same. The CNPD needs not be informed prior to the start of each internal investigation and will only be involved if a complaint is filed concerning the employer.

c) The prosecution authorities do not have the right to be informed; however, voluntary involvement and a cooperative stance can be advantageous in case of a potential conviction.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Upon the decision of the Board of Directors or management to carry out an internal investigation to assess potential wrongful acts carried out within the company, employees are bound to cooperate. However, employees are entitled to the privilege against self-incrimination established in the Portuguese Criminal Code, according to which individuals are not obliged to self-report.

An employee's refusal to cooperate in an internal investigation may be regarded as a breach of their duty of obedience towards the employer, permitting the company to impose disciplinary measures on the respective employee.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

The employer must commence the disciplinary proceeding within 60 days of becoming aware of the relevant facts (i.e. identification of the party responsible and a detailed description of the circumstances of the infringement). The 60-day deadline can only be interrupted by the presentation of the notice of misconduct ("*nota de culpa*") to the employee. If the employer lacks detailed knowledge of the circumstances of the infringement, the employer must commence the preliminary enquiry proceedings within 30 days of the suspicion of irregular behavior.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

The GDPR and Law 58/2019, of 8 August ("**Law 58/2019**") concern any processing of data.

b) Reviewing emails?

Private communications are highly protected under Portuguese law. The Portuguese Constitution establishes the right to privacy and the inadmissibility of evidence collected with an abusive intrusion into the personal life, residence, communications or telecommunications of citizens. The Portuguese Labor Code ("**PLC**") establishes the general principle of the confidentiality of personal messages and non-professional

information. Law 58/2019 and Resolution 1638/2013 of the CNPD establish a prohibition of access by the company in connection with any messages of the employee of a personal nature and any non-professional information. Therefore, the employee's express consent is required for the processing of private or non-professional information.

c) Collecting (electronic) documents and/or other information?

Please refer to the answer to question 5b above.

d) Analyzing accounting and/or other mere business databases?

There are no relevant laws that must be taken into account before analyzing accounting and/or other business databases.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no general and statutory obligation to provide written instructions to the employee.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

Pursuant to Portuguese law, the interviewer is not obliged to inform the interviewee that they must not make statements that would mean any kind of accusation. However, individuals are not obliged to self-report any wrongdoing to the company or to any authorities concerning crimes or administrative offenses.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

Pursuant to Portuguese law, the interviewer is not obliged to formally inform the interviewee that they are the company's lawyer, although it is recommendable to do so.

d) Be informed that they have the right that their lawyer attends?

Pursuant to the statutes of the Portuguese Bar Association, the assistance of a lawyer is allowed at all times and cannot be prevented in any jurisdiction or by any authority, public or private entity, specifically for the defense of rights or within verification procedures. Therefore, and although case law is not settled regarding this matter, it is generally recommendable to inform the employee that they are entitled to be assisted by a lawyer.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is no legal right for the interviewee to be assisted by a representative from the works council.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The employee must be informed and their consent must be requested. Pursuant to the GDPR, the transfer of data to non-EU countries is only allowed if the conditions established in Chapter V of the GDPR are satisfied by the controller and by the processor.

g) Sign a data privacy waiver?

The employee generally must sign a data-privacy waiver concerning personal data and non-professional information before the interview takes place. The waiver could be of subsequent use in potential judicial proceedings.

h) Be informed that the information gathered might be passed on to authorities?

The employee should be informed of the possibility of passing the collected information to authorities. Moreover, under Law 58/2019 and the PLC, the images and other personal data recorded through the use of video or other remote surveillance mechanisms may only be used within the scope of criminal proceedings (and within the scope of disciplinary proceedings insofar as it is used within criminal proceedings).

i) Be informed that written notes will be taken?

The employee generally must be informed that written notes will be taken during the interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law governing this matter. However, issuing document hold notices is common in Portugal. Such notices should be clear, detailed, clearly delimited and issued as early as possible. The scope of the hold notices can only include information of an exclusively professional nature given that companies are generally prohibited from accessing non-professional information. Please refer to the answer to question 5b above.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Should the internal investigation be conducted by lawyers, companies may claim attorney-client privilege over any findings arising from the investigation. In fact, any attorney-client relationship is subject to strict duties of professional secrecy regarding facts and circumstances acknowledged exclusively by the disclosure of the respective client. The duty of professional secrecy can only be waived under exceptional circumstances and at the request of the concerned attorney to the president of the respective Regional Council of the Portuguese Bar Association.

Additionally, companies are also protected from self-incrimination as established in the Portuguese Criminal Code. Please refer to the answer to question 3 above.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Yes. Attorney-client privilege is also applicable to documents created by — and communication with — in-house counsel.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

These notifications are generally not required, unless specifically established in the respective insurance policy.

b) To business partners (e.g. banks and creditors)?

These notifications are generally not required, unless established in a specific contract.

c) To shareholders?

These notifications are generally not required. However, if the internal investigation concerns an issuer of financial instruments, the company is obliged to inform the public, as soon as possible, of inside information directly concerning that issuer. Pursuant to Article 7 of Regulation 596/2014 of the European Parliament and the Council of 16 April 2014, and to Article 248-A of the CVM, the concept of inside information includes, *inter alia*, information of a *precise nature* that has not been made public, relating directly or indirectly, to one or more issuers of *financial instruments* or to one or more financial instruments that, if made public, would be likely to have a *significant effect* on the prices of those financial instruments or on the price of the derivative financial instruments.

d) To authorities?

These notifications are not required. However, voluntary involvement of the authorities and a cooperative stance can be advantageous in the event of a potential conviction.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

The start of an internal investigation does not trigger any measures to be taken with regard to authorities. The company should, however, ensure that any alleged ongoing breach of law by the company or its employees is ceased immediately.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices do not ask for specific steps to be observed nor do they have any concerns about internal investigations. Additionally, Portuguese law does not establish a general duty to report criminal or administrative offenses to the local prosecutor's offices. However, voluntary involvement of the authorities and a cooperative stance can be advantageous in the event of a potential conviction. Nevertheless, the conclusions drawn in internal investigations may be used by the prosecutor's office against the company as evidence of misconduct; as such, the voluntary involvement of the authorities should be thoroughly considered when initiating internal investigations.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Pursuant to the Portuguese Criminal Procedure Code ("**PCPC**"), searches and seizures are admissible upon the verification of the formal and material legal requirements.

Searches must be authorized, ordered or validated by a judicial authority, if there is reasonable evidence that any objects related to a crime or which may be used as evidence are within a private or restricted space. The judicial warrant will be valid for 30 days.

Seizures must also be authorized or ordered by a judicial authority. Police authorities may carry out a seizure during the course of a search when there is urgency or a danger in delay. In such cases, the seizure must subsequently be validated by the judicial authority within the following 72 hours. The seizure of communications must be authorized or ordered by a judge. The seizure of personal documents or documents covered by legal privilege is strictly forbidden. Please refer to the answer to question 5b above.

Within financial institutions, the seizures of documents, securities, valuables, monetary amounts and other objects should be carried out personally by a judge (with the assistance of the police authorities, if needed), upon the verification of sound reasons that they are linked to a crime.

Evidence collected in breach of these formalities is deemed inadmissible, and therefore cannot be used against the company.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Outside of specific lenience provisions, any deals and non-prosecution agreements entered into by legal or natural persons are strictly prohibited. As a result, evidence collected within criminal proceedings upon (unlawful) promises of leniency is inadmissible. However, under certain circumstances the prosecutor's office may agree not to indict the defendant and suspend the criminal proceedings (*suspensão provisória do processo*) until specific injunctions undertaken voluntarily by the defendant are performed and close the proceedings after they are performed. Those circumstances may, for example, be crimes punishable by imprisonment of no longer than five years, lack of a previous conviction for a crime of the same nature, lack of a high degree of guilt or acceptance by the victim's assistant to the prosecution. This possibility should not be considered a deal insofar as the prosecutor's office is theoretically bound to suspend the proceedings if the legal requirements are met. Despite not being considered a deal, some of the requirements are highly subjective (e.g. the lack of a high degree of guilt) and the

prosecutor's office therefore has, in practice, discretionary power. The prosecutor's office is therefore undoubtedly tempted to demand cooperation from the suspect in return for the suspension of the proceedings.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

The main penalties imposed upon companies include fines or, when the company has been incorporated with the exclusive or primary purpose of committing crimes, dissolution. Potential ancillary sanctions include judiciary injunctions, prohibitions against pursuing specific activities or applying for subsidies or grants.

Corporate liability does not exclude individual liability; natural persons may be subject to sanctions such as imprisonment, fines, dismissal with just cause and potentially debarment from respective professional associations.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Pursuant to the Portuguese Criminal Code, the existence and effective implementation of adequate compliance systems within the company prior to the alleged misconduct can potentially exclude corporate liability. This may apply in case the individual acted in contravention of specific orders or instructions issued by the corporate body or entity.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The Portuguese government has set up a working group with a view to studying the possibility of implementing specific anti-corruption measures. A report on the findings of the working group was published in September 2020. The working group recommended, *inter alia*, the assessment of allowing for the possibility of entering into deals concerning the applicable sanctions (and not concerning the criminal culpability), during the trial stage of the criminal proceedings, based on a willing and voluntary confession of the defendant.

CONTACTS

URÍA MENÉNDEZ
PROENÇA DE CARVALHO

Edifício Rodrigo Uría
Praça Marquês de Pombal, 12
1250-162 Lisboa
Portugal

Tel.: +351 21 030 8600
Fax: +351 21 030 8601
www.uria.com

Nuno Salazar Casanova
Partner
Uría Menéndez – Proença de Carvalho
T +351 21 030 8609
nuno.casanova@uria.com

Nuno Salazar Casanova has been a lawyer in the litigation practice area of Uría Menéndez Proença de Carvalho's Lisbon office since 2004. He was made partner at Uría Menéndez – Proença de Carvalho in January 2015.

Mr. Casanova leads high-profile often cross-border disputes, including regulatory investigations and enforcement, class actions and other major reputation-threatening litigation, especially where a global strategy is required to deal with litigation that is intertwined simultaneously with civil, criminal, regulatory and administrative issues.

He has ample experience in representing clients before the public prosecution office in investigations involving corporate and economic crimes and before supervisory authorities in infringements to banking, finance, securities, and environmental law.

Melissa Pereira Filgueira
Associate
Uría Menéndez – Proença de Carvalho
T +351 21 030 8600
melissa.filgueira@uria.com

Melissa Pereira Filgueira joined Uría Menéndez – Proença de Carvalho in 2014 as a trainee lawyer, and became an associate in 2019.

She focuses her practice on a wide range of litigation and arbitration matters, including civil, commercial, criminal, and administrative proceedings.

Romania

Mareş & Mareş

Dr. Mihai Mareş

Overview

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

Question List

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Romania has adopted a special law for the protection of whistleblowers, in force since 2004, namely Law No. 571/2004. However, it applies only to personnel hired within public authorities, public institutions, and other budget units. Private-sector employees are not protected by this law.

Law No. 571/2004 offers protection before the discipline commission or other similar bodies, as follows:

- Whistleblowers benefit from the presumption of good faith, until proven otherwise.
- At the request of the whistleblower, following a warning act, disciplinary commissions or other similar bodies within public authorities or public institutions have the obligation to invite the press and a representative of the trade union or professional association.
- If the wrongdoer is a hierarchical superior, directly or indirectly, or has control, inspection or evaluation powers over the whistleblower, the disciplinary commission or other similar bodies will ensure the protection of the whistleblower by concealing their identity.

In case the whistleblower reports on corruption offenses, offenses assimilated to corruption offenses, forgery offenses, offenses committed in office or work-related offenses, and offenses against the financial interests of the European Union, the protection measures set out under Article 12 paragraph 2 of Law No. 682/2002 on the protection of witnesses shall be applied *ex officio*.

In labor disputes or in those regarding labor relations, the courts may order the annulment of the disciplinary or administrative sanction imposed on a whistleblower, if the sanction was applied following a report done by the whistleblower in good faith.

Regarding the protection of whistleblowers in the private environment, some degree of protection is currently offered indirectly under Romanian law. For instance, an employee cannot be dismissed solely on grounds of submitting a whistleblower report that set off an internal investigation. This is due to the fact that, pursuant to the Romanian Labor Code, there are strict conditions that must be met for a dismissal of an employee. Reporting misconduct is none of the conditions under this law.

The Whistleblowers Directive – Directive (EU) 2019/1937 – will result in a harmonization of the legal provisions governing whistleblowers until 2021 for all EU Member States, including Romania.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) The only set of general provisions regarding internal investigations are to be found in the Romanian Labor Code, regulating the disciplinary investigation of an employee in case of disciplinary misconduct. There are also specific procedures for internal disciplinary investigations, particularized for specific professions.

Disciplinary misconduct is a work-related act consisting of an action or omission committed by the employee, thereby violating the legal provisions, the internal regulation, the individual employment contract or the applicable collective labor contract, the orders and the lawful commands of hierarchical leaders.

In case of an internal disciplinary investigation, the law requires that the employee be summoned in writing for an interview, by the person empowered by the employer to carry out the investigation. If the employer does not comply with this requirement, a decision of sanctioning the employee will be void.

The only measure that may be ordered without carrying out a disciplinary investigation is the warning.

There is no other obligation for informing other people or employee representative bodies.

An employee who is being disciplinarily investigated has the right to request that a member of the trade union, of which they are a member of, participates in the interview.

For any other type of misconduct, the law does not provide any regulations for conducting an internal investigation. Nevertheless, provisions regarding internal investigation for other types of misconduct may be provided by internal regulations of any legal person.

b) The Romanian Law does not impose an obligation for a data protection officer or data privacy authority to be informed about the investigation. Nevertheless, in case the operator detects a data security breach, the Romanian Data Protection Authority must be notified.

c) In accordance with Article 267 of the Romanian Criminal Code, if a public servant becomes aware of a criminal offense that is related to the work place where they carry out their job duties, the public servant must immediately refer it to the criminal prosecution body. Otherwise, the public servant may be subject to criminal liability punishable with imprisonment of three months to three years or with a fine, when committed willfully, or imprisonment of three months to one year or by a fine, when committed negligently. There is no such reporting obligation of an employee of a private sector company.

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

There is no explicit obligation of this nature under Romanian law in case of an internal disciplinary investigation. The employee that is summoned to an interview does not have a duty to support the investigation and they may participate in the interview or not. Also, they may provide information regarding the accusation brought against them, or not. However, if the employee unjustifiably refuses to adhere to their employee's instruction to appear, the company may impose disciplinary measures without having to perform the prior disciplinary investigation.

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

According to the Romanian Labor Code, following a disciplinary investigation, the employer can apply a sanction within 30 calendar days as of becoming aware of the disciplinary misconduct, but no later than six months from the date of the act.

Regarding the first time-period, of 30 calendar days, the Romanian Supreme Court established that the term will start to run from the date when the employer took note of what is written in the report following the disciplinary investigation.

Should any of the two time-periods lapse, the employer loses the right to sanction the respective employee.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Data privacy laws or laws protecting classified information apply to any type of data processing, as the case may be.

The relevant legal framework applicable in Romania essentially comprises the following pieces of legislation:

- The Romanian Criminal Code: Articles 226 (violation of privacy), 302 (violating privacy of correspondence), 303 (disclosure of information classified as state secret), 304 (disclosure of information classified as professional secret or not public), 305 (negligence in storing information);
- Regulation (EU) 2016/679 – the General Data Protection Regulation ("GDPR");
- Directive (EU) 2016/680 – the Data Protection Directive (transposed in Romania mainly through Law No. 363/2018 regulating data protection and other pieces of domestic legislation);
- Law No. 129/2018 amending and supplementing Law no. 102/2005 regarding the establishment, organization and function of the National Supervisory Authority for the Processing of Personal Data, as well as for the repeal of Law No. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data;
- Law No. 182/2002 regarding classified information.

b) Reviewing emails?

Private communication is protected under Romanian Law, and access to private communications is permitted only under the conditions set out by law, namely if it is approved in advance by a judge and enforced by the judicial bodies.

Otherwise, accessing an email without permission may constitute the criminal offenses of violating the privacy of correspondence (as per Article 302 of the Romanian Criminal Code) and of accessing a computer system illegally (Article 360 Criminal Code).

Criminal liability may be excluded and such private communication may be used without impunity if it was originally viewed accidentally and only if it proves the perpetration of an offense or if it serves a general interest (e.g. acts of public interest, meaningful for the community), of higher import than the potential damage caused.

In this context, when assessing the lawfulness of accessing professional emails used within an organization, the ownership of the information contained therein must be established as a first step; either it is deemed to belong to the employer or it is attributed solely to the employee.

c) Collecting (electronic) documents and/or other information?

Any and all processing of documents and/or data must take into account the applicable provisions of data privacy laws. In case of an internal investigation the company holds ownership over the equipment used and data/information processed by the employee under employment provisions. As such, the employer may

secure, collect and review such work data and work products, subject to an assessment of the applicable data privacy laws.

On the contrary, accessing/collection of documents or information exceeding the scope of work relations may only be permitted to state authorities, pursuant to special legal procedures (e.g. searches and seizures).

d) Analyzing accounting and/or other mere business databases?

Analyzing private databases is only permitted pursuant to the procedures provided for by law (e.g. expert reports). Any professional accounting and/or business databases pertaining to labor relations between the employer and their employees generally constitute the property of the employer, thus being fully accessible to such employer.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no legal obligation to provide written instructions to an employee regarding legal circumstances or their rights. Nevertheless, the company internal regulation, which shall be made available to all employees, must contain specific provisions and information as to the disciplinary procedures enforced by such company.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

The Romanian Criminal Procedure Code provides that a suspect or a defendant will be informed about the right to remain silent during interrogations conducted by the judicial bodies. There is no corresponding obligation for other types of interviews, including interviews as part of an internal investigation.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no obligation for an Upjohn warning under Romanian law.

d) Be informed that they have the right that their lawyer attends?

According to Article 251 paragraph 4 of the Romanian Labor Code, during an internal disciplinary investigation, the employee, who allegedly committed the wrongdoing, has the right to defend themself and to give the person empowered to carry out the investigation all the evidence and motivations they consider necessary. The same paragraph offers the employee access to a lawyer, upon request. However, there is no explicit legal obligation of the employer to inform their employees about that right. The company's internal regulation, which shall be made available to all employees, must however contain specific provisions in that regard.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Article 251 paragraph 4 of the Romanian Labor Code provides the employee the right to be assisted, at their request by a representative of the trade union of which they are a member of in case of a disciplinary investigation. The company's internal regulation, which shall be made available to all employees, must contain specific provisions in that regard. However, there is no explicit legal obligation of the employer to inform their employees.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

According to the provisions of Law No. 363/2018 as well as the relevant European legal provisions (GDPR), the data subject has to be informed of the purpose of data processing. This also includes any processing of personal data conducted during an internal investigation. The information process also has to include any references to where the personal data is transferred to and the rights of the data subject in relation to such processing.

In order to avoid any further approvals from the Romanian Data Protection Authority for transferring the personal data to the U.S., data subject consent for such transfer is compulsory. In all other cases, transfers of

personal data are based on a decision of adequacy from the European Commission or based on adequate guarantees.

g) Sign a data privacy waiver?

Under Romanian law, the employer is not obliged to ask the employee to sign a data privacy waiver. However, in practice, the employer will request such document to be signed for evidentiary purposes.

The right to the protection of personal data, which applies to all employees, implies the right to information regarding all relevant data privacy matters (such as the identity of the operator, the purpose of data processing, the rights of the persons concerned and the conditions for exercising them), the right of access to data, the right to rectification and erasure of data, the right to restriction of processing, the right to data portability as well as the right to opposition.

h) Be informed that the information gathered might be passed on to authorities?

There is no obligation for the employer to inform the employee of passing information to authorities under Romanian law.

i) Be informed that written notes will be taken?

There is no obligation for the employer to inform the employee that written notes will be taken under Romanian law.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no legal provision under Romanian Law for this kind of activity. Thus, such notices are allowed and are generally in the discretion of the employer.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege may be claimed over findings of the internal investigation.

According to the Lawyer Profession Statute, the lawyer is required to keep professional secrecy on any aspect of the case entrusted to them.

The professional secrecy applies to any information and data of any kind, in any form and on any support, as well as any documents drawn up by a lawyer containing information or data provided by the client or based on them for the purpose of providing legal assistance and whose confidentiality has been requested by the client.

In order to ensure privilege protection, any documents, information, or data regarding an investigation should be kept only at the professional headquarters of the lawyer – which can also be situated at the lawyer's domicile – or in areas approved by the Bar. Documents of professional nature are inviolable.

Also, for ensuring the professional secrecy, correspondence with a client or notes regarding the defense of a client are exempted from seizure and confiscation. Moreover, the lawyer-client relationship cannot be subject to technical surveillance measures unless strictly prescribed by law.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

In case the lawyer is an active member of the Bar and is not bound by an employee-employer relation but exercises the legal profession based on an agreement of legal services, the attorney-client privilege will apply under any circumstances in regard to the documents, data and information mentioned at question 8.

---

10. Are any early notifications required when starting an investigation?

As a general principle, we note that there is no legal obligation under the Romanian law for such notifications, unless they are necessary under respective financing or insurance contracts of the respective legal entity. As such, a case by case evaluation must be performed, as to the subject matter of the internal investigation, by reference to any stakeholders, including the below.

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

To the extent that the internal investigation may generate any liability or claim under the employer's/employee's insurance policies, the specific notification obligations under the insurance policy must be thoroughly observed. Moreover, special attention should be paid to the timelines and deadlines provided by such insurance documentation, as their lapse may prevent a successful insurance claim.

b) To business partners (e.g. banks and creditors)?

Specific contractual provisions pertaining to the respective business partnership must be reviewed and analyzed in order to determine potential reporting obligations arising from an internal investigation.

c) To shareholders?

To the extent that the subject matter of the internal investigation may be interpreted as a potential trigger on the company's stock price, a thorough analysis should be performed as to whether the matter of the internal investigation should be notified to the regulatory/supervisory authorities and/or to the company shareholders (including the legal provisions on insider trading).

Specific criteria must be met in order for the internal investigation to be subject to the company's legal notification obligations. Nevertheless, if such conditions are met and the company fails to report it to the supervisory authority, its liability may be incurred.

d) To authorities?

There is no specific duty to inform criminal law authorities when conducting an internal investigation. Nevertheless, the company may find it in its best interest to immediately inform the prosecutor's office if and as soon as the internal investigation uncovers acts that meet the specific criteria of criminal offenses.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

If a company becomes aware of a breach of laws by the company or its employees, the company must take all suitable steps to end such behavior.

Also, as described above, a public official that gains knowledge of the commission of criminal actions pertaining to the workplace in which the said public official fulfills their duties has to immediately refer to the criminal prosecution body.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

The prosecutor's offices will not be concerned about internal investigations.

In any case, if a criminal offense has been committed and the prosecutor office learns about it, either *ex officio*, or through complaint or denunciation, there is an obligation for criminal proceedings to be initiated.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

The domiciliary search warrant in Romania must be issued by a judge of a court of law and its content must comply with certain formal requirements.

The search can be conducted only by the prosecutor, or by criminal investigation bodies, accompanied, as applicable, by operative workers.

Searches cannot be initiated before 6.00 a.m. or after 8.00 p.m., except for in-the-act offenses, or when a search is to be conducted in a place open to the public at that time.

In case the legal prerequisites are not fulfilled, the evidence may be subject to exclusion, carried-out through the nullity sanction.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

The Romanian Criminal Procedure Code allows for the conclusion of a plea bargain between the defendant and the prosecutor. This possibility is also available to legal entities, although less common in practice. The effects of such agreement are the reduction of the penalty limits provided by law for a particular offense by one-third in case of prison sentences or one-fourth in case of criminal fines.

In the trial phase, the admission to the charges may entail special, more expeditious proceedings, which also result in the reduction of the penalty limits as indicated above.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

A company can face either criminal or administrative penalties in Romania.

As far as criminal penalties are concerned, the primary penalty for companies is fines. Depending on the offense, companies may also face the following complementary penalties:

- Liquidation;
- Suspension of the activity, or of one of the activities performed thereby;
- Closure of individual company sites;
- Prohibition to participate in public procurement proceedings;
- Placement under judicial supervision; and/or
- Display or publication of the conviction sentence.

The directors, officers, or employees, as individuals, can face fines, imprisonment, or disciplinary measures, depending on the nature of the misconduct. Also, some of their rights may be restricted as part of the criminal sentencing system.

The criminal liability of a legal person does not exclude criminal liability of the natural person that contributed to the commission of the same act.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

In the private sector, Romanian companies are not specifically legally required to implement compliance programs, but companies operating in certain fields (e.g. the banking industry) have such programs in place. Subsidiaries of foreign companies also usually opt to set up compliance programs in their code of conduct or other internal regulations.

The integrity and compliance programs implemented in the private sector are generally inspired by the provisions of Law no. 571/2004, which provides protection for whistleblowers in the public sector, or the integrity and compliance policies adopted by multinational companies or other private organizations.

From a criminal law perspective, the implementation of a compliance system is not a legal criterion for excluding penalties. These facts may be deemed as mitigating judicial circumstances at most. The competent judge will evaluate and decide whether this factor will be taken into consideration when assessing the individual penalty applied against the company, director, officer, or employee.

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Currently, the public attention in Romania focuses on legislative proposals to amend the laws on the justice system.

The most important topic currently under public scrutiny is the abolition of the Special Division for Investigating Justice-Related Offenses ("**SIIJ**"), applicable since the end of 2018, because it triggered very severe criticism from the European partners as well as many protests and grievances coming from the national magistrates.

CONTACT

MAREȘ & MAREȘ
AVOCAȚI

55-55 bis Carol I Blvd., 2nd District
020915 Bucharest
Romania

Tel.: +4 031 43 78 324
Fax: +4 031 43 78 327
www.mares.ro

Dr. Mihai Mareş
Managing Partner
Mareş & Mareş
T +4 031 43 78 324
mihai.mares@mares.ro

Mihai is one of the founders and the Managing Partner of Mareş & Mareş, as well the partner in charge of the white collar crime department.

His practice focuses exclusive on criminal defense for senior executives, entrepreneurs, major industrial groups, financial institutions and large international and domestic companies, in a wide range of matters involving accounting, financial, securities and tax fraud; bribery, antitrust, or money laundry cases.

In addition, he advises clients in internal investigations and audits involving money laundering, fraud and other corporate misconduct. In international criminal law, Mihai acts in international corruption, freezing of assets, multi-jurisdictional investigations and extradition.

Mihai Mareş is member of European Criminal Bar Association and International Bar Association (Business Crime Committee), speaking regularly in local and international seminars related to white collar crime matters.

Russia

Hogan Lovells (CIS)

Alexei Dudko Daria Pavelieva

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes		X	X	X	
No	X No criminal liability of companies; only administrative fines.				X No formal defense, but could be viewed as the absence of fault.

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Russian law provides neither for any specific procedures nor for any specific protection in connection with whistleblower reports.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) The discussed requirements are set by Russian law only for investigations of accidents at work which caused death or injuries to employee(s). In case of investigations with a different subject, the company is not obliged to inform employee representative bodies about the investigation or invite them to participate in it.

A duty to do so can be provided by a collective agreement between the company and its employees. Also, the employee may authorize a trade union to represent their interests in labor relations with the employer, which may result in the trade union's participation in the investigation. The discussed situations are rare in practice. Trade unions (if they exist) usually get involved at a late stage, after the investigation is completed and the company proceeds with the dismissal of the employee.

b) There is no requirement to inform a data protection officer or authority about the investigation or invite them to participate in it.

c) The requirement to inform certain local authorities about the investigation is set only for investigations of accidents at work which caused death or injuries to employee(s). A representative of certain local authorities must participate in an investigation of such accidents.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

In general, the employee's refusal to participate in or support the investigation does not form a ground for dismissal or other disciplinary action. To be able to hold the employee liable for a failure to cooperate during the investigation, the company should provide in documents mandatory for an employee a specific obligation to cooperate and indicate what actions are required from the employee, such as to provide oral and written explanations, to help gather relevant documents and to preserve documents related to the issues under investigation. Such documents could be a labor contract, job description, internal code of labor conduct or ethics code, provided that such documents have been properly adopted by the company and countersigned (with wet signature) by employees. These documents could also indicate what actions are prohibited, e.g. distortion of documents related to the issues under investigation and disclosure of information about the investigation to third parties.

Every person has the constitutional right to refuse giving testimony incriminating themself, their spouse or close relatives. Thus, the employee may not be held liable for refusing to provide responses of a self-incriminatory nature.

Finally, the employee may be dismissed for a failure to cooperate during the investigation only if previously they already committed a disciplinary offense and less than one year has passed since they were held liable for it.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Disciplinary sanctions may be imposed on an employee within (i) one month after a person whom they reports to at work (regardless of whether this person is authorized to impose disciplinary sanctions) became aware of the misconduct; and (ii) six months (two years for violations of the anti-corruption law or misconduct revealed as a result of an audit or inspection) after the misconduct occurred.

If the employer intends to withhold from the employee's salary the amount of damages caused by them, it should issue an order within one month after the amount of the damage was finally determined. The employer may request reimbursement of direct actual damages only. The withdrawal is allowed in the amount not exceeding the employee's average monthly salary, whereas the recovery of the remaining amount of damages (if any) requires application to the court.

This should be taken into account when planning and documenting the investigation. If final conclusions have not yet been reached, the employer should make sure that any preliminary findings are marked as preliminary and subject to confirmation, and avoid definitive statements regarding the employee's misconduct or amount of damages caused by them.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?
b) Reviewing emails?
c) Collecting (electronic) documents and/or other information?
d) Analyzing accounting and/or other mere business databases?

For any of the abovementioned activities the following restrictions shall be taken into account.

Personal data

Emails and other documents usually contain a wide range of personal data: name, address, email address, contact telephone number, instant messenger accounts, etc. Any operations with such information, including their collection, storage, review and transfer, as a general rule require the data subject's prior express consent. Data protection law contains two main exceptions for cases where the data is processed: 1) to protect rights and legitimate interests of an operator or third parties; or 2) to perform duties and obligations imposed on the operator by Russian laws. In such cases the consent is not required, but it is not determined whether the Russian data protection authorities will agree with the application of this ground to internal investigations. Recent comments of representatives of the Russian data protection authority communicated during a conference organized by it in January 2020, confirmed that these grounds could apply to internal investigations.

Employers often obtain data processing consents from employees as part of their employment. If such consents fully cover the investigation (e.g. types of data, types of operations, purpose of processing, possible recipients), they may be relied upon. Otherwise a separate consent should be obtained.

If the employer decides to transfer its employees' personal data to third parties involved in an internal investigation, they will need to enter into data processing agreements, setting out the purpose of data processing, operations to be performed, data protection obligations, etc.

Any transfer of employees' personal data to third parties requires written consent of employees as well. Thus the safest approach would be to get written consents of employees covering purposes of internal investigations and the list of involved third parties that would process such data.

For the information about cross-border transfer of personal data, see response to question 6f.

Information about private life

Collection, storage, use and dissemination of information about the private life of a person, including review of their correspondence and telephone conversations, require their prior consent. This consent should be obtained before taking any actions that could lead to obtaining such information (i.e. usually at the start of the investigation and in any case before reviewing the employee's emails and other files).

Employers are advised to obtain such consents in advance, at the start of employment. Labor contracts or internal policies should contain provisions prohibiting employees from using business facilities (mailbox, cell phone, laptop, fax, etc.) for personal needs and allowing the employer to review any information stored at or derived from such facilities. Employers need to be especially careful with this type of information as the failure to handle it properly could trigger criminal liability under Russian law.

Other types of information

There are no statutes specifically blocking transfer and review of general financial, accounting or other business information abroad. Restrictions are set for information constituting state secrets or commercial secrets. Any access to such information requires a license/permit by state authorities (in case of state secret) or consent of the holder of the information (in case of commercial secret).

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no requirement to issue written instructions. When starting the interview the interviewer generally briefly explains the reason for the interview and its procedure.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no express requirement to do so. However, as stated in response to question 3, every person has a basic constitutional right to refuse providing information of a self-incriminatory nature. To enhance the evidentiary force of the interview, the interviewer could remind the employee about this right and reflect it in the interview protocol.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no express requirement to do so, but it is regarded as a best practice.

d) Be informed that they have the right that their lawyer attends?

The interviewer may not prohibit the employee from bringing a lawyer to the interview. However, there is no formal requirement to inform the employee about this right. In practice, employees insist on legal representation only in exceptional cases.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is no formal requirement to do so.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Such restrictions apply to personal data. Cross-border transfer of personal data, subject to certain limited exceptions, requires a prior written consent of the data subject. In case of a transfer of personal data to countries that are considered not to provide adequate protection of personal data (e.g. the United States, Hong Kong, China), the data subject's consent should be made in a specific form and include the data subject's identification document details and address, a detailed list of actions to be undertaken with respect to the data, purpose of the transfer, etc. In case of a transfer of personal data to countries that provide adequate protection of personal data, the consent may be made in a simple form.

g) Sign a data privacy waiver?

See response to question 5.

h) Be informed that the information gathered might be passed on to authorities?

Transfer of personal data or private data to authorities (as well as any other third parties) is subject to the employee's consent. For other types of information, there is no formal requirement to inform the employee that the information might be passed to authorities. It may be advisable to do so to enhance the evidentiary force of the interview.

i) Be informed that written notes will be taken?

There is no formal requirement to do so. To enhance the evidentiary force of the interview, the interviewer could prepare the interview minutes and ask the employee to sign it to confirm its accuracy.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There are no special rules governing such notices in Russia. Companies usually use them in the form of internal orders to make them mandatory for the company's employees. It is recommended to obtain a written acknowledgment from each of the company's employees that they read the notice, understands its content and will comply with it.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege is known in Russia as 'advocate secrecy'. Advocate secrecy in Russia applies to any information relating to legal advice provided by a lawyer admitted to the Russian Bar who has the status of an 'advocate'. If an internal investigation is conducted by a duly retained advocate, it is likely that the information regarding the investigation and obtained in the course of the investigation will be protected by advocate secrecy.

It is highly recommended to mark all the documents produced or obtained in the course of an internal investigation as "confidential" and "subject to advocate secrecy" as well as to keep the most important documents and information in the offices or on the servers of the advocates to reduce the risk of their seizure by the authorities.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

The privilege applies only to advocates and does not apply to lawyers who are not advocates, whether they are inside or outside counsel. Advocates may only practice law as self-employed practitioners through specific Bar institutions, they are not allowed to be employed.

The said approach is also shared by foreign courts. In 2014 in *Veleron Holding, B.V. v. BNP Paribas SA et al.* the United States District Court for the Southern District of New York granted a request for production of communications with Russian attorneys on the basis that "Russian law does not recognize attorney-client privilege or work product immunity for communications between or work product provided by in-house counsel or 'outside' counsel who are not licensed 'advocates' registered with the Russian Ministry of Justice".

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Only if provided by the terms of the insurance contract.

b) To business partners (e.g. banks and creditors)?

Only if provided by the terms of a contract.

c) To shareholders?

A company with a registered securities prospectus or a prospectus of bonds/Russian depositary receipts admitted to trade at a stock exchange is obliged to disclose information about any facts that, in the company's view, can materially affect the value of its securities. Theoretically, suspicions of certain violations and the opening of an internal investigation can fall within this category.

d) To authorities?

Only for investigations of accidents at work, as mentioned in the response to question 2c above.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Russian law does not provide for any such measures.

A company self-reporting to the authorities and cooperating with an investigation can release it from liability for bribery. Remediation actions can be treated by court as a mitigating circumstance and reduce an administrative fine to be imposed on the company.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Companies are not required to alert the prosecutor office about the start of an investigation. It might be advisable to do so when there is a duty of self-reporting in relation to the issue under foreign law or the company's policy. It may also be advisable to self-report when the risk of leaks about the issue is significant and such self-reporting is part of the risk mitigation strategy.

If the company informs the prosecutor office about the investigation, the Russian authorities are expected to start their own investigation rather than interfere in the internal investigation.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Searches at companies' offices are conducted on the basis of the investigator's order while searches of private premises require the court's prior approval, which in exceptional urgent cases may be substituted by the court's

subsequent approval. Searches at an advocate's offices or premises where they live are subject to the court's prior approval and a number of additional limitations aimed at preserving advocate secrecy (e.g. presence of a representative of a local Bar Association).

Searches should be attended by a person in whose premises the search is carried out (in case of a company, its representative) and at least two attesting witnesses. An advocate of the person in whose premises the search is carried out may also attend. Searches shall not be carried out at night unless there is an urgent need.

Russian law does not have a separate concept of dawn raids. The investigator announces the decision to conduct the search when they arrive at the premise, shortly before the search. No advance notices are required.

If the search was conducted in violation of applicable laws, the evidence obtained upon it is deemed inadmissible.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Non-prosecution agreements or deferred prosecution agreements are not available in Russia. A release from liability is granted where a person self-reported bribery and cooperated with investigation.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Sanctions under criminal law include fines, disqualification, compulsory community service, corrective or compulsory labor, restriction of liberty, arrest, and jail. In addition, assets received as a result of certain criminal offenses are subject to confiscation.

Only individuals can be held criminally liable. There is no criminal liability for legal entities. If a criminal offense is committed in the interests or on behalf of a legal entity, an individual (director, officer, or employee) involved in the offense will be held criminally liable while the company may be held liable for an administrative offense. Administrative sanctions for companies are warnings, fines, confiscation, and suspension of operations.

A company may not participate in public procurement under Federal Law No. 44-FZ on the Contract System in the Area of Procurement of Goods, Work and Services to Support State and Municipal Needs, dated 5 April 2013 if any of the following applies:

- The company was held liable for bribery within two preceding years;
- The operations of the company have been suspended as a punishment for an administrative offense; or
- The company's director, member of the executive board, person performing functions of the CEO or chief accountant: (i) has been held criminally liable for economic crimes or bribery; (ii) has been disqualified; or (iii) has been prohibited to hold positions and carry out activities related to goods, works, or services which are the subject of the relevant procurement.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

There is no formal adequate procedures defense. However, the basis for liability of legal entities is defined in Russian administrative law as a failure to take all measures within a company's control to prevent an offense. Thus a company that implemented an efficient compliance system prior to the alleged misconduct could be viewed as non-guilty and avoid liability for bribery. However, the current court practice on this issue is not favorable to companies. Courts tend to recognize compliance measures taken by companies as insufficient.

In addition, we are not aware of cases where the subsequent implementation of an efficient compliance system helped reduce the penalties.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The main focus of prosecution has been on public officials, state companies and other recipients of state funds (e.g. private companies participating in public procurement). The latter can be held liable even if they participate in public tenders indirectly, through distributors.

Russian competition authorities have been particularly active. They put intense efforts into countering price collusion and other competition violations at public tenders and share information with other state authorities about suspected irregularities, which increases chances of bribery at public tenders being investigated as well. This makes companies in Russia pay increased attention to their practices of participating in public procurement, including through distributors and other intermediaries.

CONTACTS

Summit Business Center
22 Tverskaya Street, 9th floor
125009 Moscow
Russia

Tel.: +7 495 933 3000
Fax: +7 495 933 3001
www.hoganlovells.com

Alexei Dudko
Partner
Hogan Lovells Moscow
T +7 495 933 3000
alexei.dudko@hoganlovells.com

Heading the Russian dispute resolution practice of the firm, Alexei offers clients the benefit of over 20 years' experience as an accomplished litigator and advisor. Alexei has built a strong portfolio of winning complex cases in both commercial and general courts in Russia and in international arbitrations. He is a recognized authority on Russian and international fraud and asset tracing litigation.

Daria Pavelieva
Senior Associate
Hogan Lovells Moscow
T +7 495 933 3000
daria.pavelieva@hoganlovells.com

Daria is a senior associate in Hogan Lovells' Investigations practice. She provides legal support to clients during investigations by state authorities and conducts internal investigations into allegations of fraud, corruption and export control violations. She also helps clients develop and implement robust compliance programs.

Slovakia

HAVEL & PARTNERS s.r.o. attorneys-at-law


Ondřej Majer Anikó Gőghová

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

The Slovak Whistleblowing Act No. 54/2019 Coll. provides *inter alia* certain obligations of selected legal entities and natural persons who have the status of an employer. An employer with at least 50 employees and an employer as a public authority with at least five employees are obliged at least to (i) determine the so-called responsible person, (ii) harmonize its internal system for handling whistleblower reports including the related internal regulation, (iii) examine all of the submitted whistleblower reports, and (iv) archive records on whistleblower reports etc.

The identity of the responsible person and options for the submission of whistleblower reports as well as briefly and clearly formulated written information on the internal system for screening whistleblower reports must be disclosed and available for all employees in a usual and commonly available manner. At least one of the provided submission options must be continuously available.

The employer's internal regulation on details of its internal system for handling whistleblower reports must contain *inter alia* the details on maintaining the confidentiality of the whistleblower's identity.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) There are no specific legal requirements stipulated by law. The possibility of including these rights of employee's representative is not excluded in collective agreements. Acknowledgment of these rights has to be duly assessed beforehand and must not impact the general requirement to conduct internal investigations independently. This applies without prejudice to the employers' obligation to involve the employees' representatives in the employment termination processes in time (mostly before commencement).

b) Neither the data protection officer ("**DPO**") nor the data privacy authority ("**DPA**") have to be informed. However, it is advisable to inform and/or involve DPO in the investigation.

c) No specific legal requirements are applicable in relation to internal investigations.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

There are no specific legal requirements directly stipulated by the Slovak Labor Code No. 311/2001 Coll., as amended ("**LC**").

The employees' obligations to support the investigation or participate in interviews are derived from the provisions of LC stipulating *inter alia* the obligation to: (i) comply with the instructions of senior employees, (ii) protect the employer's property against damage, loss, destruction and abuse; (iii) not act in contradiction to the justified interests of the employer; (iv) observe the internal rules of the employer such as work rules (where the given obligations of the employee can also be stipulated); and (v) maintain confidentiality over matters relating the employment, and which, in the interests of the employer, may not be disclosed to other persons etc. The employee's obligation to maintain confidentiality does not apply to notification of crimes or other so-called anti-social activities as defined by the law.

The employee's refusal to support the investigation or participate in interviews may be considered as breach of their obligations. Depending on its seriousness, this may be a sufficient reason for a formal warning, for giving notice or for immediate termination of the employment.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

The internal investigation has no impact on any labor law deadlines including the right to sanction employees.

An employer may give notice to an employee or immediately terminate the employment only within a period of two months from the day the employer became aware of the reason for notice or immediate termination, but not later than one year from the day when the reason for notice or immediate termination occurred.

In order to ensure any employer's rights to respond to any employee failure, setting the exact rules of the investigation process is recommended.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

In general, no deviation is applicable from the GDPR. Personal data processed at interviews are subject to data privacy laws. It is highly recommended to perform an early assessment of the information that shall be processed from the viewpoint of the applicable data privacy laws as well as its nature regarding the category and sensitivity of the information that shall be processed.

b) Reviewing emails?

The Slovak Labor Code would primarily apply. The employer must not, except for serious reasons relating to the specific character of the employer's activities, intrude upon the privacy of an employee in the workplace and common areas of the employer by monitoring them, keep records of telephone calls made with the employer's equipment or review emails sent from a work email address and delivered to such an address, without giving notice in advance.

Such activities may be possible without prior notice if there were serious reasons relating to the specific character of the employer's activities.

In case the employer intends to implement a surveillance mechanism, the employer is obliged to consult this with the employee's representatives and inform the employees in advance.

As to the employee's private communication, stricter legal protections apply.

c) Collecting (electronic) documents and/or other information?

In general, no deviation is applicable from the GDPR. In case the electronic documents and/or information include personal data, data privacy laws apply. It is highly recommended to perform an early assessment of the information that shall be processed from the viewpoint of the applicable data privacy laws as well as its nature regarding the category and sensitivity of the information that shall be processed.

d) Analyzing accounting and/or other mere business databases?

In general, the analysis of accounting and other business databases of a company are allowed. However, depending on the manner and purposes of the analysis as well as categories of data, please see the information added to points 5a-c above.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

In general, there is no specific obligation to instruct an employee on their rights.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

The right to remain silent which specifically applies during interrogations of criminal authorities i.e. for criminal proceedings, does not apply. In general, there is no corresponding right in internal investigations.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no obligation to provide an Upjohn warning or similar information under Slovak law.

d) Be informed that they have the right that their lawyer attends?

There is no obligation of the company to inform the employee about their given right. However, the employee has a constitutional right to legal assistance of their lawyer. This right to legal assistance was also confirmed by case law of the Constitutional Court of the Slovak Republic.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is no specific legal requirement stipulated by law in relation to the attendance of an employee representative at the interview or in relation to the employee's right to have employee representatives attend.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The employee must be informed of the occasion of gathering the data, *inter alia* that the controller intends to transfer the personal data to a third country (e.g. to the United States).

g) Sign a data privacy waiver?

The concept of "in advance waiver" is not recognized in Slovakia and thus signing a waiver by the interviewee would not have the intended legal effect.

h) Be informed that the information gathered might be passed on to authorities?

There is no specific legal obligation stipulated by law that requires the employee to be informed.

i) Be informed that written notes will be taken?

There is no specific legal obligation stipulated by Slovak law to inform the employee that written notes will be taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There are no specific legal requirements on issuing document hold notices. Thus, there are no legal barriers to issuing such notices in practice.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege may be claimed over findings of the internal investigation. However, the privilege rule applies only to information gathered or created when providing legal services by an attorney registered with the Slovak Bar Association. The rules do not apply to in-house lawyers.

In order to ensure privilege, the safest way is to involve a registered attorney as external counsel. In addition, it may also be helpful to label the privileged documents with tape informing of the attorney-client privilege.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

The attorney-client privilege does not apply to in-house counsel in Slovakia, or to any communication with in-house counsel and documents created by in-house counsel.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

No specific legal requirements are applicable. The notification in question will depend on the terms and conditions of the insurance agreement as well as the related circumstances and the definition of an insurance event that connects the company's claim against the insurance company; the insured company should make a notification of circumstances to the insurer.

b) To business partners (e.g. banks and creditors)?

There are no specific legal requirements stipulated to notify the business partners on starting an investigation. Any possible notification obligations may arise from the contractual obligations agreed between the company and its business partners. Even if there is no explicit provision in the contract, the company must consider notification with regard to the purpose of the agreement.

c) To shareholders?

There are no specific legal requirements applicable in relation to investigations. In general, the company must properly assess in all individual cases whether providing certain information could be a breach of law, cause damage to the company or its controlled companies, or threaten the interests of the company or its shareholder's. The provision of information can be refused as long as the information does not relate to the economic activities and property conditions of the company. The possibilities of such refusal must be assessed by taking into account the legal form of the company as well as the provisions of corporate documents in which certain differences may apply.

d) To authorities?

In general, there is no legal obligation stipulated by law to inform the authorities of an internal investigation or potential misconduct within the company. However, depending on the information and outcomes of the investigation, the company is obliged under Act No. 301/2005 Coll., the Criminal Procedure Code, as amended ("**CPC**"), to file a criminal complaint if there are circumstances suggesting that specific serious crimes were committed.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

There are no specific legal requirements stipulated by law. In any case, it is recommended that in order to mitigate any possible damage, the company should audit its procedures, identify the breach, and eliminate or minimize ongoing illicit activities.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

In general, local prosecutor's offices are not involved in internal investigations. Pursuant to the CPC, early communication and cooperation with the local prosecutor's office is recommended.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

The legal requirements for search warrants are stipulated by the CPC and for dawn raids are stipulated by the Slovak Competition Act No. 136/2001 Coll., as amended (the "**Competition Act**").

Pursuant to the CPC, a search may be conducted if there is reasonable suspicion that the apartment or other premises serving as a residence or premises attached to them contains an item important to the criminal proceedings or that a person suspected of committing a criminal offense is hiding within, or if it is necessary to perform a seizure of movable assets to satisfy the entitlement to damages of the victim. For the same reasons, a search of non-residential premises ("**other premises**") and land that is not publicly accessible may be performed. In both cases, the *search warrant* must be issued in written form as described by CPC and signed by the person determined by the CPC.

In the absence of a warrant or authorisation a police officer may conduct the search of other premises or property only if such warrant or authorisation could not be secured in advance and in cases of emergency, or if it involves a person caught in the act of committing a crime or a person in respect of whom the arrest warrant was issued or a persecuted person who hides in such premises. Such a procedure, however, has to be immediately reported to the body authorized to issue the warrant or to grant authorisation.

In competition matters, the Authorisation for Dawn Raid ("**Inspection**") serves to fulfill tasks stated by the Competition Act and has to be issued in writing by the Antimonopoly Office of the Slovak Republic (the "**Office**"). Such an authorisation must contain certain information stipulated by the Competition Act. The authorisation is limited to entry to all premises and means of transport of the company that are related to the activity or the conduct of the company.

If there is a reasonable suspicion that materials or documents, based on which it is possible to prove restriction of competition, relating to the activity or conduct of the company, are located in other premises or means of transport of the company, as well as in the private premises or private means of transport of the company's current or former employees, the Office may carry out an inspection in those premises only based on the consent of the court with an inspection issued at the request of the Office.

In case the Inspection is conducted by the European Commission ("**Commission**"), the Office ensures submission of application to a court for approving;

i. When the company objects to the inspection performed in its premises, land, means of transport and associations, including further related activities of the Commission; and/or

ii. When the inspection will be conducted in any other premises, land and means of transport, including the homes of directors, managers and other members of the company's staff and associations.

In general, if legal requirements are not fulfilled, the seized evidence should not be used, which has been confirmed by case law of the Supreme Court of the Slovak Republic.

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

The CPC provides possibilities corresponding to deals, non-prosecution agreements or deferred prosecution agreements. All of them are available for individuals as well as for corporations.

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

The company may face the following penalties:

a. Prohibition of activities (from one to 10 years);

b. Forfeiture of items;

c. Pecuniary penalty (from €1,500 to €1.6 million);

d. Forfeiture of a property;

e. Dissolution of the corporate entity (if the activities were used fully or partially for committing a crime);

f. Prohibition of participation in public procurement (from one to 10 years);

g. Prohibition of receiving subsidies or subventions;

h. Prohibition of receiving help and support provided from EU funds (from one to 10 years);

i. Publication of condemnatory sentence (at the expense of the corporate entity).

It is not excluded that individuals may face criminal prosecution in specific situations also for misconduct of other employees when they failed to implement sufficient supervision or control. In this case they may face the following penalties:

a. Imprisonment;

b. Home confinement;

c. Community service work;

d. Pecuniary penalty (from €160 to €331,930);

e. Forfeiture a property;

f. Forfeiture of items;

g. Prohibition of activity;

h. Prohibition of residence;

i. Prohibition of participation in public events;

j. Loss of honorary degrees and distinctions;

k. Loss of military and other rank; and

l. Expulsion.

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Under the Slovak Act No. 91/2016 Coll. on the Criminal Liability of Legal Entities, the existence of an efficient compliance system is not directly a reason for discharging or suspending the liability of the company for the misconduct.

However, pursuant to the CPC, an efficient compliance system may be considered as mitigating circumstance resulting in a possible reduction of penalties for companies.

In order to qualify as mitigating factor when imposing a penalty, the compliance system has to be efficient and implemented prior to the alleged misconduct.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

In general, we expect an increased focus on companies' activities and internal systems including its anticorruption measures, its level of transparency and effectiveness. In addition, we expect an increase in authorities' activities to combat corruption, environmental crimes, tax crimes, money laundering, and terrorism financing.

CONTACTS

HAVEL & PARTNERS
CONNECTED THROUGH SUCCESS

Zuckermandel Center, Žižkova 7803/9
811 02 Bratislava
Slovak Republic

Tel.: +421 232 113 900
Email: office@havelpartners.sk

HAVEL & PARTNERS, with offices in Prague, Brno, Bratislava, Pilsen, Olomouc, and Ostrava, has a team of 220 lawyers and tax advisors, approx. 150 associates and 500 employees in total, including employees of the affiliated debt collection agency Cash Collectors, and is the largest independent law firm in Central Europe.

Ondřej Majer

Partner
HAVEL & PARTNERS
T +421 232 113 900
M +420 737 150 145
ondrej.majer@havelpartners.sk

Ondřej specializes *inter alia* in commercial and contractual law, corporate law including compliance programs, mergers and acquisitions, real estate law, litigation and bankruptcy law.

Ondřej has extensive experience in the automotive, energy, real estate and construction sectors, both in Czech Republic and in Slovakia.

In mergers and acquisitions, he has represented a number of clients, on the side of both sellers and buyers, in the Czech Republic and in Slovakia.

In litigation and insolvency, Ondřej has represented clients in a number of comprehensive litigation matters, including cross-border disputes, cross-border insolvencies, disputes with an international element, and corporate law disputes.

Anikó Gőghová

Associate
HAVEL & PARTNERS
T +421 232 113 909
M +421 910 822 594
aniko.goghova@havelpartners.sk

Anikó specializes in particular in corporate law, compliance programs as well as criminal law including the criminal responsibility of legal entities. She also advizes clients on banking and insurance and anti-money laundering legal requirements.

In all her practice areas, she prepares legal analyzes and due diligence reports, revises and creates compliance programs and anti-money laundering programs for companies operating in various fields of law.

Slovenia

Law firm Miro Senica and attorneys, Ltd.


Uroš Čop


Žiga Sternad


Katarina Mervič

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X Corporations (legal persons) can be criminally liable under the conditions defined in the Liability of Legal Persons for Criminal Offenses Act ("**ZOPOKD**").	X	X	X	
No					X

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

There is no general Slovenian law that regulates whistleblower protection in case an internal investigation is set off.

However, certain statutes contain some provisions relating to whistleblower protection.

Firstly, Article 23 of the Integrity and Prevention of Corruption Act stipulates, *inter alia*, that the whistleblower's identity has to be protected by competent authorities to whom a report is made (under condition that the whistleblower's report was made in good faith and/or if whistleblower reasonably concluded that the information he reported was true and correct).

Secondly, the Slovenian Employment Relationship Act ("**ZDR-1**") contains a general prohibition of discrimination and retribution (Article 6) and of sexual and/or other harassment and mobbing (Article 7) by employer towards an employee at workplace.

Thirdly, Article 294 of the Criminal Code ("**KZ-1**") stipulates that the punishment of a person, who prevents the continuation of criminal society activities, can be reduced. Moreover, Article 142 KZ-1 stipulates that a person, who reports about information they obtained as advocate, lawyer, doctor, priest, social worker, psychologist, or as another professional person, may not be punished if the report is made for the legitimate public interest or to the benefit of another. This may only apply if the interest for revealing the information outweighs the (benefit of) secrecy or if one is relieved from the duty of secrecy by law (statute).

Fourthly, Article 260 KZ-1 stipulates that a person who discloses classified information shall be sentenced to imprisonment for not more than three years. However, this person shall not be punished if such classified information reveals unlawful restriction of human rights and fundamental freedoms, other constitutional and legally established rights, serious abuse of authority or powers or other serious irregularities while exercising (public) authority or conducting public service. Further, the disclosure of classified information must not be

committed out of self-serving interest, must not be life threatening or have any serious or irreparable detrimental effects for the safety or legally protected interests of Slovenia. Furthermore, whoever obtains such classified information without authority and with the intention of using this information shall be sentenced to imprisonment for not more than three years. However, this person shall not be punished if the circumstances of the case show that there is a stronger public interest for disclosing it than for keeping it confidential. This only applies if lives are not directly put at stake.

Fifthly, Article 239 of the Slovenian Banking Act ("**ZBan-2**") stipulates that the Bank of Slovenia is obliged to create a system for the protection of whistleblowers who are employees of banks.

And lastly, the Slovenian Sovereign Holding Act ("**ZSDH-1**") contains provisions in relation to a whistleblower protection scheme that is applicable for the employees of the Slovenian Sovereign Holding.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Pursuant to the Slovenian Worker Participation in Management Act ("**ZSDU**") workers have the ability to participate in companies' management via representative bodies or functions.

Although the ZSDU does not specifically require employee representative bodies to be informed and/or to participate in an internal investigation, an agreement between employer and works council may stipulate such obligations.

According to Article 174 ZDR-1, an association may participate in disciplinary proceedings against an employee, if authorized by the employee. Members of the association could be another employee, the works council or a trustee.

According to Article 86(1) ZDR-1 the association has to be informed in writing about the intended termination of the employee's employment contract if so requested by the employee. According to Article 85(3) ZDR-1, a representative of an association authorized by the worker may participate in the employees' defense before the ordinary termination of an employment contract.

Violations of particular provisions of the ZSDU or ZDR-1 may be sanctioned with administrative fines.

b) The main regulation regarding the processing of personal data is the EU General Data Protection Regulation ("**GDPR**"). According to the GDPR, one of the Data Protection Officer's ("**DPO**") duties would be to consult the employees regarding their data privacy rights. Subject to the company's internal regulations, the DPO in general has to be informed about all data privacy related procedures and processes of an internal investigation.

c) There is neither a need to inform authorities about the investigation nor do they have to be invited to participate. However, informing authorities may be advantageous.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

According to Article 34 ZDR-1, an employee has to follow the employer's requirements and instructions in relation to the execution of its contractual obligations and employments' relationship obligations. They therefore generally have to participate in an internal investigation.

Further, according to Article 172 ZDR-1, disciplinary measures may be imposed upon an employee if they violate contractual employment obligations or other obligations from the employment relationship.

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Investigative actions may trigger notification and termination deadlines.

According to Article 85 ZDR-1, prior to an ordinary termination of an employment contract due to misconduct, the employer is obliged to remind an employee that in case of repeated violations their employment contract could be terminated within 60 days following the identification of the violation (relative deadline) or no later than six months (absolute deadline) from the occurrence of the violation.

The employer should not be informed about the results of the investigation until comprehensive results are gathered to avoid a premature triggering of this deadline.

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

According to Article 48 ZDR-1, personal data may only be collected, processed, used or transferred to third parties if required by statutory law or in case collecting, processing, using and transferring of data is necessary for the execution of rights or obligations arising from the employment relationship.

b) Reviewing emails?

Privacy of communication is protected on a constitutional level (Article 37 of the Slovenian Constitution). The Electronic Communications Act ("**ZEKom-1**") regulates the privacy of communication. In general, an employee has to be informed in advance under which conditions their emails may be reviewed. This should be stipulated in the employer's internal regulations. Employers have to provide an employee with the chance to delete their private emails, prior to the review of those emails. Further, reviewing of emails has to be necessary, which means a legitimate aim for the review must exist. In this process, a balancing of interests test has to be performed.

c) Collecting (electronic) documents and/or other information?

The police may request employers to provide documents and/or other information on the basis of the Slovenian Police Tasks and Powers Act. In case of a doubtful legal basis we suggest to wait until an authority makes a formal written request with the announcement for enforcement.

d) Analyzing accounting and/or other mere business databases?

There is no specific legal basis applicable for analyzing accounting and/or mere business databases during an internal investigation. In the broadest sense there are two (general) legal bases:

Pursuant to Article 53 of the Slovenian Accounting Act companies are obliged to regulate the controlling of data and internal auditing in accordance with applicable law and companies' internal acts. Further, Article 281a(2) of the Slovenian Companies Act ("**ZGD**") (applicable for joint-stock companies and private limited companies) stipulates that the supervisory board has to give its consent to the company's internal policies stipulating the purpose, meaning and assignments of internal audit.

According to Article 19 of the Slovenian Inspection Act ("**ZIN**") – regulating inspection procedures conducted by authorities – the inspector has a right to inspect business documentation and all other documents needed for the inspection. This documentation may also be retained under conditions specified in the ZIN.

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

The Slovenian law does not contain any statutory obligation to instruct an employee about the legal circumstances and their rights regarding internal investigation procedures.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

In contrast to an individual's right to remain silent in case of self-accusation during interrogations of criminal authorities, there is no corresponding right with regard to employee interviews as part of internal investigations.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

Giving an Upjohn warning is an accepted best practice in Slovenia. However, there is no explicit legal obligation to do so under Slovenian law.

d) Be informed that they have the right that their lawyer attends?

There is no such legal obligation. However, companies are obliged to allow such attendance of the employee's lawyer during termination procedure interviews.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is generally no such explicit legal obligation in internal investigations.

In case the internal investigation is part of disciplinary or termination procedures the employee representative body has the right to attend if the employee under investigation requests so.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

When transferring personal data cross-border and if the employer has no statutory right or obligation for the transfer of data to the United States, the employer is obliged to inform the employee and to obtain their written consent before transferring the data cross-border.

g) Sign a data privacy waiver?

This is not necessary if no other personal data shall be gathered than the data already gathered by the employer according to the applicable labor law legislation, such as employee name, address, ID number, tax number.

h) Be informed that the information gathered might be passed on to authorities?

There is no such legal obligation with regard to internal investigations.

i) Be informed that written notes will be taken?

There is no legal obligation to do so. However, it is a common practice in companies to inform the interviewee that written notes shall be taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law regulating this matter.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The confidential relationship between a defense counsel and a defendant is protected by the Slovenian Constitution. This relationship is protected irrespective of whether the documents or information are intended for defense in criminal proceedings. This is because, for example, in case of a search of a law firm, there is the danger that the police will obtain documents and objects that are not related to the criminal offense which is the subject of the investigation. The investigating authorities have to adhere to the rights referred to in the Slovenian Constitution.

Thus, they may not seize such documents when in custody of the defense counsel. The legal protection of this confidential relationship encourages the client to communicate with an attorney or defense counsel without restrictions, i.e. without the fear that any subsequent disclosure of confidential information would jeopardize their legal position. Documents in the custody of the client may, however, be seized and used in proceedings against the client.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

No. The confidential relationship is binding only for attorneys who must keep secret everything that the client has entrusted to them (Article 6 of the Slovenian Attorneys Act). This obligation also applies to other persons working in a law firm, but it does not apply to in-house lawyers.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

If any kind of circumstance arises which could trigger a claim against insurance companies, the latter should be informed. A general duty to notify the insurance company is stipulated in Article 941 of the Slovenian Obligations Code. According to this law, the policyholder must inform the agency regarding any insurance case within three days after gaining knowledge about it.

b) To business partners (e.g. banks and creditors)?

Whether there is a duty to notify business partners should be evaluated in each individual case. Even if a business contract does not contain specific notification duties of the contracting parties, such duties may be construed on the basis of general principles of the Slovenian obligations law. This applies in particular if the information concerning the start of the investigation constitutes information important for the other party and is relevant with respect to the purpose of the agreement.

c) To shareholders?

Slovenian Law does not provide any specific duty to inform shareholders about starting an investigation. However, according to of Article 305(1) ZGD, shareholders have a right to be informed about "*reliable information on the company's affairs if this information is important for the assessment of the agenda [for the general meeting]*". According to Article 305(2) ZGD the management is not required to provide information in the following cases:

(i) If the provision of information could, by reasonable economic judgment, cause damage to the company or its affiliate;

(ii) If the information refers to the methods of accounting and assessment, provided that the statement of methods of this kind in the annex is sufficient for an assessment of the actual situation of the company in terms of property, financial standing; and profitability;

(iii) If the provision of information would constitute a criminal act, a minor offense, or a breach of good business practice; or

(iv) If the information is published on the company's website in the form of questions and answers at least seven days before the general meeting.

Please be advised that information regarding internal investigations may have a significant effect on stock price and therefore may be considered as insider information, which may be subject to abuse.

d) To authorities?

There is no general duty to inform authorities about internal investigations. However, in certain cases failure to report that particular severe crimes may have been committed could be criminally prosecuted.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Companies under investigation are generally not obliged to cooperate in the investigation or in investigative actions. The public prosecutor is the institution in charge that investigates and collects evidence in order to confirm the suspicion of a criminal offense.

However, there may be a duty to reveal evidence. The Criminal Procedure Act ("**ZKP**") stipulates that anyone possessing objects which must be seized under the KZ-1, or which may be evidence in criminal proceedings, is obliged to hand them over to the court upon request. A custodian who declines to deliver the requested objects may be fined. In case of being fined and still refusing to surrender those objects, they may be arrested. The detention lasts until the objects have been delivered or until the end of the criminal proceedings, but no longer than one month.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Actions conducted by companies' management or supervisory bodies may be regarded by authorities as positive counteractions aimed at remedying the consequences of criminal acts or misdemeanors committed by the company's employees and/or responsible persons. Article 11(1) Liability of Legal Persons for Criminal Offenses Act ("**ZOPOKD**") stipulates that a company's criminal sanction, which derives from management or supervisory bodies' lack of control over employees, is to be mitigated in cases where companies' management or supervisory bodies voluntarily indicated to authorities the person who committed the criminal act (on behalf of the company) before authorities gain knowledge about that person.

Pursuant to Article 11(2) of ZOPOKD, a company's criminal sanction, which derives from management or supervisory bodies' lack of control over employees, is to be remitted if the perpetuator is indicated to authorities before they gain knowledge about them and

- an order for immediate return of unlawful gains is given; or
- the damage is otherwise remedied; or
- the merits of other company's criminal liability are indicated to authorities.

Similarly, pursuant to Article 21 of the Minor Offenses Act a reprimand instead of an administrative fine may be issued to the company in an administrative procedure, if the misdemeanor was committed in circumstances which make the misdemeanor evidently insignificant (paragraph 1), or if the damage consequential to the misdemeanor was remedied prior administrative body fined the perpetuator (paragraph 2).

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Slovenian searches conducted by authorities are led by an investigative judge. Authorities' searches cannot be initiated without the prosecutor's motion. The latter has to be made by a competent prosecutor and contain the following information:

- The subject of investigation;
- The description of facts pertaining to alleged criminal offense;
- Reasonable doubts; and
- A list of already gained evidence.

There is no general bright line rule regarding the admissibility of evidence in Slovenia.

Article 18 ZKP stipulates that only evidence permissible by law may be part of the procedure. Inadmissible means of evidence on this occasion is evidence obtained in violation of the Slovenian Constitution, the ZKP, if expressly stipulated, poisonous tree evidence or fishing expedition evidence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

The prosecution is bound by law to prosecute all alleged criminal offenses *ex officio* regardless of the will of other subjects (e.g. injured compromised party). Therefore, non-prosecution agreements are not possible. However, prosecution could be put on hold in the course of alternative extra-judicial resolving of criminal matters. The latter can be done with the compromised party's consent in case of criminal offenses punishable with fines or imprisonment up to three years.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

In Slovenia legal entities can generally not be held criminally liable. However, in specific cases legal entities could be subject to criminal liability to the extent that the conditions specified in the ZOPOKD are met. The following punishments may be imposed upon legal entities:

- Financial punishment, such as fines;
- Assets forfeiture;
- Termination of legal entity; and/or
- Prohibition of disposing securities held by the legal entity.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Under Slovenian law, the implementation of an efficient compliance system is not regulated as a specific and explicit reason for the suspension or reduction of penalties. It can be, however, evoked in substance when (generally) claiming mitigating circumstances in relation to the setting of the penalties.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The topic of business compliance is gaining more and more attention every day in Slovenia. Slovenian corporations are establishing their own compliance departments (e.g. banks, insurance companies or pharmaceutical companies) and are implementing their own internal compliance policies.

Moreover, certain non-governmental organizations and business associations are addressing this topic daily and intensively.

Further legislative changes implementing Directive (EU) 2019/1937 are envisaged. However, no specific national regulation implementing the Directive has been prepared or put forward at the time of this article.

CONTACTS

Law Firm
Miro Senica and Attorneys
Collaborating with Andersen Global in Slovenia

Barjanska cesta 3
p.p. 1945
1001 Ljubljana
Slovenia

Tel.: +386 1 252 8000
Fax: +386 1 252 8080
www.senica.si

The Law firm Miro Senica and Attorneys, Ltd. was founded in 1986 by attorney at law Miro Senica. Since then it has become one of the largest law firms in Slovenia providing its clients with a full service of legal counselling and representation in all areas of law. The Firm's clients range from leading international to largest Slovenian corporations, as well as emerging companies from various industries. The attorneys at Law firm Miro Senica and Attorneys, Ltd. give legal advice, represent clients and conduct cases in the fields of Banking & Finance, Corporate & Commercial law, Civil law, Compulsory settlement, bankruptcy and liquidation procedures, Dispute Resolution, Arbitration and Mediation, Employment (Labor), Intellectual Property, Mergers & Acquisitions, Public Procurement, Real Estate, Securities and Taxes.

Uroš Čop
Managing Partner and Attorney at law
Miro Senica and attorneys, Ltd
T +386 1 252 8000
uros.cop@senica.si

Uroš Čop is a Head of Criminal and Constitutional Law Department also a specialist in the areas of intellectual and industrial property law, corporate and commercial law, criminal and constitutional law. He also represents foreign clients and cooperates at cross-border transactions. He is a manager of Adriatic Legal Network, which has been co-founded by Law firm Miro Senica and Attorney, Ltd.

Žiga Sternad
Attorney at law
Miro Senica and attorneys, Ltd
T +386 1 252 8000
ziga.sternad@senica.si

Žiga Sternad specializes in labor law, but also performs services in the area of commercial law, civil law, administrative law and contract law.

Katarina Mervič
Attorney at law
Miro Senica and attorneys, Ltd
T +386 1 252 8000
katarina.mervic@senica.si

Katarina Mervič specializes in criminal law, but also performs services in the area of copyright and industrial property law, contract law and representation of foreign clients.

Spain

Hogan Lovells International LLP

Ignacio Sánchez

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

There are no Spanish laws establishing specific procedures to be considered within the framework of an internal investigation with regard to whistleblower protection.

However, companies can implement their own internal procedures which should respect the minimum standards set out in the Spanish Workers' Statute ("**WS**"). This entails the non-discrimination of workers' rights, respect for their privacy, protection against harassment and the exertion of their individual rights deriving from their work contract.

In addition, Section 24 of the Spanish Data Protection Act ("**SDPA-GDR**") imposes a number of conditions on the processing of personal data in the context of internal reporting channel systems, such as the limitation of access to the data contained in the system, the adoption of necessary measures to preserve the whistleblower's identity and ensure the confidentiality of the data provided, as well as its storage and preservation.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Unless otherwise stated on collective bargaining agreements, employees' legal representatives are required to be informed when the investigation involves the search on the personal belongings and lockers of the employees. In these cases, employee's legal representatives are allowed to be present during the search.

b) Data privacy authorities do not generally have to be informed. However, companies that must appoint a data protection officer pursuant to the new European General Data Protection Regulation ("**GDPR**") must also inform them about all existing data-privacy related internal procedures, including those regarding investigations.

c) It is not compulsory to inform local authorities before starting an internal investigation.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees are not legally required to support or participate in internal investigations being conducted in the employer's company.

However, their refusal to liaise could entail loss of trust and eventually be deemed as a violation of the contractual good faith. This could result in sanctions or even dismissal pursuant to the WS.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

As a general rule, different deadlines apply depending on the severity of the misconduct. The deadlines may vary between 10 to 60 days since the company became aware of the infringement or, in any case, six months since the infringement was committed.

However, if the company can prove that it did not become aware of the infringements until it started an internal investigation to have the whole picture of the situation, such deadlines may start only once the internal investigation was concluded.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Data privacy laws apply to the processing of personal data. Therefore, the interviewee shall be informed, prior to the interview, about the processing of their personal data.

Further, access to the information processed as part of the investigation must be granted strictly on a need-to-know basis to those roles/teams assigned to perform internal control and compliance functions. Moreover, only personal data that is relevant and relevant for the purposes of the investigation should be processed, in compliance with the minimization principle.

b) Reviewing emails?

Generally, private communications are highly protected under Spanish law. Hence, emails sent from/to employees' corporate email accounts might under certain circumstances be considered as "private" communications.

From a labor law perspective, the employer has management and control powers provided that the dignity of the employee is respected. The employer must take sufficient steps to eliminate its employees' expectation of privacy and confidentiality, limiting the use of the corporate email exclusively to a professional use and implementing an adequate policy on use of company equipment.

In line with the above, and from a data protection standpoint, the SDPA-GDR specifically allows the employer to access content resulting from the use of digital media provided to employees in order to monitor compliance with their work obligations and ensure the integrity of the devices, provided that the following conditions are met:

- Setting criteria/rules for the use of digital devices respecting minimum standards of employee's privacy protection;
- In the event that the employer allows the use of digital devices for private purposes, the authorized uses must be precisely specified in advance and adequate safeguards must be put in place in order to preserve employees' privacy;
- Necessarily involving employees' representatives in the development of these criteria/rules; and

– Informing employees as above and have the means to demonstrate that such information has been provided.

From a criminal law perspective, non-compliance with data privacy, employment and case law requirements may lead to decisions of courts declaring the respective evidence null and void.

c) Collecting (electronic) documents and/or other information?

Please see the answer to 5a above. Furthermore, please note that in the event that personal data is collected from sources other than the data subject, the information requirements set forth in Article 14 GDPR must be fulfilled.

d) Analyzing accounting and/or other mere business databases?

Please see the answer to letter 5a above. Furthermore, please note that in the event that personal data is collected from sources other than the data subject, the information requirements set forth in Article 14 GDPR must be fulfilled.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There are no specific regulations on how to conduct employee interviews. However, as a matter of best practice, interviewees are normally provided with written instructions including a brief description of the background of the investigation and the purposes behind the interview.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

Despite the absence of specific formalities, the right against self-incrimination is a fundamental right that should be guaranteed when conducting an internal investigation. The interviewee should not feel pressured to provide the information. Therefore, it is advisable to inform the interviewees that their collaboration is voluntary (despite disciplinary actions), that they do not have to make self-incriminatory statements, and that they will have the "final say"– i.e. provide a last version of the facts.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no explicit legal obligation to do so, though it is advisable to always make clear to the interviewee that the lawyer attending the interview represents the company. However, when there are connections to U.S. law, an Upjohn warning must always be given.

d) Be informed that they have the right that their lawyer attends?

There is no specific provision under Spanish law. If the interviewee demands to be assisted by a lawyer, allowing such attendance could be considered, even more if the interviewee is a suspect. However, there is no obligation to do so.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is no legal obligation, but it would be advisable to give such opportunity unless it can be considered unfeasible.

In case the employee requests such attendance, the person conducting the interview should not refuse it. Only in exceptional cases the interviewer could refuse the attendance of an employees' representative (e.g. when the works council is also subject to the investigation).

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Yes. Under the GDPR the data controller must inform the data subject about certain mandatory aspects of the processing of their personal data (e.g. the data transfers outside the European Union, the identity of the data controller, the purposes of the processing and the legal basis, etc.).

g) Sign a data privacy waiver?

The signature of a data privacy waiver would not be required. However, the data subject must receive prior information about the processing of such data.

h) Be informed that the information gathered might be passed on to authorities?

Yes. In compliance with the information obligation referred to above, the data controller must inform data subjects about the recipients of the personal data, if any. In the context of whistleblowing systems, the SDPA-GDR expressly refers to the transfer of data to the competent authority when necessary for the adoption of disciplinary actions or the handling of legal proceedings.

i) Be informed that written notes will be taken?

There is no such legal obligation under Spanish law. It is normal practice to memorialize interviews documenting all discussed facts. Preferably, the interviewee should be asked to review the notes to double check if she/he agrees or wants to provide further explanation of certain facts.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific legal provision in this regard under Spanish law. However, document-retention notices are generally admitted and used in order to preserve the aim of internal investigations and also in order for the company to be able to prove that this notice was served on and received by the individuals involved.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege is not expressly provided for in Spanish law. A similar institution would be the professional secrecy. This is a wider concept and is based on the duty of confidentiality that lawyers owe in respect of any information received from their clients while acting on their behalf. Therefore, as both concepts entail similar consequences, attorney-client privilege or professional secrecy rights may be claimed over findings of an internal investigation.

Recommended steps to ensure this protection would be as follows:

- Labelling privileged documents accordingly;
- Appointing one or few individuals as the contact persons with the attorney to be considered as the "client";
- Limiting access of other individuals in the company to privileged communications or documents and, of course, avoid disclosure to anyone outside the company;
- Limiting the amount of generated work products where findings and conclusions over the investigations are described; and
- Avoiding keeping work product at the company's premises, but at the outside counsel's instead.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

It is under discussion, but the most recent Supreme Court rulings argue that attorney-client privilege or professional secrecy does not apply to in-house counsel under Spanish law.

There is case law establishing that communication between client and legal counsel and documents drafted within such attorney-client relationship are privileged provided that (i) correspondence is related to the rights of defense of the client and (ii) communication is conducted with independent lawyers.

Insofar as in-house lawyers are not independent but employees of the company, communication with inside counsel and documents drafted by them are not privileged.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

As far as circumstances arise which could give reason to a claim against the insurance company, it is advisable that the policy holder makes a notification of circumstances to the insurer. The respective insurance policy should be checked in that regard.

b) To business partners (e.g. banks and creditors)?

This has to be decided on a case-by-case basis. The following aspects should be taken into account:

- Are there any contractual obligations to provide such information; and
- Might the notice be deemed utterly important for the counterparty with regard to the purpose of the agreement, according to contractual good faith? These interests of the business partner need to be evaluated against the legitimate interests of the company.

c) To shareholders?

The Securities Market Act imposes the obligation to communicate relevant information to the investors of listed companies. Any information that could concern the investors in their decision to trade in securities or could affect the securities' price is relevant. For instance, if the company initiates an internal investigation based on serious indications that, for example, a criminal offense was committed, it could – depending on a case-by-case analysis – be reasonable to convey such information to the investors.

d) To authorities?

Listed companies also have to notify the Securities Market National Commission of any relevant information as described under 10c above.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Considering that committing an illegal behavior within a company may be an indication that the management body did not exercise its duties of care, surveillance and control, once an investigation is started one would generally check whether there are any shortcomings in the corporate compliance program.

Additionally, the company can take two opposite decisions depending on the defense procedural strategy it intends to choose. The company can either (i) try to defend the alleged infringer or (ii) try to react by sanctioning them in order to demonstrate its intolerance with illegal or unethical conducts by publicly condemning the behaviors committed and providing resources so that third parties can help clarify the case at hand.

In any case, the company should make sure that any ongoing breach of law is immediately stopped and consider other mitigation actions.

Lastly, it is crucial to ensure the preservation of all relevant material which could serve as evidence in a judiciary proceeding.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

In Spain, internal investigations are not broadly developed. However, the General Public Prosecutor's Office recently stated that providing the prosecution with the results of an internal investigation is an indication of ethical commitment and could entail exoneration from corporate criminal liability.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Search warrants and dawn raids are foreseen and regulated in the Spanish Competition Act, the Spanish General Taxation Act and the Criminal Procedural Act. With regard to Competition Law, the Spanish Competition Commission ("**SCC**") has the right to access business and domestic premises if there are indications of anticompetitive behavior if approved by the Director of Investigation or a judge.

Tax inspectors can only perform a dawn raid upon a judicial warrant or when the owner or entitled individual of the company expressly authorizes them to access the premises of the company.

In the context of criminal proceedings search warrants and dawn raids have to be ordered by an examining magistrate, *ex officio,* or at the police's request, and have to be strongly justified specifying reasons with solid indications of a criminal offense, the dawn raid's goal, the objects to be searched, how and when the search should be performed, who must be present, etc. Account books and documents may not be seized by the police unless the magistrate's order mentions them specifically.

In case these legal requirements are not fulfilled, it will generally lead to a declaration of the seized pieces of evidence as null and void and to invalidation of other pieces of evidence that may be deemed directly related to such evidence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Spanish law does not expressly provide for non-prosecution agreements and deferred prosecution agreements.

However, a plea bargain is not uncommon. Accused individuals or entities tend to reach agreements with the prosecutor once the investigating stage ends to terminate the proceedings with a plea bargain ("*sentencia de conformidad*"). This does not overrule criminal liability, but generally results in more lenient penalties.

Additionally, the Spanish Public Prosecutor Office has stated that in the event that a company detects an offense committed within it and reports it to the authority, the prosecutor must not press charges against the company.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

As a general rule, individuals cannot face criminal liability for misconduct of other individuals. However, omissions may give rise to criminal liability when an individual, in this case a director, breaches their duty of care. Criminal liability may then arise if the director has actively caused such misconduct, given the fact that they had effective control over the activities of the respective individual and should have acted to avoid such misconduct. In these cases, penalties to individuals can include fines, imprisonment, or even special barring from public employment and office, profession, trade, industry, or commerce, etc.

Companies can be held criminally liable for misconduct of other individuals (its employees, officers, or directors) acting on its behalf.

When a legal entity is criminally punished, it must be fined. Other penalties may be imposed additionally. This includes suspension of activities, closure of premises, prohibition to develop the activities through which the offense was committed or concealed, prohibition from receiving public subsidies and public procurement debarment.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

According to Section 31 B of the Spanish Criminal Code ("**SCC**") the company shall be exempt from liability if the following conditions are met:

- The management body adopted and effectively implemented, prior to commission of the offense, a compliance program to prevent the commission of similar offenses, or significantly reduce the risk of the commission thereof;
- Supervision of the compliance management system was entrusted to a person or a body of the legal entity which has independent powers of initiative and control;
- The perpetrators committed the offense by fraudulently evading the compliance program; and
- There was no negligent lack of supervision or control by the person or body in charge of the compliance program.

If only partially fulfilled, these circumstances shall mitigate the penalty.

There is no specific legal provision in Spanish law with respect to directors, officers, and employees.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The Securities Market Commission received more than 700 anonymous complaints in the first year of operations of its whistleblowing tool (2018) through which any person can report any violation of supervisory provisions. 45 percent of said complaints contained sufficient factual evidence to proceed with its analysis. In 2019 60 percent of the investigations conducted by the Spanish Authorities on Competition resulted from reports received via the Authorities' whistleblower email hotline.

Further, in 2019 the SCC was amended in order to incorporate certain EU Directives. Said amendments expanded the closed list of offenses which can trigger criminal corporate liability, extended the scope of private corruption and public bribery and broadened the concept of public official with regard to bribery and embezzlement. In addition, the maximum duration of criminal investigations provided for in the Code of Criminal Procedure has been extended from six months to one year, subject to extension, and there is a debate around the possibility of making Public Prosecutors the main investigators in judicial proceedings, instead of being the Judges.

Lastly, on the one hand, several relevant judicial investigations are being carried out in Spain regarding financial markets (Banco Popular) and corruption (the Villarejo Case, which involves more than 15 high profile companies from all sectors). On the other hand, there are other relevant judicial investigations that have concluded, with both acquittals (Bankia) and convictions (Pescanova).

CONTACT

Paseo de la Castellana, 36-38
Planta 9
28046 Madrid
Spain

Tel.: +34 91 349 82 00
Fax: +34 91 349 82 01
www.hoganlovells.com

Ignacio Sánchez
Partner
Hogan Lovells Madrid
T +34 91 349 82 93
ignacio.sanchez@hoganlovells.com

Ignacio Sánchez is a vocational criminal lawyer who will go the extra mile by using creative alternatives, meticulous preparation and attention to detail. He has a wealth of experience on various commercial fraud matters, including fraud relating to banking, insurance, the Internet, insolvency, embezzlement and employees' fraud.

Recognized for his significant experience in the Investigation, White Collar and Fraud practice, Ignacio advises and represents high profile clients in complex and sensitive criminal proceedings acting either as a prosecuting party or defense. According to his clients, he "knows how to handle the situation, and when things get complicated, I like having a lawyer like him".

Ignacio also advises on tax related crimes, money laundering and intellectual property crimes and on the development of corporate compliance programs. In addition, he conducts independent investigations on behalf of corporate boards and supervisory authorities to assess liability determine implications and deal with authorities and agencies.

Sweden

Nordia Law


Hans Strandberg


Olle Kullinger


Carl-Johan Allansson

Overview

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes		X	X	X Only for certain crimes, but wide interpretation of when a crime has been committed in Sweden.	X Only in some cases, and not if a crime has been committed by a leading individual of a company.
No	X No criminal liability for companies, but companies can, in certain circumstances, be fined for crimes committed by employees or executives acting within the scope of their duties.				

Question List

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Swedish law makes a distinction between whistleblower protection in the public and private sectors.

In the private and public sector, an employee who reports internally about severe misconduct within the employer's operation is in general protected against reprisals. The same applies in relation to an external report if an employee first reported the misconduct internally and the employer did not take reasonable actions, or an employee by other reason had reasonable grounds to first report externally and there was substance to the allegation.

Within the public sector, an employer is generally not allowed to investigate who the whistleblower is, and, if the employer knows who the employer is, the employer is not allowed to take any sanctions against the whistleblower. A prerequisite for the protection is, however, that the employee make their report available to the media for the purposes of publication.

If a whistleblower report is made, it is good practice for the employer to investigate, unless exceptional circumstances exist, like the report is clearly made in bad faith or is clearly implausible.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Unless disciplinary actions are initiated against the employee, there is no requirement to notify the works council of an internal investigation.

b) In accordance with the European General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the data protection officer ("**DPO**") must consult with employees regarding data privacy rights and must monitor data protection. A company, therefore, will need to inform the DPO about all data privacy related procedures and processes of an investigation.

c) Companies do not have a general duty under Swedish law to inform the prosecution authority of an internal investigation. However, a certain special legislation exists that requires reporting to authorities, e.g. the Money Laundering and Terrorist Financing (Prevention) Act, the Public Employment Act, and the Companies Act (in regards to auditors of limited liability companies).

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Under Swedish labor law employees have a duty of loyalty to their employer, which is expansive. In general, due to the duty of loyalty, employees are required to support an investigation and participate in interviews. The employer cannot force an employee to participate, but a refusal to participate may be regarded as misconduct and can lead to sanctions, such as dismissal.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Notice of termination or dismissal must be given by the employer within two months of knowledge of the reason for the termination or dismissal. If the company initiates an internal investigation, the two-month deadline would most likely begin if/when the employer has sufficient information concerning the conduct of the individual.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Data privacy laws, mainly the GDPR and the Data Protection Act which is a supplement to the GDPR, apply to the processing of data, including securing, collecting, and reviewing personal data. This includes the compiling of (electronic) documentation, which relates to the scope of an investigation (e.g. creation of a database). It is important to perform an early assessment of the applicable data privacy laws and to document the steps taken.

b) Reviewing emails?

The employer needs to adhere to the GDPR and the Data Protection Act, which means that the employer, in general, must inform the employees about the inspections that might be performed and the purpose for which their personal data will be processed. As a main rule, the employer has no right to read or otherwise take note of an employee's private emails or files. Exceptions exist where there is a serious suspicion of unfair or criminal conduct or where the employee is using IT equipment contrary to internal guidelines. It

should be stressed that such personal data may only be processed if the employer has a legitimate interest in processing the data, and that such an interest is not overruled by the rights or freedoms of the employee. Thus, the employer's legitimate interest must always be weighed against the employee's rights and freedoms.

c) Collecting (electronic) documents and/or other information?

Data privacy laws apply to the collection of personal data.

d) Analyzing accounting and/or other mere business databases?

An employer may analyze any documents that belong to the company. However, if such databases include personal data, data privacy laws may be implicated.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There are no regulations in Sweden governing the conduct of internal interviews of employees by companies. Therefore, a company has no legal obligation to instruct an employee about the legal circumstances and their rights. However, ethical considerations counsel in favor of giving the employee a brief description of the background and subject matter of the investigation. There is no specific form prescribed for such a description.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no legal obligation in Sweden to inform an interviewee in an internal investigation about self-incrimination.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no legal obligation in Sweden to give an interviewee an Upjohn warning, but it is required, according to the Code of Ethics for members of the Swedish Bar Association, to do so in certain situations. In a matter before the courts, members of the Swedish Bar Association are legally obliged to follow the Code of Ethics. If a company lawyer is attending the interview, the interviewee can be informed that they have the right to hire their own lawyer. There is, however, no duty to inform.

d) Be informed that they have the right that their lawyer attends?

There is no legal obligation in Sweden to inform the interviewee that they have the right that their lawyer attends. However, the company should recommend that an interviewee suspected of criminal misconduct retain legal counsel. If the interviewee has already retained counsel, the interviewee should not be contacted directly by the company's lawyer, without prior approval from the interviewee's lawyer.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Unless disciplinary actions are taken against the employee, there is neither a right for the employee to have a representative attend the interview nor a requirement for the company to inform the employee.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The relevant employees must be informed in the event that their personal data will be transferred to a recipient in a country outside of the European Union. Moreover, personal data may only be transferred outside of the European Union in the event that the conditions for such transfers, laid down in the GDPR, are complied with. For example, personal data may be transferred outside of the European Union without the prior consent of the person concerned, if the data protection level in the foreign country is considered to be adequate pursuant to an adequacy decision adopted by the Commission. The United States were previously approved as "adequate", if the data receiver was connected to the EU-U.S. Privacy Shield, in accordance with the Commission's adequacy decision on the EU-U.S. Privacy Shield. However, the Court of Justice of the European Union declared the adequacy decision on the EU-U.S. Privacy Shield invalid in its judgment in *Facebook Ireland and Schrems* (C-311/18) on 16 July 2020. Hence, the adequacy decision on the EU-U.S. Privacy Shield no longer constitutes a valid basis for transfers of personal data to data receivers

in the United States under the GDPR. This means that transfers of personal data to recipients in the United States must either be subject to appropriate safeguards (according to Article 46 of the GDPR) or fulfill at least one of the conditions for derogations specified in Article 49 of the GDPR (derogations for specific situations).

g) Sign a data privacy waiver?

There is no requirement in the GDPR and/or the Data Protection Act that a data privacy waiver shall be signed prior to an employee interview. The employee shall however receive information about the processing of his or her personal data at the time when the personal data is obtained, pursuant to the GDPR. Such information can be provided in writing or be supplied orally at the interview.

As already mentioned, personal data may be processed if the employer has a legitimate interest in processing the data, and such an interest is not overruled by the rights or freedoms of the employee. In the context of an investigation, an employer generally has a legitimate interest to process personal data. That said, the employer must always balance its interest against the employee's rights and freedoms.

The GDPR sets out certain requirements that must be met in order for consent to be valid. Among others, the consent must be freely given, i.e. consent is not valid if it was given under pressure from the employer. It is therefore questionable whether and/or to what extent the processing of personal data for the purpose of an internal investigation may be based on the employee's consent.

The GDPR does not contain any provision that governs how consent should be obtained. It is, nevertheless, good practice to sign a data privacy waiver when the employee's consent constitutes the applicable legal basis for the processing. This is, however, not a pre-requisite for an interview.

h) Be informed that the information gathered might be passed on to authorities?

There is no legal obligation in Sweden to inform the interviewee that the information gathered might be passed on to authorities. It is, however, considered good practice.

i) Be informed that written notes will be taken?

There is no legal obligation in Sweden to inform the interviewee that the interview will be documented. It is, however, considered good practice.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is neither a regulation applicable to document hold notices in Sweden nor an accepted practice in this regard.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Swedish regulations concerning attorney-client privilege are limited and their applicability is highly dependent on where the documents are located and the type of information in the documents. Documents collected in the course of an internal investigation (e.g. emails) are not *per se* protected by privilege. However, analysis and conclusion drafted by an attorney, as well as correspondence relating to such analysis and conclusions, may be protected.

In order to ensure privilege, it is recommended to involve an attorney admitted to the Swedish Bar Association (advokat). In accordance with the Code of Ethics for members of the Bar Association, an advokat has a duty of confidentiality and, therefore, correspondence with an advokat is, in general, treated as confidential. Further, attorney-client privilege also applies to correspondence with attorneys admitted to the bar in the EU when they conduct business in Sweden. This provision is not applicable when a non-Swedish attorney provides services from their home country to a client in Sweden through a letter, phone, or telefax. Documents or correspondence from an attorney operating outside of Sweden is, therefore, not covered by attorney-client privilege. Documents in the custody of external attorneys are also, in general, protected. Therefore, for sensitive matters, it is recommended that

any documents generated in the course of the investigation be stored only on external attorney's servers, instead of on the company's premises.

It is recommended to label documents as privileged and confidential, even though labeling is neither required for privilege protection nor ensures privilege.

Privilege protection will more likely be granted if the advice is provided in relation to a (potential) investigation by authorities. This can be shown by setting up a separate engagement letter for the internal investigation.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

According to Swedish law, communication with in-house counsel is not protected from disclosure by attorney client-privilege, as an in-house counsel may not be a member of the Swedish Bar Association.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

It is always advisable to notify the insurance company as soon as possible, as the insurance agreement can impose different notification requirements. Further, the Swedish Insurance Agreements Act Chapter 7 Section 4 contains provisions on the statute of limitations.

b) To business partners (e.g. banks and creditors)?

There is no general requirement to notify business partners of an internal investigation, except for business partners that may have a claim for damages due to the underlying conduct.

c) To shareholders?

A listed company is obliged to disclose price-sensitive information to the market. Knowledge of an internal investigation constitutes price-sensitive information when a director is served a notice of suspicion by authorities, but it may also be price-sensitive well before that occurs.

d) To authorities?

There is no requirement to notify the prosecution authority of an internal investigation. It is advisable to be cooperative with the prosecutor as this may prevent unexpected measures by the authorities, such as dawn raids. However, there is no legal ground for relief from penalties (e.g. corporate fines) for cooperating with authorities.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

As mentioned under 10c above, a listed company is obliged to disclose price-sensitive information. A company should also try to stop ongoing criminal behavior conducted within the company's operations. It is further considered good practice, when permitted under labor law, to investigate and freeze email accounts and other similar measures.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices do not, in general, have any concerns about internal investigations. An internal investigation is a company's own matter and the prosecutor has no right to intervene. However, the prosecutor may take independent actions against the company, such as confiscating documents. Documents concerning the investigation itself, if covered by attorney-client privilege, will not be confiscated.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

The police, the prosecutor, or the court can decide to issue a search warrant if there is reason to believe that a criminal offense punishable by imprisonment has been committed. A search warrant can be obtained for a company if: (i) the offense is believed to have been committed on the company's premises; (ii) the suspect was detained on the company's premises; or (iii) extraordinary reasons indicate the search will lead to an item or information regarding the offense. In relation to extraordinary reasons, there must be one or more factual circumstances that substantially show one can reasonably expect to recover evidence for the investigation.

The principle of free adducing of evidence and the principle of free evaluation of evidence under Swedish law allow the prosecution authority to use, and the court to evaluate, evidence obtained even through an unlawful search and seizure.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

No deals, non-prosecution agreements, or deferred prosecution agreements can be made under Swedish law.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Corporations are not subject to criminal liability under Swedish law but can be fined for crimes committed by employees or executives acting within the scope of their duties where (i) the company has not done what was reasonably be required to prevent the crime or (ii) the crime is committed by an individual in a leading position or with a particular supervisory or control responsibility in the company. In such situations, any illegally obtained profits may be forfeited.

There is no possibility for a court to impose a general debarment on a company in a criminal trial, but according to the Swedish rules on public procurement, a prior verdict imposing a corporate fine on a company may, in certain cases, lead to the company's debarment from a procurement.

Directors and/or employees to whom certain responsibilities have been delegated may be criminally liable for their acts of omission, for example regarding bookkeeping crimes, work environment crimes, and reckless financing of bribery. Penalties for such crimes are fines or imprisonment, but several combinations and types of conditional sentences may be imposed.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

The Penal Code only criminalizes acts by natural persons (individuals), which is in line with the principles of the Swedish Criminal Law that only natural persons can be held criminally responsible. As a result, companies cannot be prosecuted.

If a person has committed a crime, and the act was committed as part of a company's business activity, the company could face criminal trial and be imposed corporate fines between 5,000 Swedish kronor and 500 million Swedish kronor. Corporate fines under Swedish law are not a criminal sanction, even though closely related, but a special effect of a crime (committed by an individual) and sanction companies for not effectively preventing corruption. Hence, a company could be subjected to corporate fines if it fails to act in a way that reasonably would have prevented a crime.

There is no specific provision stating that penalties for individuals may be reduced if the company in question has implemented a compliance system. But a corporate fine may be suspended or reduced if the company on a best effort basis has tried to prevent a crime or taken action to mitigate the effects of a crime. Corporate fines could also

be reduced if a compliance system has been implemented after a crime has been committed and the company – as a consequence of the implementation – reports the crime.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The recent most significant event is the revised provisions concerning corporate fines that came into effect on 1 January 2020. The new rules contain several amendments, the most noteworthy being that the maximum fine is increased from 10 million Swedish kronor to 500 million Swedish kronor, and that Swedish courts are given extended jurisdiction to try international bribery crimes. Further, the new provision will make it possible to impose corporate fines not only on corporations or other entities that conduct business but also on public sector entities which operations are comparable to business activities.

CONTACTS

NORDIA
SWEDEN • NORWAY • DENMARK • FINLAND • LAW

World Trade Center
Kungsbron 1, Entrance F, 4th floor
111 22 Stockholm
Sweden

Tel.: +46 8 563 08 100
Fax: +46 8 563 08 101
www.nordialaw.com

Hans Strandberg
Partner
Nordia Law
T +46 8 563 08 100
hans.strandberg@nordialaw.com

Hans Strandberg is a former judge in District Court and the Court of Appeal where he served for 10 years. He has been a lawyer since 1986 specialized in company and business related criminal law, besides of compliance and securities law. On his client list are more than 15 of the largest Swedish public companies, some multinational foreign public companies and foreign states. He is litigator and has appeared in most of the public criminal cases involving listed companies as well as in the Supreme Court. He has also been involved in legislative work regarding Swedish corruption law and has been active in producing the Swedish Code of Conduct related to corruption for companies. He is also active in examining lawyers when becoming members of the Swedish Bar Association.

Olle Kullinger
Partner
Nordia Law
T +46 8 563 08 100
olle.kullinger@nordialaw.com

Olle Kullinger has been with the firm since 2007 and specializes in company and business related criminal law, as well as compliance and securities law. Olle Kullinger has worked with many of the largest listed companies in Sweden as well as a range of other companies whose businesses have been questioned. He is a litigator and has appeared in a number of cases concerning white collar crimes, representing both companies and directors. Olle Kullinger has appeared as counsel two times before the Supreme Court. Olle Kullinger has headed and taken part in a number of internal investigations. He has also been involved in legislations work regarding the Swedish corruption legislation and has been active in producing the Code on Gifts, Rewards and other Benefits in Business together with a number of the largest listed companies in Sweden.

Carl-Johan Allansson
Partner
Nordia Law
T +46 8 563 08 100
carl-johan.allansson@nordialaw.com

Carl-Johan Allansson has been with the firm since 2007. He is specialized in company and business related criminal law and litigation. Carl-Johan Allansson has worked with many of the largest listed companies in Sweden as well as a range of other companies whose businesses have been questioned. Carl-Johan Allansson has assisted in a number of internal investigations.

Switzerland

taormina law AG

Dr. iur. Andrea
Taormina LL.M.

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	Limited	X	X	Very limited	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

Despite recent legislative efforts, no general laws for handling of whistleblower reports and whistleblower protection have been enacted in Switzerland. Employers are subject to a general duty of care towards their employees, which might include protective measures in case of internal conflicts or mobbing triggered by a whistleblower report. In some cases it may be advisable to suspend whistleblowers (on full pay) following their report.

Termination following a whistleblowing report may be lawful in some cases, unlawful in others. In the absence of clear-cut rules, each individual whistleblowing case has to be decided on its own merits.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Internal investigations do not require prior disclosure to employees or to their representatives.

b) No information duty applies with regard to the data protection authorities or the company's (internal) data protection officer.

c) There are no information requirements to other local authorities.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees have a general duty of loyalty towards the employer's legitimate interests. This includes supporting an internal investigation. Disciplinary measures for non-compliance are possible in principle, provided employee personality rights are respected.

Termination on grounds of non-cooperation is not advisable in most cases, however, and might be frowned upon by authorities, since employees should remain available for any subsequent official investigation.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

Investigative actions do not trigger any specific deadlines. Neither can they be qualified as waivers of any rights of the employer.

On the other hand, a whistleblowing report might lead to the suspension of termination rights. As a general rule, termination of an employee's contract may be unlawful if said employee has asserted claims under the employment relationship in good faith prior to the termination. Thus, in cases where investigative action was triggered by a (rightful) complaint of an employee, said employee is protected from termination for a certain time afterwards.

Although no general whistleblower protection exists under Swiss law, this rule has in practice been applied to certain whistleblowers who acted in good faith and correctly followed any applicable procedures.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

Secrecy obligations, such as banking secrecy, might be applicable depending on the sector in which the company is active. General data protection principles must be observed. While not part of Swiss legislation, under certain circumstances (targeting criterion), the General Data Protection Regulation of 27 April 2016 (Regulation (EU) 2016/679 of the European Parliament and the Council) may have to be observed.

The presence of external counsel at the interview (in the role of conductor of the investigation or of employee counsel) is unproblematic if such counsel is subject to professional secrecy. Other third parties must not be present at interviews if secrecy obligations apply.

b) Reviewing emails?

Private correspondence by employees must not be reviewed. If employees' email accounts are legitimately used for private purposes, such correspondence must be excluded from the review. Such exclusion can require time-consuming and costly triage procedures. Preventive measures (email policy, clause in employment agreement) are therefore highly recommended.

As soon as emails are disclosed to third parties, secrecy obligations may have to be observed in certain sectors.

c) Collecting (electronic) documents and/or other information?

The collection of documents and other information (unlike their disclosure) is not subject to any secrecy/privacy obligations, as long as they are solely intended to be used in an internal investigation or in an official procedure by a Swiss authority.

In the case of procedures by foreign authorities or proceedings before foreign courts, the mere collection of documents on Swiss territory might qualify as an unlawful activity on behalf of a foreign state (punishable by imprisonment or monetary penalty). It is important to note that pre-trial discovery can be problematic under this rule. Exemptions can be requested (prior to the investigation) from the competent Swiss authority.

Permanent electronic supervision of employees (by cameras or by constant monitoring of information technology use) is only permitted in exceptional circumstances.

d) Analyzing accounting and/or other mere business databases?

In this regard no secrecy/privacy obligations apply.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

Written instructions are not mandatory by law, but highly recommended. They might subsequently serve as evidence that procedural requirements have been met.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no directly applicable legal duty to inform employees thereof. However, it is general practice in Switzerland that such information is given. With a view to the future use of employee statements in a criminal/civil procedure, such information is highly recommended.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

No formal requirement applies. It is, however, highly recommended to clearly explain (in writing) the circumstances of the interview to the employee.

d) Be informed that they have the right that their lawyer attends?

Swiss law does not grant an explicit right to the employee to request attendance of their lawyer. Nonetheless, it is general practice to allow such attendance. It is advisable (rather than mandatory) to inform the employee thereof.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There are no such attendance rights that would exist under Swiss law.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Swiss data protection law requires transparency in this regard, thus the employee must be informed that data may be transferred abroad.

In addition, the transfer to countries lacking an adequate level of data protection requires specific legal justification. The list of such countries, compiled by the Swiss data protection authority, includes the United States of America. Employee consent is one possible form of justification. Other forms include overriding private or public interests, as well as group privilege in case of multinationals.

It is important to observe that the disclosure of sensitive information to a foreign recipient might be problematic in spite of explicit consent by the information owner. The provision on industrial espionage prohibits the disclosure of trade secrets to foreign agents. Since this provision protects public as well as private interests, a waiver by the information owner is not sufficient in some cases.

g) Sign a data privacy waiver?

Disclosure of data requires legal justification. Employee consent is one possible form of justification. Other forms include overriding private or public interests. Thus, data privacy waivers are only necessary in absence of other grounds for disclosure.

h) Be informed that the information gathered might be passed on to authorities?

General data protection principles require the employer to specify the possible use of personal data provided by the employee. It is advisable to explain the investigation procedure to the employee.

i) Be informed that written notes will be taken?

In this regard no express information requirement applies. It is, however, advisable to explain the investigation procedure to the employee.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Document hold notices are unknown in Switzerland. If issued regardless, they are without legal effect. This must not be interpreted as permission to destroy evidence. Such destruction could unfavorably influence the outcome of a trial, since it would be taken into account by the court when weighing the evidence.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Under Swiss law, attorney-client privilege exclusively applies to external counsel. If an investigation is conducted by external counsel, any work products or forms of correspondence are protected. No formal steps such as expressly marking documents as confidential are required. Nevertheless, it is advisable to use such markers, in particular if documents could potentially be disclosed abroad at a later stage.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Under Swiss law, attorney-client privilege does not apply to in-house counsel or compliance officers. Thus, any findings in investigations conducted without assistance of external counsel are outside the scope of attorney-client privilege.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

In this regard, no general rules apply. Notification requirements might be included in the terms of any specific insurance policy.

b) To business partners (e.g. banks and creditors)?

In this regard, no general rules apply. Banks and other creditors may include specific clauses in loan agreements and other contractual instruments.

c) To shareholders?

Shareholders must be informed annually about the course of business of the company at the general meeting. They are entitled to demand additional information at this opportunity. Outside the general meeting, no information duty applies and no such requests by shareholders are possible.

Listed companies are subject to *ad hoc* publicity requirements. Facts that are not known publicly and that (from an *ex ante* perspective) could potentially lead to a significant change in share prices must be communicated to the public. Under these rules and subject to a case-by-case analysis, serious incidents (such as big-scale bribery) which trigger investigations must be disclosed to the public.

d) To authorities?

No general information requirement applies. Even in the case of criminal acts, companies are under no general obligation to notify authorities. Notification might, however, have a mitigating effect in criminal or administrative procedures.

A specific leniency application program applies to cartel investigations. The first party to report the cartel to the Swiss Competition Commission ("**COMCO**") might benefit from a full immunity from fines.

Companies under supervision by sector-specific authorities might be subject to specific requirements. This applies in particular to the reporting duty towards the Swiss Financial Market Supervisory Authority ("**FINMA**") in the financial sector.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Employers are subject to a duty of care towards their employees. If the alleged conduct leads to any threat or damage to employees' interests, immediate measures to protect other employees might be required under Swiss employment law. Suspension of employment is possible at any time under Swiss law. It might be advisable to suspend certain employees on full pay.

No general duty to prevent criminal behavior exists under Swiss law. Nonetheless, companies are under an express duty to take reasonable and sufficient preventative measures against certain offenses, namely money laundering, bribery and terrorism financing. In view of the rules on corporate criminal responsibility and general principles of corporate governance, companies are generally recommended to enact and uphold an effective compliance program.

Regardless of the nature of the (alleged) offense, companies are recommended to take immediate measures aimed at the discontinuation of any discovered or suspected criminal conduct by employees. Specialist legal advice might be required to determine the nature and scope of such measures to prevent prejudice to the investigation's outcome (or a premature admission of employer negligence).

Measures aimed at limiting the company's financial damage might also be advisable with a view to future damage claims against perpetrators. A general duty to mitigate damages exists under Swiss law.

In the case of a limited number of offenses (namely money laundering, bribery and terrorism financing), companies can be fined regardless of any individual's responsibility, if they failed to take reasonable and sufficient preventative measures.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

In general, public prosecutors and other authorities encourage and reward internal investigations. The conduct of a thorough internal investigation might lead to a considerable mitigation in case of criminal or administrative sanctions.

With a view to future criminal or civil proceedings, it is advisable to observe basic procedural requirements when conducting an internal investigation. Even then, interview transcripts will generally not suffice the strict requirements for evidence in official proceedings. They might, nonetheless, serve to give authorities indications as to how to establish the relevant facts in the course of their investigation.

As soon as a criminal or civil procedure is imminent or opened, contact to (potential) witnesses might be problematic. Complex, largely unwritten, rules apply. Thus, professional advice is highly recommended in this regard.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Although search warrants must be issued in writing by the prosecutor, oral warrants are admissible in urgent cases. Searches can be conducted against the will of the occupant of the premises if evidence is expected to be found. Sealing of any seized items or (electronic) records can be demanded. The prosecutor will subsequently have to file a request for removal of the seal.

In principle, any unlawfully obtained evidence is inadmissible. Exceptions to this rule are, however, granted routinely if the evidence could have been obtained legally and if its use considerably furthers the establishment of the truth. The "fruit of the poisonous tree" doctrine is not applicable under Swiss law.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Public prosecutors have limited discretion regarding the opening of an investigation against a certain subject. Nonetheless, self-reporting and maximum cooperation might be beneficial at this stage.

With regard to criminal prosecution, a guilty plea can enable an abbreviated procedure, leading to a summary judgment which is drafted by the prosecutor and approved by a court. Abbreviated procedures are only possible for penalties up to five years' imprisonment, in cases where the defendant fully acknowledges the facts of the case and recognizes, in principle, any civil claims brought in connection with the offense.

Minor offenses can lead to a punishment order, provided the defendant acknowledges the facts. Such cases are resolved without the involvement of a court.

FINMA and COMCO conclude their procedures with formal decisions. Self-reporting and cooperation by the subject of the investigation is taken into account when deciding upon sanctions. Prior to the opening of a formal procedure, maximum cooperation may lead to the abandonment of the investigation.

A specific leniency application procedure applies in the case of cartel investigations. COMCO may grant full immunity from fines to the leniency applicant.

Specialist legal advice regarding self-reporting and cooperation is highly recommended, since detailed knowledge of the legal framework as well as experience in dealing with the authorities involved is essential when determining the best strategy for an impending official investigation.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

In Swiss criminal law, the focus lies on the responsibility of the individual. Directors, officers, or employees may face monetary penalties and imprisonment. Additionally, criminal courts can impose professional bans or issue expulsion orders for foreign nationals.

The scope of corporate criminal liability is limited. Companies cannot be convicted as perpetrators of a crime. Rather, the law penalizes organizational shortfalls within the company. Thus, companies can be fined if a criminal offense by an employee or director cannot be attributed to an individual due to organizational deficiencies. In the case of a limited number of offenses (namely money laundering, bribery, and terrorism financing), companies can be fined regardless of any individual's responsibility if they failed to take reasonable and sufficient preventative measures. Thus, the introduction of adequate and effective compliance procedures can serve to protect companies from criminal liability. The upper limit for fines imposed on companies is five million Swiss francs.

In COMCO proceedings, fines are imposed upon companies and/or individuals. Fines for companies can be calculated in proportion to their turnover.

In FINMA proceedings companies can be fined and individuals face fines or (rarely) imprisonment. Other possible sanctions include the revocation of a company's license or occupational bans for individuals.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Penalties for companies are assessed, *inter alia*, based on the gravity of the company's lack of proper organization. Accordingly, serious organizational deficiencies will likely increase the penalty. This rule only applies if the compliance system was implemented prior to the alleged misconduct.

As a general rule, penalties of directors, officers, and employees are not reduced or suspended in case of an efficient compliance system.

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Internal investigations were not traditionally part of the Swiss legal landscape. This is still apparent in the lack of specific legislation for this field. In the last decades, however, internal investigations have rapidly become a much-practiced instrument. They are being recognized and encouraged by authorities.

The U.S. Department of Justice Program of 29 August 2013 led to a massive surge in internal investigations, since approximately 100 Swiss banks decided to investigate whether there were indications of past violations of U.S. tax laws.

Recent changes in anti-bribery legislation (tightening of laws against private-sector bribery) may lead to a further increase of the number of internal investigations conducted by Swiss companies.

CONTACT

taormina

Kanzleistrasse 127
CH-8004 Zürich
Switzerland

Tel.: +41 44 455 66 60
www.taormina-law.ch

Dr. iur. Andrea Taormina, LL.M.
Specialist Criminal Attorney, SBA
taormina law AG
T +41 44 455 66 60
taormina@taormina-law.ch

Andrea Taormina advises clients and represents them in court, specializing in criminal law and international mutual legal assistance in criminal matters.

Andrea Taormina holds a Doctorate in Law [Dr. iur.] from Freiburg University (Switzerland) and is admitted to the bar in the Canton of Zurich. In 2002, he was awarded an LL.M. degree from the University of Chicago Law School. From 2002 to 2004, Andrea Taormina worked in the U.S. Law Group at Allen & Overy in London. From 2004 to 2005 he worked at Homburger Rechtsanwälte in Zurich, after which he set up his own independent criminal law practice in Zurich. In addition, Andrea is a member of the Commission on Legal Fees of the Zurich Bar Association.

Turkey

Cerrahoğlu Law Firm

Onur Gülsaran

Yasemin Antakyalıoğlu Kastowski

Overview

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X Corporates cannot be criminally liable under Turkish law but may be liable under adminis-trative law.	X	X	X	X
No					

Question List

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

There is no specific Turkish legislation providing whistleblower protection. The position is governed by general employment law principles. As such, an employee cannot be dismissed on the grounds that they have reported misconduct or suspected misconduct. However, a dismissal of the employee with immediate effect may be justified if the employee discloses trade secrets to authorities or the public without having a genuine suspicion or knowledge of actual misconduct (e.g. where the employee's report is untruthful and/or vexatious). Under Turkish law, the company does not have a duty to investigate a whistleblower report, although it will generally be good practice to do so. At the end of an internal investigation, if any offense is detected, the company should report the offense to the prosecution authorities if it is ongoing at the time of the investigation (subject to the right to avoid self-incrimination under the Turkish Constitution).

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Many companies in Turkey have labor unions and an associated collective bargaining agreement between management and employees. An employee representative from the labor union has the right to be informed about and/or to participate in the investigation, if this was agreed in the collective bargaining agreement. In

the absence of such an agreement, the employee representative body has no automatic statutory right to be involved in an investigation.

b) There is no specific provision in the applicable Turkish Data Protection legislation giving the data protection officer or data privacy authority the right to be informed about and/or to participate in the investigation.

c) Where the relevant misconduct being investigated is also an offense regulated under the Turkish Criminal Code, this Code provides that the offense must be reported to the prosecution authorities, if it is ongoing at the time of the investigation. In general, even if the relevant misconduct is deemed an offense under Turkish Criminal Code, if the offense is not being committed at the time of the investigation, there is no reporting obligation. However, certain cases, such as money laundering offenses uncovered as a result of an internal investigation, should be reported to the relevant authority (see question 9 below).

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

In general, employees have the labor law duty to cooperate with an internal investigation as far as the facts to be investigated relate to activities conducted or matters known to them as part of their employment. They must answer work-related questions truthfully and completely. If the matters under investigation are unrelated to the employee's work or position in the company, a balancing of interests has to be performed to determine if a duty to cooperate exists.

Where an employee is required to participate, the employee's refusal may be regarded as a breach of duty and such misconduct may justify dismissal.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

The legal period under Turkish labor law for dismissal for cause is six working days following the date the employer becomes aware of the relevant misconduct giving rise to the dismissal. In case an investigation is carried out, this six working day period will in general not commence until the investigation is finalized and a report is provided to the relevant person/body within the company in charge of employee dismissals. If a claim for unfair dismissal is brought before the courts, the burden is on the employer to prove that the termination is justified.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

The Law of Protection of Personal Data (General Data Protection Regulation is not applicable in Turkey) which entered into force on 7 April 2016 applies to processing of data. This includes securing, collecting and reviewing data, as well as the creation of work products such as interview file notes and final reports. Therefore, it is very important to perform an early assessment of the applicable data privacy laws and to document the steps taken.

b) Reviewing emails?

Private communications are protected under Turkish law. Reviewing private emails of employees may even constitute a criminal offense if data privacy requirements are not observed. Provided that a general disclaimer is provided to the employee, stating that their business related communications (including work emails) could be monitored by the company at any time, the work emails of the employee can generally be reviewed. This disclaimer should be signed by all employees at the start of their employment contract.

c) Collecting (electronic) documents and/or other information?

As with emails, all other forms of documents containing personal data or private communications will be protected by Turkish law.

d) Analyzing accounting and/or other mere business databases?

There is no specific regulation in this respect, unless the relevant databases contain personal data, in which case the Law of Protection of Personal Data will apply.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no general statutory obligation that the employee to be interviewed should receive written instructions. Nevertheless, explanations are considered to be ethically required and advisable. In general, this includes a brief description on the background of the investigation and the subject matter. For documentation purposes, it is advisable to provide these instructions in written form to be countersigned by the interviewee.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no legal requirement to inform the employee in this regard.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no legal requirement to inform the employee in this regard. However, where the investigation may have a U.S. context, an Upjohn warning would be advisable.

d) Be informed that they have the right that their lawyer attends?

There is no legal requirement to inform the employee in this regard. However, should the employee request the presence of their lawyer, it is advisable to allow the lawyer to represent their client at the interview.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Where there is a labor union in the workplace and there is a provision to such purpose in the collective bargaining agreement, then the employee representative would have the right to be informed about and/or to participate in the interview.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The employee should be informed and their explicit consent should be requested before their data is transferred outside Turkey. Under Turkish data privacy law, transfer of data to a foreign country is permissible if explicit consent for such transfer is given.

g) Sign a data privacy waiver?

According to Turkish data privacy legislation, the employee needs to consent to the company's use of their personal data. Where the personal data of the interviewee might be used for other purposes in the future, (such as in possible court proceedings), a data privacy waiver signed by the interviewee can be very helpful.

h) Be informed that the information gathered might be passed on to authorities?

Although there is no legal obligation in Turkey in this regard, this should be included in the interview instructions as a matter of good practice.

i) Be informed that written notes will be taken?

For reasons of transparency, the fact that the information provided in the interview will be recorded (e.g. for reports and potentially for disclosure) should be explained. It is also advisable to have a copy of the written notes signed by the relevant employee and maintained in the investigation records. However, there is no such legal obligation under Turkish law.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law requiring that a document retention notice should be issued, but issuing such notices is advisable. Such notices should be clear, be sent to all potentially relevant addressees and be issued as early as possible. Before issuing the document retention notice, the company should consider which employee's documents should be retained and what types of documents should be sought (e.g. physical documentation, emails, documents contained on hard-drives and mobile devices). The document retention notice should briefly describe the terms of reference of the investigation, bearing in mind the need to maintain confidentiality.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege exists under Turkish law, although there are no specific rules in relation to its application in internal investigations. The documents relating to the findings of an internal investigation may be subject to attorney-client privilege protection if they have been prepared by an independent attorney and to the extent they concern the client's defense rights. Accordingly, to protect and render such documents out of the scope of the public investigation, it is recommended to mark these documents as "Confidential, Privileged, Attorney-client Privileged" and "Relating to Defense Rights".

Prosecutors may search company offices, although they will need a warrant to do so and the search must be done in the presence of a public prosecutor. It is recommended to have a lawyer present at the company offices during a raid. During such a raid, it is important to object to the seizure of any privileged documents and to ensure that this objection is documented in the minutes of the raid. Such objections will be considered by the public prosecutor or relevant judge when assessing the claim for privilege. Where the claim for privilege is successful, the public prosecutor or judge shall return these documents to the company.

Prosecutors may also search an attorney's office, but will need a court warrant to do so, and the search must be done in the presence of a public prosecutor. In case of a raid at an attorney's office, the attorney and/or the bar representative present at the raid may claim during the raid that a document, which is about to be confiscated, is related to the client's defense rights. In this case, the document is put in a separate envelope and the envelope's flap is sealed. The evaluation of attorney-client privilege status of the document is done by the magistrate in cases of criminal investigation, and by the criminal judge in cases of prosecution, in each case within 24 hours. If it is decided that the document falls under the scope of attorney-client privilege, it is immediately returned to the attorney and the correspondence relating to the document is destroyed. Therefore, in order to ensure privilege protection, it is advisable to keep the important documents relating to an internal investigation at the office of an outside counsel rather than on company premises, and to write "Confidential/Attorney-client correspondence" and "Relating to Defense Rights" on them.

Under the Criminal Procedure Code, upon a judge's warrant, a public prosecutor may seize computers and/or computer files. It is important to obtain a copy of the seized computer files and raise written objections with respect to potentially privileged documents during the raid. A claim for privilege may also be raised following the raid, but, where possible, it is advisable to object during the seizure proceedings, since these objections may be taken into account during the search of the copies of computer files by the relevant authorities.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Attorney-client privilege does not apply to in-house counsel. A recent decision of the Turkish Competition Board held that correspondence with an independent attorney will fall within the scope of attorney-client privilege. The decision implied that, as in-house counsel are employed by the company, they are not considered independent attorneys.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

As far as circumstances arise which could give rise to a claim under an insurance policy, (for example, under a D&O policy in relation to conduct of company directors), the company should make a notification of circumstances to the insurer. Each individual policy should be reviewed to ensure notification requirements are met.

b) To business partners (e.g. banks and creditors)?

Duties to inform business partners may arise from contractual obligations between the company and the business partner, particularly where the matter under investigation may have implications for the business partner. Even if there is no explicit provision in the relevant contract, there may be an obligation to notify a business partner of an internal investigation, where that information is highly significant to the business partner and relevant to its contract with the company. The interests of the business partner need to be evaluated against the legitimate interests of the company. Therefore, it depends on the individual case whether and when the business partner needs to be notified.

c) To shareholders?

Potential reporting duties towards shareholders compete with the company's requirements to maintain business confidentiality. Such reporting duty would play an essential role in companies, since certain investigations may require a mandatory disclosure under law (for example, companies listed on the BORSA Istanbul stock exchange will be required to disclose an investigation if it is deemed a material event). In addition to statutory disclosure obligations, the company has to evaluate on a case by case basis if there is an *ad hoc* duty to report to the shareholders. If the internal investigation affects the market price significantly and fulfills certain criteria (e.g. relating to the risk, scope, and suspects involved in the internal investigation) an obligation to disclose exits.

d) To authorities?

In general, there is no duty to inform the prosecutor about an internal investigation or potential misconduct within the company. However, there are exceptions where certain types of serious misconduct are uncovered during an investigation. For example, under the Regulation on Suspension of Transactions within the scope of Laundering Proceeds of Crime and Financing of Terrorism, certain companies (e.g. financial and insurance institutions, lawyers, and accountants) are required to notify the Turkish Financial Crimes Investigation Board if a serious indication exists which shows that a suspicious transaction has been performed or attempted. Even where no statutory duty to report exists, a cooperative approach with the local prosecutor may prevent adverse and unexpected measures by the authorities.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

The company has to minimize damages, stop any ongoing misconduct and try to prevent new cases of misconduct. Additionally, the company may have to reevaluate its compliance system, especially its compliance policies (such as its Code of Conduct) and the related training provided to the employees, in order to eliminate potential deficits and to improve its existing system. Further, the company may impose sanctions on the concerned employees including termination, in order to show that misconduct is not tolerated inside the company. Depending on the individual investigation and the industry sector concerned, notification to certain regulators may be advisable for strategic, risk management reasons.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Internal investigations are not very common in Turkey and usually Turkish subsidiaries of global companies conduct such investigations. As of today, the findings of such investigations are reported to the authorities in rare cases. Therefore the case law on the matter is very limited. However, where criminal misconduct is found in an internal investigation, a detailed internal investigation report of such misconduct would be helpful to the prosecution office (although there are no provisions under Turkish law relating to self-disclosure by the company to the prosecutors).

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

A search of company premises can be carried with a judge's warrant, or by the prosecutor's warrant in urgent cases. The search warrant should detail the suspected criminal act to which the search relates, the person(s) to be searched, the address, the property to be searched and the duration of the warrant. In principle, the prosecutor should be present during the search. However, where this is not possible, the search can be made in the presence of two aldermen or neighbors. "Aldermen" are elected government officials who act as neighborhood representatives, and a "neighbor" is someone who lives in the same neighborhood and who agrees to be a witness during a search.

In case of non-compliance with the rules on search warrants, the evidence gathered in the search cannot be used in court proceedings. Furthermore, anybody whose rights are violated by a non-compliant search can claim pecuniary and non-pecuniary damages.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

In principle, deals and non-prosecution or deferred prosecution agreements are not available under Turkish law except the following:

With the amendment made to the Criminal Procedural Law on 23 October 2019, a system called "serial procedure" has been adopted for certain offenses to be effective commencing from 1 January 2020.

The types of offenses to which this system will be applied are explicitly enumerated in the law. In summary, this system can be applied for light crimes and for crimes the proof of which require high technical nature such as fraud in money, endangering traffic safety, deliberate jeopardy of general security, false declarations in the issuance of official documents and seal breaking.

The basic rule of the serial procedure is that the public prosecutor agrees with the suspect, who accepts the fact that they have committed the act. The public prosecutor then, without indictment, conducts a detailed trial activity, and imposes half of the amount of the punishment prescribed in the law for the offense considered to have been committed by the suspect. Instead of the indictment, the report prepared by the public prosecutor containing the prescribed provision shall be forwarded to the relevant court and shall be issued as a verdict in case the defendant declares the acceptance before the Court with the presence of their lawyer.

This system, which is a kind of agreement, has been introduced with the aim of a quick conclusion of the proceedings in respect of certain crimes. If the proposal is not accepted by the suspect, the investigation and prosecution will be carried out according to the general principles of trial.

In addition, prosecutors have discretionary powers whether to commence criminal action under certain circumstances. For criminal acts which require filing of a complaint and are punishable by maximum one year of imprisonment, if the defendant has no criminal past, the prosecutor can defer the criminal case for five years. If the suspect does not commit any crime during this five-year period, the prosecutor may decide not to commence any criminal proceedings.

Since criminal liability does not attach to companies, the deferment of prosecution would only be applicable for the company's related directors, officers, or employees.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Corporations are not subject to criminal responsibility under Turkish law. However they can be subject to sanctions such as administrative fines, cancellation of business, and permits or expropriation (i.e.taking possession of assets). This will depend on the type of the misconduct committed by their directors or officers.

Individuals who have supervisory duties may face sanctions not only for their own misconduct but also in relation to misconduct of other employees under their supervision. These may include imprisonment, fines, or official debarment from their profession.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

If companies (i) have an effective internal investigation mechanism in place, (ii) report the evidence obtained as a result of their investigations and the actions considered to constitute a crime to the public prosecutor's office in due time, (iii) have taken the necessary prevention measures, and/or (iv) take further measures based on the nature of the action, this shall be taken into account by the relevant judge and can be used as a defense argument.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Since internal investigations are not common and not widely conducted in the country, precedents are very rare. As a result of the accession talks between Turkey and the European Union, there is a tendency for local corporations to follow the practices in Europe. Although the process for new legislation is slow, as long as the accession talks continue as planned, the legal environment in this regard would most probably evolve accordingly.

CONTACTS

CERRAHOĞLU
AVUKATLIK BÜROSU / LAW FIRM

Barbaros Bulvarı, Mustafa İzzet Efendi Sokak
No:11 Cerrahoğlu Binası Balmumcu - Beşiktaş
34349 İstanbul
Turkey

Tel.: +90 212 355 30 00
Fax: +90 212 266 39 00
www.cerrahoglu.av.tr

Onur Gülsaran
Partner
Cerrahoglu Law Firm
T +90 212 355 30 00
onur.gulsaran@cerrahoglu.av.tr

Onur Gülsaran qualified as a Partner in 2008 and is a member of the Corporate Law Department.

He provides consultancy services regarding corporate issues (i.e. incorporation, general assemblies, board meetings), anti-corruption, lease, franchise, loan and asset purchase.

He speaks English and Turkish and currently holds membership in Istanbul Bar Association since 1996.

Yasemin Antakyalıoğlu Kastowski
Founder
Antakyalıoğlu Law Office
T +90 212 355 30 00
yasemin@antakyalıoglu.com

Yasemin Antakyalıoğlu Kastowski is the founder of Antakyalıoğlu Law Office in Istanbul.

She especially focuses on criminal law and compliance issues. Ms. Antakyalıoğlu Kastowski has an extensive knowledge in all range of white collar crimes and compliance investigations. She advises, represents and defends her national and international clients in every step of criminal investigations and cases such as fraud, tax fraud, custom fraud, misappropriation, forgery of documents, fraudulent bankruptcy, and defamation. She also advices and assists other prestigious law offices in criminal law matters. Before establishing her own office, she worked with a well-known criminal law Professor in Istanbul and as a senior associate in the criminal law department of an international law firm based in Istanbul.

She speaks English, German, and Turkish and currently holds membership in Istanbul Bar Association since 2006.

Ukraine

Sayenko Kharenko

Ario Dehghani Yuliia Brusko

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	
No					X

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

There are no specific rules on whistleblower reports. Companies falling in the scope of the Anti-Corruption Law must have an anti-corruption program (the "**Model Anti-Corruption Program**") in place. The respective anti-corruption authority published a template for such a program. According to this template, such programs must also include processes on the performance of internal investigations, including, e.g., responsibilities, the timing of the investigation, internal and external reporting obligations, documentation, retention periods, and retaliation measures.

As a general rule, where the internal investigation relates to potential criminal conduct, all companies are obliged to notify law enforcement authorities about "serious" and "particularly serious" crimes. A failure to notify the same is a crime.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Trade unions established within individual companies (so-called "primary trade union organizations") will only have the right to be informed about and/or participate in, an internal investigation when the investigation relates to accidents and/or occupational diseases of employees who are members of the respective trade union (i.e. a disease that occurs as a result of work or occupational activity). Violation of this right can result in a small fine.

b) Companies have the obligation to notify the data protection authority in Ukraine (the Ukrainian Parliament Commissioner for Human Rights) about the processing of sensitive personal data, not related to

employment issues, within 30 days after the start of processing. This obligation also applies to internal investigations where such data is being processed.

Non-compliance with this obligation can lead to an administrative fine of up to UAH 6,800 (approximately €206) for each violation and up to UAH 34,000 (approx. €1,030) for repeated violations.

There are no obligations to notify the data protection officer(s) of the investigated company.

c) Where the company is public (as described in question 1), upon becoming aware of any corruption incident or after receiving information about a possible corruption incident, the heads of the public body and its departments must take measures to stop the violation and immediately inform the responsible anti-corruption state authorities.

Financial institutions (e.g. banks and insurance companies), stock exchanges and other companies conducting financial monitoring have to notify the State Financial Monitoring Service of Ukraine and the respective law enforcement authorities within a day when a financial transaction conducted or monitored by them is, or may be, related to a crime.

Private companies are not obliged to notify law enforcement authorities or involve them in internal investigations.

However, the company must notify the law enforcement authorities about the results of the investigation if a corruption offense was determined. Besides, Ukrainian law foresees a notification obligation for individuals and potential criminal liability in cases where an individual becomes aware of conduct pertaining to certain serious and/or particularly serious crimes.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

There is no explicit obligation under Ukrainian law for employees to support an internal investigation. However, the employee is obliged to fulfill any lawful order of the employer. This can also include an order to support an internal investigation. Not supporting the investigation may trigger disciplinary penalties, including dismissal.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

There are no labor law deadlines triggered or any rights to sanction employees waived by investigative actions. However, disciplinary actions against an employee under labor law can only be conducted within six months after the violation took place. This time limit only affects labor law actions against the employee.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

The provisions relating to personal data are contained in the law "On Personal Data Protection". Currently, Ukrainian lawmakers are working on an update of this law, which will reflect standards of the EU General Data Protection Regulation 2016/679.

Personal data includes all information which can be used to identify an individual. If a company or its representatives collect personal data of individuals during an internal investigation, the company is obliged to inform the respective data subjects about the purposes of the collection, the respective processing actions (e.g. transfer, retention, and use of the data), the persons involved in the processing actions, the data subject's rights and potential transfers of the data to foreign countries.

We suggest obtaining a waiver of data protection rights from the interviewee beforehand and/or asking to sign a commonly used privacy notice.

Ukrainian law prohibits the transfer of personal data from Ukraine to outside Ukraine, if the relevant country does not have an adequate level of data protection compared to Ukrainian law. Under Ukrainian law, "safe" countries to transfer data to are, in particular,

- Member States of the European Economic Area;
- Signatories of the ETS No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; and
- Countries with a data protection regime approved by the Government of Ukraine (no such approval published yet).

Ukrainian law further prohibits the provision of data or information relating to (i) state secrets or bank secrets, (ii) falling under a professional confidentiality obligation (e.g. doctor-patient, attorney-client), and (iii) specifically labelled as confidential information by the owning company. During an internal investigation, interviewees with access to such information are prohibited to disclose it. Ukrainian law only allows the release of such information when it is officially requested by public authorities. We suggest assessing beforehand if the information requested from the interviewee can fall into one of the above categories.

We suggest anonymizing the collected personal data as far as possible to avoid any potential violation of Ukrainian Data Protection law and not to burden the investigating company with unnecessary notification obligations.

b) Reviewing emails?

Reviewing private emails without a court ruling can constitute a violation of the constitutional right for secrecy of correspondence and can be a criminal offense.

The potential obligations for the investigating company in relation to data privacy, state secrecy and confidentiality outlined above at question 5a also apply in relation to the collection and review and other use of emails of employees and/or third parties. The investigating company would have the obligation to inform each data subject about the processing actions and the purpose, as well as about safeguarding actions undertaken (e.g. in cases of data transfer abroad).

In this regard, we also suggest anonymizing the collected personal data as far as possible.

c) Collecting (electronic) documents and/or other information?

The potential obligations for the investigating company in relation to data privacy, state secrecy and confidentiality outlined above at question 5a also apply in relation to the collection and use of other documents and information. In this regard, we also suggest anonymizing the collected personal data as far as possible.

d) Analyzing accounting and/or other mere business databases?

Accounting or business databases may contain personal data or information constituting state secrets or bank secrets. In such cases, the restrictions and obligations as outlined above in question 5 a) would also apply here.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no obligation for a company to provide any instructions to its employees before interviewing them as part of an internal investigation.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

The right not to incriminate oneself is a constitutional right. An employee can assert it during any internal investigations.

There is no obligation of the employer to inform interviewed employees about this right.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no such concept in Ukrainian law and no obligations in this regard.

d) Be informed that they have the right that their lawyer attends?

There is no such obligation for the employer. Such an obligation only applies to public criminal proceedings, and not interviews conducted as part of an internal investigation. However, the employee at their sole discretion has a right to take a lawyer to the interview.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is no general obligation for the employer to notify the interviewed employees about such right. Further, such right only exists where the investigation relates to accidents and/or occupational professional diseases of employees, who are members of the respective trade union.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Yes. When transferring personal data outside of Ukraine, the employee must give a prior general consent to the transfer and the receiving country must have an appropriate level of data protection (for countries with an appropriate level of data protection, see question 5a above).

When the receiving country does not have the appropriate level of protection (e.g. the United States), the employer can only transfer personal data to such country if one of the following exceptions is met:

- They have received additional explicit consent from the data subject for the transfer; or
- To protect the public interest or perform legal requirements.

The law requires the employer to inform its employees that their personal data has been passed to third parties within 10 days after the transfer. This can be done by the prior signing of a privacy notice. Notification is not required when such transfer is required by investigating authorities, or if the employee signed a waiver of notice.

g) Sign a data privacy waiver?

Ukrainian law does not require employees to waive their data privacy rights before conducting employee interviews. However, the employer can ask the employee to sign such waiver on a voluntary basis.

h) Be informed that the information gathered might be passed on to authorities?

Yes. The law requires the employer to inform its employees that their personal data has been passed to third parties within 10 days after the transfer.

i) Be informed that written notes will be taken?

Ukrainian law does not provide for such an obligation.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Yes. Although it is currently not common practice in Ukraine, we recommend to always use document-retention notices in connection with internal investigations and to include an adequately long period of retention. Such an approach can be very helpful in case of later investigations conducted by law enforcement authorities (e.g. the prosecutor department).

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege can be claimed in Ukraine and has no time limitation. However, attorney-client privilege covers only attorneys who have a special attorney license and are independent.

Attorney-client privilege covers client information, substantive advice, consultations, clarifications, documents drafted by the attorney, and other documents and information received from the client as part of the provision of legal advice. It also applies to the information provided by a person who consulted an attorney but did not become a client.

We suggest trying to include as many outside attorneys as possible when conducting an internal investigation to secure privilege, also with regard to foreign law regimes (e.g. the United States or the European Union).

In practice, Ukrainian public authorities occasionally still infringe attorney-client privilege. However, there are court proceedings which can help to protect the privilege rights.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Attorney-client privilege in Ukraine covers only attorneys who have a special attorney license and are independent. Most lawyers practicing in Ukraine, including in-house counsel, do not have such a license. In-house counsel (i.e. those in possession of an attorney license) can act as attorneys for their employers on the basis of a legal assistance agreement.

However, an in-house counsel may not be seen as independent as necessary to obtain attorney-client privilege. Therefore, attorney-client privilege may not apply to in-house counsel. Future case law will show if the formal requirements will be sufficient to obtain a solid attorney-client privilege.

Nevertheless, it is generally advisable to try to include as many outside attorneys as possible when conducting an internal investigation to secure the privilege rights, also concerning foreign law regimes (e.g. the United States or the European Union).

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

D&O insurance is generally not offered by Ukrainian insurance companies. For other types of insurance (e.g. professional indemnity insurance, third-party insurance, product liability insurance), notification obligations are set by individual insurance contracts.

b) To business partners (e.g. banks and creditors)?

Relations between business partners are usually regulated by contract. Notification obligations may be set out in such contracts.

c) To shareholders?

The law does not specify an express obligation to inform shareholders when starting an internal investigation.

However, under Ukrainian law, the director is generally obliged to act in the interests of the company, in good faith and reasonably. This obligation can also include an upfront notification of shareholders before launching an internal investigation. Such an obligation should be assessed on a case-by-case basis.

There is an additional obligation for the director to provide information about the company's activity, also including an internal investigation, at the shareholder's explicit request.

The Model Anti-Corruption Program establishes an obligation to notify shareholders if a corruption violation has occurred or is suspected. Although this obligation is only obligatory for companies that participate in a public procurement procedure for projects exceeding UAH 20 million, and only during the specific tender procedure, state authorities recommend that other companies also should use such approach.

Corporate governance rules in this regard are not well-developed on a legislative level, although usually companies develop detailed internal regulations. An obligation to notify the shareholders might, therefore, also be based on the individual charter or policy of the respective company.

d) To authorities?

The Anti-Corruption Law and Model Anti-Corruption Program provides an obligation for the authorized representatives of the company (e.g., the CEO) to notify the respective public authorities about an administrative or criminal corruption offense known and discovered within an internal investigation. The Anti-Corruption Program is obligatory for companies participating in a public procurement procedure for projects exceeding UAH 20 million (currently, approx. €606,060) and only with regard to the specific tender procedure. However, state authorities recommend that other companies also should adopt this approach.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

Private companies have no obligation to take immediate measures with regard to an internal investigation. However, as a matter of practice, the company should try to stop any ongoing misconduct and consider remediation measures.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

There are no concerns or specific steps required by prosecutors regarding internal investigations.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Searches can be conducted only within the scope of an open criminal investigation. They are based on the mandatory ruling of the investigating judge. The initiators can be a prosecutor, or an investigator together with a prosecutor.

The court ruling must be provided to the company. The scope of the search must be within its outlined purpose. When the search is at a company's premises, the search record is provided to the representative of the company.

Dawn raids without the prior approval of the investigating judge can be conducted by the investigator in exceptional cases, such as to save people's lives or when chasing a suspect. Even in this case, the dawn raid must be authorized by the investigating judge retrospectively. If the dawn raid is not subsequently authorized, its results are considered invalid and inadmissible.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Ukrainian law does not provide for deferred prosecution agreements or non-prosecution agreements. However, in criminal proceedings there is the possibility to conclude:

- A settlement agreement between the victim and the accused of minor crimes, crimes deemed to be of average weight and in criminal proceedings in the form of a private prosecution; and
- A plea agreement between the prosecutor and the accused for:
  - Minor crimes, crimes with average weight, and serious crimes; and
  - Particularly serious crimes investigated by the National Anti-Corruption Bureau (in relation to corruption-related offenses by public officials), when the accused reveals other suspects committing a similar crime which can be substantiated by evidence; and
  - Particularly serious crimes committed by conspiracy by a group of individuals, an organized group or criminal organization or terrorist group, provided that (i) they are exposed by a suspect who is not the head

of such group or organization, and (ii) the suspect reveals the criminal acts of other members of the group or other crimes committed by the group or organization and supports these by evidence.

Criminal liability (currently, in the form of penalty fines of up to UAH 1,275,000 (currently, approx. €38,636), confiscation of property and compulsory liquidation of the entity) can also apply to companies. In such cases, a settlement agreement or a plea agreement cannot be concluded.

A plea agreement requires the prior consent of the person whose private interests have been damaged. The agreement has to be approved by the competent court. Such agreements are common in Ukraine.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Under Ukrainian law, directors can face liability for: (i) tax evasion (fines up to UAH 425,000 (currently, approx. €12,878), and loss of the right to hold specific posts for up to three years and confiscation of assets), (ii) forgery of documents submitted for state registration of a legal entity (fine up to UAH 34,000 (currently, approx. €1,030) or custodial restraint for five years and loss of the right to hold specific posts for up to three years), (iii) contentious insolvency (fine up to UAH 51,000 (currently, approx. €1,545) and loss of the right to hold specific posts for up to three years), and (iv) violation of labor law.

Furthermore, directors can face liability claims from shareholders based on improper management which causes damage to the company. This is based on the director's obligation to act in the best interests of the company.

Criminal liability for the company can be based on the misconduct of the employee (or its authorized agent) benefitting the company. These offenses may include, for example:

- Bribery of public officials or private companies;
- Money laundering; or
- Financing of terrorism.

Criminal liability measures for private companies include a fine of up to UAH 1,275,000 (approx. €38,636), confiscation of property or compulsory liquidation of the entity. The private company also has to compensate all losses, and, in case of a corruption offense, the amount of illegal benefit received or which could have been received as a result of the offense.

Public bodies, public entities financed from state or local budgets, or by international organizations are as legal persons exempted from certain criminal liabilities. However, their public officials and executives can, as individuals, be penalized for committing corruption offenses, including potential imprisonment of up to 12 years.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

Yes, according to Ukrainian legislation, the existence of an implemented compliance system (in other words, measures taken by the company to prevent a crime) may reduce potential penalties. However, Ukraine has no strong case law or administrative guidelines for courts on how to take an existing compliance system into account. Therefore, a previously existing compliance system may influence the court's decision, but this will rather depend on the specific judge.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Recently, the Ukrainian Parliament adopted an updated Anti-Money Laundering Law. The new law implements international legislative standards for anti-money laundering regimes. At the same time, the number of internal

investigations is further increasing. For example, alleged corruption offenses committed by the former executives of the Ukrainian state company "Ukroboronprom" are now the subject of an internal investigation. Finally, Ukrainian subsidiaries of global companies and Ukrainian individuals have, in recent years, become subjects of official FCPA investigations relating to allegedly illicit activities in Ukraine.

CONTACTS

10 Muzeyny Provulok
Kyiv 01001
Ukraine

Tel.: +38 044 499 60 00
www.sk.ua

Ario Dehghani
Counsel
Sayenko Kharenko
T +38 044 499 60 00
ADehghani@sk.ua

Ario Dehghani has over 10 years of professional experience in the fields of compliance, data protection and privacy, white collar investigations and EU law. Prior to joining Sayenko Kharenko, Ario worked for more than seven years at the Hogan Lovells' Munich office, where he focused on white collar, compliance and internal investigations.

Ario Dehghani is one of the most experienced experts in Ukraine in preventing, identifying, eliminating and mitigating compliance risks at both national and global levels. He advises clients on all types of compliance matters and regularly handles sophisticated internal investigations related to, amongst others, FCPA and UK Bribery Act issues. His areas of expertise cover anti-bribery, anti-corruption, anti-money laundering, sanctions, data protection, regulatory and product compliance matters. Ario is also adept at performing compliance due diligence, implementing and auditing internal compliance systems, conducting compliance investigations and delivering customized training for in-house compliance officers. He has extensive experience across a variety of sectors, including the chemical, life science, electronic, IT, automotive, consumer goods and energy sectors.

Ario provides courses on German private and public law and holds open lectures on Compliance and EU law topics.

Yuliia Brusko
Associate
Sayenko Kharenko
T +38 044 499 60 00
YBrusko@sk.ua

Yuliia has five years of professional experience in the fields of compliance, data protection and privacy, corporate, M&A and employment law. Yuliia advises Ukrainian and foreign clients from all kinds of industry sectors.

Yuliia's experience includes advising on a wide range of anti-bribery, sanctions, data protection and regulatory compliance issues under national and extraterritorial foreign regulations also applicable in Ukraine, including the FCPA, the UK Bribery Act and the GDPR. Her skills and expertise cover the management and conduct of internal compliance investigations, the establishment of complex compliance management and data protection systems and advising within several other spheres of regulatory and in-house compliance. Yuliia gained her internal investigation and compliance expertise by advising and supporting clients, especially from the sectors of agriculture, energy, pharmaceuticals, health care and consumer products. She obtained her skills in the field of data privacy mainly by advising and supporting clients from the IT industry and healthcare sector.

United Kingdom

Hogan Lovells International LLP


Liam Naidoo


Maggie Christiansen


Reuben Vandercruyssen


Nick Roper

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defense
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Do any specific procedures need to be considered in case a whistleblower report sets off an internal investigation (e.g. for whistleblower protection)?

An internal investigation being triggered by a whistleblower does not necessitate specific procedures. However, employee protections, such as ensuring that an employee or worker who makes a protected disclosure is not subject to any detriment, should be kept in mind.

An employee or worker can claim whistleblower protection if he complains about a criminal offense, a failure to comply with a legal obligation, a miscarriage of justice, health and safety risks, risk or damage to the environment, or a "cover up" of any of the above matters. The employee must have a reasonable belief that the disclosure is made in the public interest and it must be made to an appropriate person (e.g. a lawyer or specified regulator).

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What are the consequences in case of non-compliance?

a) Employee representative bodies are not entitled to be informed about or participate in an internal investigation. In the United Kingdom, there is no formal legal mechanism for ongoing employee representation akin to a works council.

b) The United Kingdom's data privacy authority is the Information Commissioner's Office ("**ICO**"). This is the relevant supervisory authority that must be contacted within 72 hours of certain breaches of personal data. The ICO does not need to be notified of an internal investigation, subject to compliance with data privacy regulations and there being no significant risks to the protection of personal data.

c) Local authorities do not have the right to be informed about and/or to participate in an investigation.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, may the company impose disciplinary measures if the employee refuses to cooperate?

Employees are under implied contractual obligations to follow the reasonable instructions of their employer and may also be under express obligations to cooperate with their employer and to disclose any wrongdoing. Therefore, employees could be required to participate in interviews and assist an investigation. Failure to do so could result in disciplinary action being taken against them.

---

4. Can any labor law deadlines be triggered or any rights to sanction employees be waived by investigative actions? How can this be avoided?

There is no specific timescale in which an employer must take action against an employee once an investigation has commenced. Failure to sanction an employee within a specific time will not waive the employer's rights. However, disciplinary action against an employee following an internal investigation should be commenced without undue delay. In relation to both disciplinary action and civil claims, consideration should be given to whether or not further cooperation from the employee may assist the investigation.

In relation to claims arising as a result of investigative actions, the usual limitation periods under UK law will apply.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Conducting interviews?

The provision of documents before an interview may give rise to data protection issues, particularly where multiple jurisdictions are involved and other individuals' personal data is present in documents or emails being provided. It is important that personal data is not disclosed to or by an interviewee.

b) Reviewing emails?

The review of emails as part of an investigation should comply with the safeguards set out in the UK Data Protection Act 2018 (the "**DPA**") and the General Data Protection Regulation (the "**GDPR**"). Employees' emails may typically be reviewed as part of the investigation, however, consideration should be given beforehand to which emails constitute personal emails and those should be excluded from the review (subject to agreements between the employee and the company, such as the company handbook). The collection of personal data must be kept to the minimum amount necessary, in accordance with the principle of data minimization.

If the investigation is required pursuant to a court order, employee consent is likely not required to review business emails. Individuals involved in an investigation have the right to copies of the data collected pertaining to them.

c) Collecting (electronic) documents and/or other information?

The collection of documents and/or other information is subject to the data protection laws and will apply to documents collected which contain personal information or data.

d) Analyzing accounting and/or other mere business databases?

Data protection laws will apply to the extent that the databases contain personal data. If the databases do not contain personal data, obligations under the DPA and the GDPR do not arise.

Many organizations have data protection agreements in place (also known as model clauses or a Binding Corporate Rules policy) which permit the flow of information within an organization. Specialist legal advice should be sought to inform whether such agreements are sufficient under the GDPR and the DPA.

---

6. Before conducting employee interviews in your country, must the interviewee

a) Receive written instructions?

There is no specific legal requirement for the employee to receive written instructions about the matters the interview will cover.

b) Be informed that they must not make statements that would mean any kind of self-incrimination?

There is no specific legal requirement to inform the employee that they have a right not to incriminate themselves as part of an internal investigation.

c) Be informed that the lawyer attending the interview is the lawyer for the company and not the lawyer for the interviewee (so-called "Upjohn warning")?

There is no specific legal requirement to deliver an "Upjohn warning" at the start of an internal investigation interview that does not have a U.S. context. In practice, such warnings should generally be given and are more frequently being utilized in UK interviews.

d) Be informed that they have the right that their lawyer attends?

There is no specific legal requirement that an employee should be informed that they have the right to be accompanied by a lawyer, although employees cannot be prevented from attending with their lawyer.

e) Be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

There is no specific legal requirement to allow an employee to be accompanied to an internal investigatory interview by a works council or other employee representative and it would be unusual for this to be permitted.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

Cross-border data transfers are a complex area and specific advice should be sought to ensure compliance with the GDPR. Compliance with the GDPR is still necessary in the transition period, and after the United Kingdom has left the European Union. While the EU version of the GDPR will no longer be law within the United Kingdom, it will be incorporated directly into UK law to sit alongside the Data Protection Act 2018, as the UK GDPR.

The U.S. data protection regime has been found to not meet the standards required by the European Commission. The U.S.-EU Privacy Shield framework, which was previously regarded as an adequate mechanism for transferring data from the UK to the U.S., was invalidated in July 2020 by the CJEU in the case of *Schrems II* (*Data Protection Commissioner vs. Facebook Ireland Limited, Maximillian Schrems* (Case C-311/1)). Following this case, the Privacy Shield framework can no longer be used as a valid mechanism for making international data transfers to the U.S., and instead, alternative data transfer mechanisms should be implemented to conduct these international data transfers. Standard contractual clauses may need to be put in place to make up for the lack of adequate standards, before exporting any data outside the European Economic Area. There may be derogations for specific situations, so legal advice must be sought.

When personal data is collected from the data subject, the data subject must be informed whether the data is being transferred to a non-European Economic Area country or international organization.

g) Sign a data privacy waiver?

The tightening of data protections under the GDPR will likely necessitate providing an employee with a privacy notice which explains, amongst other things, the legal basis for processing their personal data, the purpose for this processing, and any related rights in relation to their data which they may possess, such as a right to access, or rectify this information.

h) Be informed that the information gathered might be passed on to authorities?

There is no specific legal requirement to inform the employee that information might be passed on to authorities (unless the investigation has a U.S. context), but it would be good practice to do so.

i) Be informed that written notes will be taken?

There is no specific legal requirement to inform the employee that written notes will be taken, but it would be good practice to do so.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

A company should take immediate steps to preserve all relevant evidence. A document hold notice should be sent to relevant custodians identifying the categories of document that should be preserved.

It is important that all documents identified as potentially relevant are isolated and remain secure throughout the investigation.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The United Kingdom recognizes the concept of legal advice privilege between a lawyer and client, which broadly reflects and is comparable to that of attorney client privilege in the United States. Legal advice privilege may apply to confidential communications between a lawyer and their client for the purpose of giving or obtaining legal advice. Legal advice privilege extends to documents which evidence such communications, including relating to the findings of the investigation.

When assessing legal advice privilege, the "client" is only those employees and officers charged with obtaining legal advice. Communications involving employees not expressly tasked to seek advice, and all communications with third parties (such as forensic accountants) are not protected; even where communications are necessary to inform lawyers of relevant events or information. Note in particular, file notes of investigation interviews may not always attract legal advice privilege, even if taken by a lawyer.

A distinct category of legal advice privilege exists through litigation privilege. Litigation privilege can be claimed over any confidential communication between a client, lawyer and third party where the sole or dominant purpose of the communication is for use in actual, pending or contemplated litigation. Litigation privilege shall only apply if litigation is reasonably contemplated when the investigation begins, and communications or documents must be created for the dominant purpose of that litigation. Litigation privilege is therefore unlikely to apply to purely internal investigations, unless and until evidence is discovered which indicates potential criminality or civil liability. Actual wrong doing needn't be established for litigation privilege to apply.

---

9. Can attorney-client privilege also apply to in-house counsel in your country?

Generally, both legal advice privilege and litigation privilege apply equally to in-house and external counsel, save for competition investigations by the European Commission in which internal advice is not considered privileged.

Notably, communications may lose privileged status where in-house counsel communications contain both legal and business/commercial information. It is clear that to ensure the maintenance of privilege, communications for the purpose of obtaining legal advice should be kept entirely separate to those of a commercial or business nature.

---

10. Are any early notifications required when starting an investigation?

a) To insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

It is likely to be a condition of certain insurance policies that the insurer is notified of issues which have given rise to an internal investigation. Each individual policy should be reviewed.

b) To business partners (e.g. banks and creditors)?

It is unlikely to be a condition of agreements with business partners that they are notified of issues which have given rise to an internal investigation. However, relevant agreements should be checked, particularly if the matters under investigation could impact or involve the business partner.

c) To shareholders?

If the allegations are serious and could expose the company or directors to liability or reputational damage, the board of the company ought to be notified but not necessarily shareholders.

Companies whose securities are admitted to trading on a market operated by the London Stock Exchange are subject to ongoing disclosure obligations. Publicly listed companies must issue a market announcement (without delay) of any major new development that may lead to a substantial share price movement.

d) To authorities?

Advice should be taken before notifying any regulatory authority about an internal investigation, especially where there are concerns of money laundering or other criminal offenses.

Generally there is no positive obligation to report crime. The main exception relates to a suspicion of money laundering, where an obligation may arise if the person or company is in the 'regulated sector' (including, for example, Financial Conduct Authority ("**FCA**") regulated firms, solicitors and accountants). Companies or persons not within the regulated sector are under less onerous obligations, but nonetheless must report money laundering if concerns exist that they are involved in an arrangement involving criminal property, for example.

---

11. Are there certain other immediate measures that have to be taken in your country or would be expected by the authorities in your country once an investigation is started, e.g. any particular immediate reaction to the alleged conduct?

A company should, as a first step, preserve all documents and materials that may be relevant to any criminal investigation.

It is a criminal offense to destroy, falsify, conceal, or dispose of relevant documents when a person knows or suspects an investigation of serious or complex fraud is already being, or is likely to be, undertaken by the police or the Serious Fraud Office ("**SFO**"). If unlawful conduct has ceased and the company was aware or suspected that it possessed funds obtained from the conduct, but it failed to take any action in respect of those funds, the company could commit a money laundering offense.

If a company failed to take any steps to address an allegation of bribery, it is unlikely that they would be able to rely upon the 'adequate procedures' defense in the event of a prosecution of corporate failure to prevent bribery under the Bribery Act 2010.

---

12. Will local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Historically, United Kingdom authorities have not generally objected to internal investigations so long as they did not hinder a criminal investigation. However, a more formalized procedure appears to be emerging, especially following the Cooperation Guidance issued by the SFO in August 2019 (the "**Guidance**"). The Guidance sets out various factors to be adhered to by corporations hoping to receive a recommendation for a Deferred Prosecution Agreement ("**DPA**").

Expectations of the SFO in relation to privilege are one example. The Guidance states that corporations will not be penalized for choosing to not waive privilege for internal investigation documents or interviews, but will not receive the corresponding cooperation credit towards a DPA. Further, claims to privilege should now be independently verified by counsel to ascertain that legal professional privilege has been applied properly.

The Guidance further suggests consultations with the SFO prior to undertaking interviews – a tighter and more procedural requirement than before.

The Guidance also sets out indicators of 'good practice.' These are extensive and are not considered to be exhaustive. Advice should be sought prior to any investigation to understand these intricacies properly.

---

13. Please describe the legal prerequisites for search warrants or dawn raids on companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Authorities that investigate corporate crime in the United Kingdom may conduct dawn raids of business or residential premises under a search warrant issued by a court. When a raid is carried out under a warrant, the authority may use reasonable force to gain entry to the premises.

Legally privileged material cannot be seized unless it was created with the intention of the furtherance of a crime (the crime-fraud exception). If legally privileged material cannot be separated from non-privileged material, it can be seized but must first be reviewed for privilege by an independent lawyer.

The Competition and Markets Authority may conduct a dawn raid of business premises without a warrant where it reasonably suspects that a cartel offense has been committed.

If there are significant defects in the process of obtaining a warrant or authorizing or executing a raid, the raid can be challenged by judicial review in the courts. If it is rendered unlawful, the raid may be deemed a civil or criminal trespass. Any material seized during the raid could become inadmissible.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for corporations in your jurisdiction?

Non-prosecution agreements are not available in the United Kingdom. DPAs have been available in England, Wales and Northern Ireland since 2014 and must all be approved by the court. They are available to the Crown Prosecution Service and the SFO.

A prosecutor may invite a suspect into DPA negotiations where it determines that the full extent of the corporate offending has been identified and the public interest is served by a DPA.

A company will be formally charged with the criminal offense, but such proceedings will be suspended for a period defined by the terms of the DPA. If there is full compliance with the DPA, the criminal proceedings will be formally discontinued at the end of the period. Criminal proceedings will resume if the DPA is breached beyond remedy. At the time of writing, there have been seven approved SFO DPA agreements.

The Guidance notes that to secure favorable consideration, such as a DPA, a corporation must adopt a genuinely proactive approach to cooperation and may be required to have practices which go above and beyond what the law requires, such as waiving privilege (as previously outlined).

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) can companies or its directors, officers, or employees face for misconduct of (other) individuals of the company?

Penalties for individuals include imprisonment, fines, disgorgement, and compensation orders. Individuals can also be disqualified from being a director of a company for up to 15 years. Companies may be debarred from public tendering for up to five years.

Certain regulatory authorities can impose additional penalties. For example, the FCA can prohibit authorized firms from undertaking specific regulated activities for up to 12 months and impose fines on firms and individuals.

---

16. Can penalties for companies, its directors, officers, or employees be reduced or suspended in case the company implemented an efficient compliance system? Does this only apply in case the efficient compliance system had already been implemented prior to the alleged misconduct?

A corporation may benefit from a complete defense against s7 of the Bribery Act (for the strict liability offense of failing to prevent bribery) if it can be shown that it had 'adequate procedures' in place to prevent bribery. In practice, this requires a risk based review to be undertaken on a regular basis to ensure that processes are efficient and proportionate to the nature of the corporate function, areas and jurisdictions of operation, and the profile and size of the corporations.

If such risk based processes are maintained, 'adequate and sufficient' protocols will provide a complete defense to liability under s7.

This exemption is likely only to apply where controls and procedures are implemented prior to the alleged misconduct, although the Bribery Act doesn't provide specific guidance on this point.

Specialist legal advice should be sought in this area due to the complexity of factors necessary to be considered on an ongoing basis.

---

17. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The SFO has become increasingly involved in internal investigations and its director, Lisa Osofsky, envisions that the SFO will be able to engage in an open dialog with corporations who are considering or undertaking an internal investigation. The breadth of the Guidance may also offer a greater opportunity for DPAs to be recommended by the SFO.

In February 2020, the SFO imposed the most significant fine for a DPA against a company to date. The fine imposed against Airbus exceeds the combined sum of all previous UK DPAs.

The United Kingdom currently implements multilateral sanctions regimes through EU legislation. The UK parliament is currently considering how it can continue to impose, update, and lift sanctions and anti-money laundering regimes following Brexit.

Privilege is an area of law which is at present shrouded in a certain degree of uncertainty due to ongoing case law. Accordingly, legal advice should be sought as soon as an internal investigation is in contemplation and before written records of its findings are created to maximize the probability that privilege will apply.

The UK government is also consulting on the extension of corporate liability for economic crimes beyond bribery.

CONTACTS

Atlantic House
Holborn Viaduct
London EC1A 2FG
United Kingdom

Tel.: +44 20 7296 2000
Fax: +44 20 7296 2001
www.hoganlovells.com

Liam Naidoo

Partner
Hogan Lovells London
T +44 20 7296 2909
liam.naidoo@hoganlovells.com

Liam is a partner in Hogan Lovells' Investigations practice focusing on business crime, fraud, bribery and corruption, Liam's practice particularly focuses on the management of internal investigations following allegations of corrupt activity of employees, agents and other third parties. This experience allows him to give targeted advice to clients on anti-corruption compliance measures. In addition, Liam has significant experience in Commercial Court litigation arising out of complex fraud and bribery actions.

Maggie Christiansen

Senior Associate
Hogan Lovells London
T +44 20 7296 2909
maggie.christiansen@hoganlovells.com

As a senior associate in our London Litigation group, Maggie Christiansen has experience in a wide range of commercial disputes. She has acted on large-scale domestic cases in industries as diverse as banking, automotive, coach and rail, aviation and defense. She also acts on complex, multi-jurisdictional matters involving global Plcs. In addition, Maggie has extensive experience in bribery and corruption investigations and compliance implementation, having completed two six-month client secondments in this field.

Reuben Vandercruyssen

Associate
Hogan Lovells London
T +44 20 7296 2824
reuben.vandercruyssen@hoganlovells.com

Reuben is an associate in Hogan Lovells' Litigation Group and has wide-ranging experience of commercial disputes and internal investigations into allegations of unlawful or corrupt acts by employees, agents and third parties. Reuben advises large corporates on anti-corruption compliance and adequate policies and procedures, particularly in the context of mergers and acquisitions in high-risk jurisdictions.

Reuben has extensive experience of high-profile Part 8 proceedings, including a judicial review involving a London-based private hire vehicle operator, a privilege dispute concerning the disclosure of documents in the context of a criminal investigation and a dispute regarding the proper construction of the rules of a trust fund. Reuben has represented clients before the First-tier Tribunal.

Nick Roper

Associate
Hogan Lovells London
T +44 20 7296 7119
nick.roper@hoganlovells.com

Nick is an associate in the Corporate litigation, Fraud and Investigations group. Nick's experience includes advising BTA Bank in its long-running litigation and in relation to their international asset recovery strategy. In additional he has assisted in advising an American company in relation their international internal investigation into potential sanction breaches.

Nick has worked in house, on secondment, in the disputes resolution team at Standard Chartered Bank. He is active in the firm's pro bono initiatives and successfully represented a client in their Employment Support Allowance appeal before the First-Tier Tribunal.

DISCLAMER

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney Advertising.