Microsoft

Compliance in the Cloud: Demystifying the Legal Landscape

November 2019

Introduction

This paper intends to provide you with an overview of the legal environment and applicable privacy and data protection laws relating to cloud services and explains Microsoft's approach to ensuring that its Enterprise Cloud Services comply with the applicable requirements. It particularly contains information about the following topics and questions:

I. Microsoft's Compliance with Relevant Data Protection Laws

1. To what extent is data protection law relevant for customers of Microsoft Enterprise Cloud Services?
2. What is the EU General Data Protection Regulation and what has changed with regard to data protection as a result of this Regulation?
3. Which rules apply with regard to data processing on behalf of private companies and how does Microsoft comply with these rules?
4. On what legal basis does Microsoft process personal data in its Enterprise Cloud Services?
5. What are Standard Contractual Clauses and does Microsoft make use of them?
6. Have Microsoft's Enterprise Cloud agreements been approved by the data protection authorities?
7. What other regulatory requirements can be applicable in addition to the data protection law?

II. Contractual Relationships

8. What are the contractual relationships if the Enterprise Cloud Services are used by different group companies of the customer?
9. What is the content of the contractual relationships when enterprises, particularly Microsoft Partner, use a Microsoft platform such as Microsoft Azure and offer the services to their customers based on such platform?

III. Data Transfers to the US

10. Which measures does Microsoft take to safeguard data transfers to the US?

11. Does Microsoft disclose customer data to US authorities, such as the National Security Agency (NSA)?
12. What is the new American CLOUD Act and why was it adopted?
13. What is the relevance of the new American CLOUD Act?
14. What are the consequences of the new American CLOUD Act for Microsoft?
15. How many requests does Microsoft receive from investigating authorities?

IV. Microsoft's Approach to Secure and Protect Data

16. Where is data stored in the Microsoft Enterprise Cloud?
17. Can Microsoft Enterprise Cloud Services be used by persons subject to professional secrecy?
18. How does Microsoft deal with encryption?
19. Can the application of data protection law be excluded by encryption?
20. How can customers fulfill their obligation to assess the compliance with all agreed technical and organizational measures?
21. How can customers store data securely for revisions?

I. Microsoft's Compliance with Relevant Data Protection Laws

In connection with providing the Cloud Services, Microsoft complies with all applicable data protection laws. This section explains the relevant data protection laws that are applicable to Microsoft and how Microsoft complies with them.

1. To what extent is data protection law relevant for customers of Microsoft Enterprise Cloud Services?

Customers may only process personal data in the Cloud if there is a legal basis. Regarding Cloud Services, such legal basis is usually found in the so called "data processing" which Microsoft reflects in its agreements.

Data protection law only applies to the processing of personal data. In short, "personal data" are all information relating to an identified or identifiable natural person, such as the name of a natural person or his or her e-mail address. In practice, a lot of personal data can usually be found in the Microsoft Enterprise Cloud. However, there are also cases where only less or only personal data with low sensitivity are being processed, e.g. when patterns of a fashion designer are being stored in Azure.

2. What is the EU General Data Protection Regulation and what has changed with regard to data protection as a result of this regulation?

The EU General Data Protection Regulation (hereinafter, GDPR) became applicable from 25 May 2018. It repeals the 1995 Data Protection Directive 95/46/EC, which had to be considered by the EU member states in their respective local data protection laws before the GDPR became effective.

In contrast to the Data Protection Directive, the GDPR is a regulation that does not require a transposition into local law by the member states' national parliaments. Rather, the GDPR applies directly in all EU member states without implementing acts. The GDPR allows member states to create national data protection legislation in certain areas on the basis of so-called opening clauses. These national regulations modify the GDPR provisions. The national regulations do deviate from each other in certain respects so that, although the GDPR harmonized the data protection laws within the EU on a large scale, there are still some differences on data protection laws within the member states, particularly with regard to the areas where the GDPR provides such opening clauses. For instance, the German legislator has created national provisions, inter alia, in the field of employee data protection or video surveillance in the new Federal Data Protection Act (BDSG).

3. Which rules apply with regard to data processing on behalf of private companies and how does Microsoft comply with these rules?

Data processing on behalf of private companies is conclusively regulated in Art. 28 GDPR, without the national data protection legislation modifying this provision.

Therefore, Art. 28 GDPR is the relevant provision in the case of so-called commissioned data processing. Microsoft offers its customers the Online Services Terms (hereafter, "OST", current version available here), with an Attachment 4 (European Union General Data Protection Regulation Terms) the terms that have to be agreed upon according to Art. 28 GDPR. This ensures that Microsoft Enterprise Services can be used in compliance with the GDPR.

4. On what legal basis does Microsoft process personal data in its Enterprise Cloud Services?

Microsoft processes personal data in its Enterprise Cloud Services in order to perform the contractual obligations as agreed in the license agreements for the use of the respective Microsoft Technology. If processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, the contract, serves as a legal basis.

Therefore, the license agreements for the use of the respective Microsoft Technology form the legal basis for the use of the services and the processing of personal data in this respect. In Europe, these license agreements are concluded between the customer and Microsoft Ireland Operations Limited (hereinafter, "MIOL").

The license agreements are supplemented by the OST. In the section "Data Protection Terms". These terms contain - among other things - the mandatory legal requirements for a data processing pursuant to Art. 28 GDPR.

5. What are Standard Contractual Clauses and does Microsoft make use of them?

Furthermore, Microsoft processes personal data in its Enterprise Cloud Services in accordance with the EU Commission's Standard Contractual Clauses (hereafter, "SCC") which are contained in Attachment 3 to the OST. The SCC are concluded between the customer and Microsoft Corporation as sub-contractor of MIOL.

The SCC are standard sets of contractual terms and conditions issued by the EU Commission which both the sender and the receiver of personal data, need to sign up to, to protect personal data transferred from the European Economic Area (EEA) to territories which are not considered to offer adequate protection to the rights and freedoms of data subjects (usually non-EU countries). The SCC have been approved by the EU Commission to offer sufficient safeguards on

data protection for those data transfers. Therefore, they serve as appropriate safeguards for international data transfers under Article 46 of the GDPR, which permit the respective international transfer of personal data, provided that the SCC are implemented unchanged.

As Microsoft incorporates the SCC in its OST, Microsoft is obligated to comply with the SCC standards and has also to impose these standards on any sub-contractor in its sub-contractor agreements.

6. Have Microsoft's Enterprise Cloud agreements been approved by the data protection authorities?

Yes. The European Data Protection Board – a consultative committee of all 28 national data protection authorities of the EU member states (formerly called Article 29 Working Party) – has confirmed to Microsoft by letter of 2 April 2014 that the Microsoft-Agreement, submitted by Microsoft is a proper implementation of the SCC and therefore creates an adequate level of data protection at recipients of personal data outside the EU (Ref. Ares(2014)1033670 - 02/04/2014). It found that the Microsoft-Agreement contains all requirements which are necessary for engaging service providers outside the EU by way of binding instructions.

For enterprises in most European countries, this means that the use of Enterprise Cloud Services does not need to be approved by the supervisory authorities. The supervisory authorities are only entitled to assess on a case by case basis whether the data processing itself is permissible. The supervisory authorities are only entitled to assess on a case by case basis whether the data processing itself is permissible (i.e., as they would be if customer would use its own data center).

7. What other regulatory requirements can be applicable in addition to the data protection law?

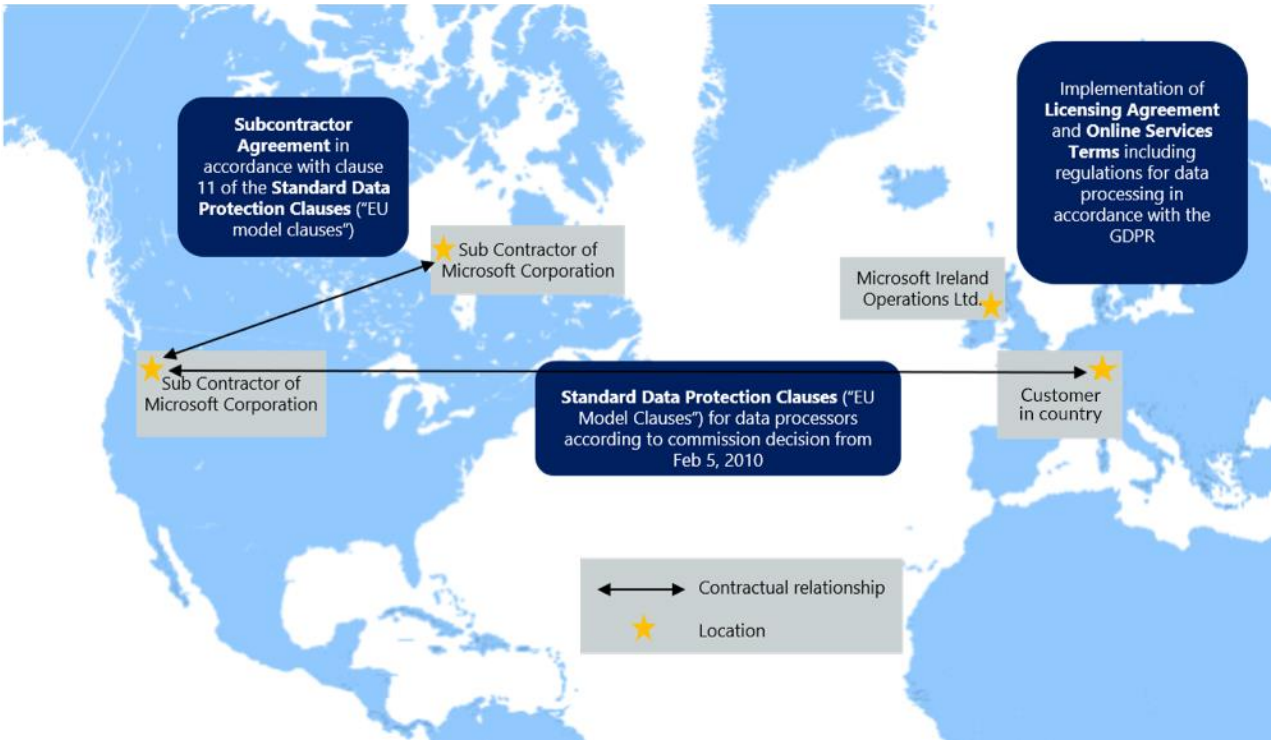
All requirements cannot be conclusively listed here. In practice, sector-specific requirements, such as special requirements in the financial services sector, can apply (you can find more information regarding requirements for cloud services in the financial services sector here. Furthermore, additional local regulatory requirements may need to be considered.

With regard to Germany – in accordance with the general bookkeeping principles provided by the commercial and tax law – proper treatment of electronic documents and orderly access to data are particularly required (German Principles for Orderly Management and Storage of Books, Records and Documents in Electronic Form and for Data Access; GoBD). Crucial point in this regard is the internal controlling system (in German: "Interne Kontrollsystem" "ICS"). To document a functioning ICS, which detects developments that could jeopardize an enterprise at an early stage, Microsoft offers customers, including their independent auditors, a certificate in accordance with the internationally accepted audit standard ISAE 3402. If a customer stores data

relevant for tax purposes exclusively in Microsoft's Enterprise Cloud at data centers within the EU, the customer must also have an approval for this from the competent German tax authority.

II. Contractual Relationships

The contractual relationship between Microsoft and its customers can become a bit complicated, especially if the Cloud Services are used by different companies of the customer. This section, including the below graphic, explains and illustrates the contractual structure to provide more clarity in this regard. Further details can be found under Microsoft Contacts Explained.



8. What are the contractual relationships if the Enterprise Cloud Services are used by different group companies of the customer?

The cloud services may continuously be procured by a central group company, e.g. by the IT-service company of the corporate group. The license agreement will be concluded between this group company and MIOL. On customer´s side, the Data Processing Agreement and the SCC should be signed by all group companies which are using the services because, from the viewpoint of the data protection authorities, these group companies are the responsible "data controllers" which must have a direct contractual relationship with the non-EU-domiciled Microsoft Corporation. Microsoft offers a supplemental agreement for this purpose.

9. What are the contractual relationships when enterprises, particularly Microsoft Partners, use a Microsoft platform such as Microsoft Azure and offer the services to their customers based on such platform?

Within the so called "platform as a service" (PaaS), the structure of the agreement depends on the specific case. If the Microsoft Partner plans to offer applications, which are developed by the Partner as a service, the Partner may want to consider not to incorporate any performance obligations in its contractual terms that exceed those the Partner has agreed with Microsoft.

III. Data Transfers to the US

Data transfers to the US are usual in connection with providing the Microsoft Enterprise Cloud Services. This section explains which safeguards and approaches Microsoft takes to protect data transferred to the US and to comply with relevant data protection laws, also with regard to the new American CLOUD Act.

10. Which measures does Microsoft take to safeguard data transfers to the US?

There are several ways of safeguarding data transfers to the US, in particular SCC, adequacy decisions by the EU-Commission and – being subject to approval – binding corporate rules or individualized contractual clauses for data transfers.

As stated in section I 5 above, Microsoft incorporates the SCC in its OST to protect data transferred to the US.

In addition, Microsoft is an EU-U.S. Privacy Shield-certified company since August 2016. The certification can be found here. The EU-U.S. Privacy Shield serves as an appropriate safeguard for data transfers to the US. It is a data protection agreement between the EU and the US government allowing US companies to voluntarily undertake to comply with the EU data protection standards set out in the agreement. On July 12, 2016, the EU Commission issued an adequacy decision stating that those companies certified in accordance with the EU-U.S. Privacy Shield provide an adequate level of data protection required for transfers to the USA. The EU-U.S. Privacy Shield is considered as a replacement for the Safe Harbor Principles, which were ruled invalid by the ECJ.

Thu, the necessary legal basis exists for the transfer of personal data to the US-established Microsoft Corp. for the Microsoft Core Services as well as for the Non-Core-Services, e.g. the Azure Non-Core-Services – irrespective of the SCC.

In view of the binding decision of the EU Commission on the EU-U.S. Privacy Shield, approval of the data transfer by the data protection supervisory authorities is not required.

11. Does Microsoft disclose customer data to US authorities, such as the National Security Agency (NSA)?

In case Microsoft receives an order to disclose data, Microsoft will not provide any data to the authorities but will directly refer the requesting authority to the customer. However, should the authority still require Microsoft to disclose data, Microsoft will comprehensively examine this request for disclosure from a legal point of view.

12. What is the new American CLOUD Act and why was it adopted?

The adoption of the Clarifying Lawful Overseas Use of Data Act (hereinafter, CLOUD Act) is a result of United States Supreme Court proceedings which were based on the question of the legality of a search warrant issued by a New York court. In that search warrant, Microsoft was requested to disclose e-mail communications of a customer stored in an Irish data center of Microsoft. Microsoft did not comply with this order, arguing that a U.S. judge has no authority to issue a warrant for information stored abroad, and won the case before the US Court of Appeals.

In March 2018, while the "New York Search Warrant" case was being heard by the US Supreme Court, Congress passed the CLOUD Act. With the CLOUD Act, the previous legal situation was changed with regard to, inter alia, the storage of data in the cloud by communication providers established in the USA, regardless of the location of the cloud servers. When the legal questions raised by the "New York Search Warrant" case became obsolete under the CLOUD Act, the US Supreme Court case was declared invalid and referred back to the lower courts to dismiss the claim. Further details can be found here and here.

13. What is the relevance of the new American CLOUD Act?

The Under the CLOUD Act, US law enforcement agencies can obtain information regarding information stored abroad from US service providers and their subsidiaries on the basis of investigation orders. The CLOUD Act serves the investigation of crimes. The CLOUD Act does not oblige cloud service providers to disclose customer information to US law enforcement agencies in any case. It merely provides a legal framework for resolving conflicts of law by enabling the US and encouraging foreign governments to conclude bilateral agreements on dealing with requests in cross-border investigations.

The UK already concluded such a bilateral agreement with the US in October 2019. Further details can be found here. The other member states have not yet concluded such bilateral agreement with the US.

Whereas the CLOUD Act creates new rights under new international treaties, the cloud service providers still have the right to go to court in the event of a conflict of laws to verify the legality of search warrants. If cloud service providers challenge investigation orders on the legal ground of a violation of national laws, this may lead to the repeal of the investigation order. Nevertheless,

the CLOUD Act states to the competent US courts that the violation of foreign law alone does not lead to annulment. Rather, the courts must make an overall assessment which in consequence can lead to the prosecution authority's prevailing interest in the (unchanged) maintenance of the investigation order.

Cloud service providers can challenge investigation orders if they fear a violation of the international comity. This is more far-reaching than a mere violation of national law as it involves mutual consideration at state level. The principle of comity implies that, for reasons of international law, States must take into account, inter alia, the law existing in other States.

Further details can be found here.

14. What are the consequences of the new American CLOUD Act for Microsoft?

To protect the privacy of its business customers in the future, Microsoft complies with the following five principles:

1. Microsoft will continue to refer US authorities to the respective business customers instead of providing data to the authorities by choice.
2. Microsoft will continue to go to court to defend the local rights of our customers if their rights are violated by the US government.
3. Microsoft will continue to push for new international agreements that strengthen the rights of our customers.
4. Microsoft will be transparent about the number of international search warrants we receive.
5. Microsoft will continue to offer our customers several alternatives for storing their data.

Further information about the principled way for Microsoft after the adoption of the CLOUD Act can be found here.

15. How many requests does Microsoft receive from investigating authorities?

Microsoft informs half-yearly about the number of worldwide official investigation requests on its website since many years. Here you can find these so-called Trust Reports under the category "Digital trust reports". In this context, it is also worth mentioning the FAQs which deal in more detail with the number of investigation requests relating to "Enterprise Cloud Customers". You can find them under the abovementioned link.

IV. Data Transfers to the US

Microsoft takes maximum efforts to secure and protect data to the extent possible for providing both the full advantages of the Enterprise Cloud Services and also safeguards with respect to the

data processed. This section explains Microsoft's approach and shows which efforts it takes to secure and protect data.

16. Where is data stored in the Microsoft Enterprise Cloud?

Microsoft pursues a regional strategy for its data centers. The country or region of the customer the administrator first chooses when initially setting up the service determines the primary storage location for the customer data of Office 365, Dynamics 365 and Windows Intune ("data at rest"). Thus, for European customers, the customer data of Microsoft Enterprise Services (Office 365, Dynamics 365 and Windows Intune) are stored by default in Microsoft data centers within the European Union, in particular in Dublin and in Amsterdam. You may find further information here at Microsoft's trust center. For Azure Services, customers can generally choose the region where their data are stored. Information about services, which do not enable regional storage may also be found in the Trust Center. You can find the corresponding links at the end of this document.

17. Can Microsoft Enterprise Cloud Services be used by persons subject to professional secrecy?

If not prohibited by local laws: Yes. In Germany, for example, Section 203 of the German Criminal Code permits the disclosure of secrets entrusted to persons subject to professional secrecy (e.g. doctors, psychologists or lawyers) to other persons involved, e.g. external IT service providers. However, this shall apply only if no more professional secrecies are disclosed than necessary for the use of the service provider and the service provider was obliged to maintain secrecy. An organizational integration into the sphere of the person who is subject to professional secrecy is not necessary.

This allows the use of supporting IT services, such as the provision and support of IT systems and applications, as well as the use of cloud applications by persons subject to professional secrecy. Microsoft offers an additional agreement for this purpose.

18. How does Microsoft deal with encryption?

In answer to reports on the access to data lines by the intelligence services of various countries, Microsoft transfers data between its data centers exclusively in an encrypted way. Microsoft has also implemented the encryption of data to its servers, in particular Enterprise Cloud Services, by the end of 2014.

19. Can the application of data protection law be excluded by encryption?

This mostly depends on the type of encryption. If encryption occurs on both, the transmission path between the customer and Microsoft and on the data that are stored in the Cloud and if the key remains solely with the customer, these data do not relate to natural persons from

Microsoft's point of view. In this case, data protection regulations do not apply to the processing by Microsoft.

For this purpose, Microsoft offers its customers the use of their own keys for encrypting data in Microsoft Azure Rights Management. The key is protected by a hardware security module (HSM) of the manufacturer Thales, so that Microsoft is unable to export and disclose the key. Such encryption would exclude the references to a natural person in the data, but could also restrict functionalities, such as the search functionality.

However, there will always be data (e.g. administrator and meta data) that cannot be encrypted, which makes it necessary to observe data protection law at least in this regard. In any case, encryption represents a form of protection that is assessed positively in terms of data protection law. For more information about encryption click here.

20. How can customers fulfill their obligation to assess compliance with all agreed technical and organizational measures?

Customers are obliged by data protection law to assess the implementation of the technical and organizational measures when conducting a commissioned data processing. Customers can meet this obligation by having presented certificates from independent third parties. Therefore, Microsoft is audited by a third party every year. Such audits are conducted by internationally recognized auditors who check whether Microsoft is ensuring the policies and procedures for security, data protection, continuity and conformity. This is based on the ISO 27001 standard which is one of the world's best security-comparison-benchmarks. Microsoft provides its customers with audit reports in accordance with ISO 27001 upon request.

Moreover, Microsoft has been certified in accordance with the international ISO/IEC 27018 standard for data protection in the Cloud as the first leading provider of Cloud services.

The ISO/IEC 27018 standard, which is an extension of the previously mentioned ISO 27001 standard, was developed by the International Organization for Standardization (ISO) to create a uniform and internationally valid concept to protect personal data stored in the Cloud. The British Standards Institution (BSI) has independently verified that Microsoft Azure, Office 365 and Dynamics 365 are in compliance with the "Codes of Practice" for the protection of personal data in Public Clouds. In addition, this test was conducted for Microsoft Intune by Bureau Veritas.

These certificates are stipulated contractually in the Microsoft OST (for the ISO/IEC 27018 standard since April 2015), but do not alter the rights given by the SCC or the GDPR.

21. How can customers store data securely for revisions?

Microsoft stores data geo-redundantly in several locations in various data centers. Accordingly, no back-ups are necessary in order to restore lost data. If the customer requires a reproduction of historical data, the customer must use an archiving solution in addition to the Microsoft Enterprise Cloud Service.

Resources

You can find further up-to-date information at:

- Microsoft Trust Center
- Office 365 Trust Center
- Microsoft Azure Trust Center
- Dynamics Trust Center
- Transparency reports

Legal Note

This compendium contains a general overview of issues our clients deal with while using Cloud Computing Solutions. It shall enable our clients to understand the legal background of cloud computing solutions. This compendium is not to be understood as an examination of individual legal matters. For an assessment of the legal requirements in the context of Microsoft cloud solutions in the individual case you must seek separate legal advice.