# GDPR Physical Security and Privacy Safeguards

The European Union General Data Protection Regulation (GDPR) requires organisations worldwide to rethink how they access, use and maintain personal data. This white paper describes scenarios of data risk that could result in administrative interventions and financial penalties under the new regulation. It also explores physical security and privacy best practices – as they represent an important but often overlooked area of data protection. Together, administrative, cybersecurity and physical safeguards can help protect sensitive personal data, and demonstrate an organisation's commitment to data privacy.

## Key Takeaways:

- Learn what the GDPR says about physical security and privacy measures to protect personal data.
- Explore what industry experts consider a reasonable level of data protection and privacy.

**Living in a Data-Driven World**

As a natural part of doing business today, most organisations collect and use personal data – whether about personnel, customers, prospects or third-parties. Typically, this data is stored in electronic form where it can be accessed by the organisation[1] and external parties. Further, some organisations' main function is to collect and analyse volumes of personal data.

While the amount and type of data gathered by each organisation varies, there is widespread agreement that finding it has never been easier. Individuals leave behind a vast trail of data when they create social media profiles, participate in online communities, conduct internet searches, respond to surveys, and take advantage of promotional offers and "free" services, such as for photo storage and music streaming.

Technology further aids the process of building robust profiles on people, with advancements in artificial intelligence, e-tags, web beacons, cookies, and other monitoring tools.

Together, technology and data mining efforts have allowed organisations to accrue troves of personal data. These repositories may reveal a person's age, marital status, birthday, education, hobbies, religion, employment history, political beliefs, buying preferences, preferred news sources, income, criminal background, and so much more.

While much of this data is centralised in company databases, pockets of data are often scattered across the supply chain in disparate systems – often lacking any mechanisms for conveying to future recipients of the data how or why it was originally collected. This leaves personal data exposed to uses far afield of the original purpose for which it was obtained.

On any given day, numerous people within an organisation can access the stored data – to perhaps pay an employee, conduct market research, launch an email marketing campaign, or track customer engagement. Each access point to these data pools represents an opportunity for personal data to be misused or fall into the wrong hands.

## Quick Facts

**What is GDPR?**
The General Data Protection Regulation (GDPR) aims to protect the privacy of individuals in the European Union (EU).

**When does it go into effect?**
May 25, 2018

**Who does it affect?**
All companies – regardless of their location – that control or process personal data of data subjects in the European Union.

**What constitutes personal data?**
Any information related to a natural person or data subject. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

**What is the impact?**
A fine of €20 Million or up to 4% of annual global turnover (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements.

**Where can I go for more information?**

- An overview of the regulation
- Read the regulation
- Physical security solutions

**65%**
of respondents say data breach incidents did cause them to lose trust in the organisation experiencing it.[5]

To understand the physical security risks that organisations face, consider these scenarios:

An employee reviews sensitive data on their phone while at the airport, and doesn't notice someone nearby looking at their screen.

- An employee loses their laptop and information on the drive is not encrypted.
- An employee steps away from their desk to refill their coffee cup, leaving customer contact information displayed on their monitor or desk as an unauthorised viewer walks by.
- A disgruntled employee takes photos of documents left on a printer, information displayed on a screen, and log-in credentials taped to a computer monitor.
- Obsolete laptops or desktops are donated to charity without fully erasing the hard-drives.
- A doctor's office closes and throws patient records in the dumpster without shredding them.

In 2016, Hackers compromised
**1 billion records**[2]

It's scenarios like these that are increasingly worrisome, as data breaches are all too common in today's digitised world. Forrester reports that in 2016, hackers compromised one billion records in just 12 months. In the first half of 2017, it was reported that 918 data breaches led to 1.9 billion data records being compromised worldwide. This represents an increase of 164 percent compared to the first six months of 2016.[2]

With each new data breach, there is increasing anxiety that data privacy is all but lost. According to a recent study, people feel their privacy is challenged by security and confidentiality issues. In fact, 91 percent fear that individuals have lost control over how their personal data is collected and used by companies. An almost equal number believe that it would be very difficult to remove inaccurate information about themselves online.[3] It's not just major breaches that are a concern. Small businesses may have less information about an individual but it's no less important to those individuals if it's stolen or misused.

These fears continue to mount, even though strict data privacy and data protection directives and regulations have been around for more than a decade. The Health Insurance Portability and Accountability Act (HIPAA), The Fair Credit Reporting Act, and The European Union's Data Protection Directive being a few prominent examples.

The Data Protection Directive outlines principles, such as the requirement that data be secure, processed for limited purposes and kept no longer than necessary. However, as a "directive" rather than a law, the implementation and the enforcement in each country in Europe varied.

**Enter the GDPR**

The GDPR is the most comprehensive and globally impactful regulation introduced to protect personal data. It was created because of the shared belief that everyone has a fundamental right to privacy. It aims to protect the privacy of individuals in the EU by enforcing a new regulation on how businesses protect, process and use personal data.

GDPR may be the most important advancement in data security and privacy regulation in 20 years – both because of its accountability requirements on record-keeping, and its potential financial impacts. With two-tiers of fines, organisations can be penalised 2 percent of annual global turnover/€10 million for violations, such as:

- Failing to notify a supervising authority and affected individuals about a data breach
- Failing to appoint a data protection officer (DPO) if the organisation requires one

Organisations can be subject to a fine of 4 percent of annual global turnover/€20 million for violations, such as:

- Failing to honor data subject rights
- Failing to comply with an order of a supervisory authority
- Failing to comply with requirements for international data transfers[4]

These fines are in addition to the loss of reputation, brand value and trust – which can be equally devastating to a company's bottom line. In fact, data breach incidents reportedly cause 65 percent of individuals to lose trust in the organisation experiencing it.[5]

GDPR compliance is no small undertaking as it holds organisations accountable for how they gather, use, maintain and purge personal data, all while keeping it secure. Even those with existing privacy and security programs in place need to re-evaluate their processes. Specifically, the GDPR

The GDPR is the most comprehensive and globally impactful regulation introduced to to protect personal data.[1]

requires organisations to implement appropriate technical and organisational measures to prevent the loss of or unauthorised access to personal data.

This has many asking questions, such as:

**Q. What constitutes personal data?**
**A.** Any information relating to an identified or identifiable natural person.[6] This could include identifiers (such as a name or an identification number) or data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, genetic data, health information, criminal offenses; work performance predictions, economic situation, personal preferences or interests, reliability or behavior, location or movements, etc.[7]

**Q. What is pseudonymisation, and why should I care about it?**
**A.** Mentioned 15 times with the GDPR is the term 'pseudonymisation' – a procedure by which identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. The GDPR recommends the application of pseudonymisation to personal data to reduce risks to data subjects and help controllers and processors meet their data-protection obligations.[8]

**Q. Can organisations get consent from individuals to gather their personal data?**
**A.** Yes, but consent needs to be given by a clear, affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data. Pre-ticked boxes, silence and inactivity do not constitute consent.[9] Organisations need to maintain a record of receiving consent, and make sure consent requests are distinguishable from other requests, using clear and plain language.[10] Article 13 outlines extensive information that needs to be provided to the data subject at the time personal data is collected, such as the purpose of gathering the information, the recipients or categories of recipients of the personal data, and the time period the data will be stored.

**Q. What is a Data Protection Impact Assessment (DPIA)?**
**A.** A DPIA, which is required for high-risk activities, helps organisations evaluate the origin, nature, particularity and severity of risks and implement appropriate measures to mitigate risks, such as encryption. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may lead to physical, material or non-material damage.[11]

**Q. Do I need to appoint a Data Protection Officer (DPO)?**
**A.** The designation of a DPO is mandatory wherever the data processing is carried out by a public authority (except courts acting in their judicial capacity) or for a company whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale. A DPO is also mandatory for all enterprises that process data regarding sensitive data, such as health, religious or political beliefs on a large scale. Specifically, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.[12]

**Physical Security and Privacy Requirements**
What should organisations do to prevent data breaches? Article 24 of the GDPR outlines an organisation's responsibility to implement "appropriate technical and organisational measures" to ensure and demonstrate proper processing of personal data. Article 32 goes a step further to explain that "In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

An important aspect of this regulation is the emphasis on preventing unauthorised access. This is where physical security is essential. Specifically, it can help safeguard data against internal and external human threats that aim to exploit gaps within your organisation's walls and through your workforce. This includes limiting what data can be observed, stolen or accessed. Review the following and assess whether your workforce has the appropriate technical and organisational measures in place to comply.

**Deploy Data Protection by Design and Default:**
To protect data by default, organisations must proactively identify and collect only the personal data necessary for their intended purposes, keep the data only for as long as necessary (minimisation principle), and they should ensure that personal data will not be made accessible to an indefinite number of people. This will likely involve making sure privacy risks are identified up front and systems are designed to mitigate these risks, pseudonymising and anonymising as appropriate, creating transparency within the processing functions, and identifying specific people or roles that need access to the data. Ask yourself: Are you considering privacy risks to individuals before designing your information systems, business practices and physical design? Have you met with your IT staff to review current systems and processing activities, and to discuss if additional steps are needed to document how personal data will be protected throughout the entire information lifecycle?

**Use Physical Safeguards:**
While cybersecurity controls, such as data encryption and complex passwords, are critical, "low-tech" administrative and physical controls are equally important. To determine where physical barriers are needed, identify where sensitive information is accessed. For example, employees frequently use mobile devices to access and share data from anywhere. A growing number of these workers access sensitive information in public places, often in full view of others. There's increased risk of data exposure inside the office too. The common open-office floor plans remove physical barriers that traditionally helped shield computer screens. Ask yourself: Have you positioned computer screens away from windows, doors and areas publicly accessible? Do you equip monitors and mobile device screens with privacy screens to obscure the viewing of information to potential onlookers? Are shared printer/copier/fax machines in protected areas or have locking covers? Do you store physical copies of data in an access-controlled facility? Are shredders standard issue to all on-site units, especially by copiers, printers, and faxes, and a prerequisite for all who telework or use remote connections to access corporate information assets?

**Schedule Employee Training:**
Training programs should cover three key aspects: Observation, Physical Access, and Theft Prevention best practices. For example, employees should be reminded to be conscious of their surroundings when accessing and managing connected devices from public places via their laptops, tablets and smartphones. Device screens should not be exposed to passersby and potential onlookers, especially when entering log-in information or viewing sensitive account details. When it comes to physical access, organisations should train employees to erase information from white boards and collect confidential papers following meetings, memorise passwords instead of writing them down, lock file cabinets and laptops, use privacy filters on computing devices and maintain a clean desk policy including logging off unattended devices. Ask yourself: Does your training program encompass situational awareness so employees learn to be mindful of their surroundings and can identify and respond to suspicious behaviors? Do employees understand our organisation's expectations of the "clean desk" policy? Do you frequently remind employees of good security practices they must follow?

**Develop Clear Policies:**
To demonstrate an organisation's commitment to implement appropriate security and privacy measures, their policies should outline the do's and dont's of information viewing and use for employees and contractors both in the workplace and when working remotely. Employee agreements should contain specific language about the responsibility to safeguard sensitive and confidential information.[13] Ask yourself: Have you communicated to individuals your privacy and security practices statement, explaining how your organisation protects, shares, disposes of, and provides access to personal data? Do you have a BYOD (bring your own device) policy governing employee conduct and required security controls for when they access corporate resources from their personal devices? Do you require, as part of your security policy, that employees use both visual and cybersecurity controls?

**Set Data Storage Limits:**
Set time periods for how long personal data will be stored –in accordance with applicable laws. Securely erase all personal data that is not absolutely required to support the business purposes for which they were collected. Ask yourself: What technical controls do you have in place so data is erased at the right time? Do your organisation's destruction processes meet strong security guidelines, such as provided by NIST Special Publication 800-88, such as physically destroying hard drives that have reached end of life?

**Verify Third-Party Suppliers:**
Only use processors that provide sufficient guarantees in terms of expert knowledge, reliability and resources to implement technical and organisational measures, including for the security of processing. Ask yourself: Do you have a vendor management program in place that includes contractual obligations and establishes management oversight activities for third parties with access to personal data?

**Create a Data Breach Protocol:**
Organisations must be prepared to notify the supervisory authority without undue delay when it becomes aware that a personal data breach has occurred (when feasible, no later than 72 hours). Or, be able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If there is a high risk, the data subject(s) must also be notified of the data breach, without undue delay.[14] Ask yourself: When did you last review your organisation's incident response and breach notification policies and plans? Do employees know who within the organisation to alert if their device is compromised or they become aware of a data breach? Do you have an up-to-date incident response and breach notification plan in place to determine when and how to notify authorities about a data breach?

**Know the Individual's Rights:**
EU residents now have the right to see what personal data organisations have regarding them – and request their data be erased under certain circumstances. The right to erasure requires organisations to erase any links to, or copies or replications of those personal data. Organisations should provide a way for people to make requests electronically, especially if personal data is processed by electronic means.[15] Ask yourself: Does your organisation understand what is considered "personal data" and how to respond to inquiries regarding personal data?

## Conclusion:

GDPR is the most important change in data privacy regulation in 20 years. It requires that personal data be managed in a manner that helps ensure appropriate security and confidentiality – a task requiring both technical and organisational security measures. And the fines for noncompliance could be crippling. However, the best practices outlined in the regulation are simply good business. No individual wants their information misused, and no organisation wants to face the repercussions of a data breach. Organisations that view privacy not as a compliance burden but as a corporate responsibility can use it as a strategic advantage to improve their reputation and brand value, attract better employees, and ultimately maintain public trust.

**www.3M.co.uk/PrivacyFilters**



[1]Forrester, Lessons Learned from the World's Biggest Security Breaches and Data Abuses, January 9, 2017
[2]2017 Gemalto Breach Level Index, http://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx
[3]GfK Privacy Panel, Public Perceptions of Privacy and Security in the Post-Snowden Era, 2014.
[4]Article 83, the GDPR, 2017
[5]Ponemon Institute, The Impact of Data Breaches on Reputation & Shared Value, sponsored by Centrify, 2017.
[6]Article 4, the GDPR, 2017
[7]Recital 75, the GDPR, 2017
[8]Recitals 26 and 28, the GDPR, 2017
[9]Recital 32, the GDPR, 2017
[10]Article 7, the GDPR, 2017
[11]Article 35 and Recitals 83-84, the GDPR, 2017
[12]Articles 37-38, the GDPR, 2017
[13]Recital 74, 77-78, the GDPR, 2017
[14]Recital 81, the GDPR, 2017
[15]Recital 59, 63, 65, 66, the GDPR, 2017

**The experts in screen privacy.** | 3M