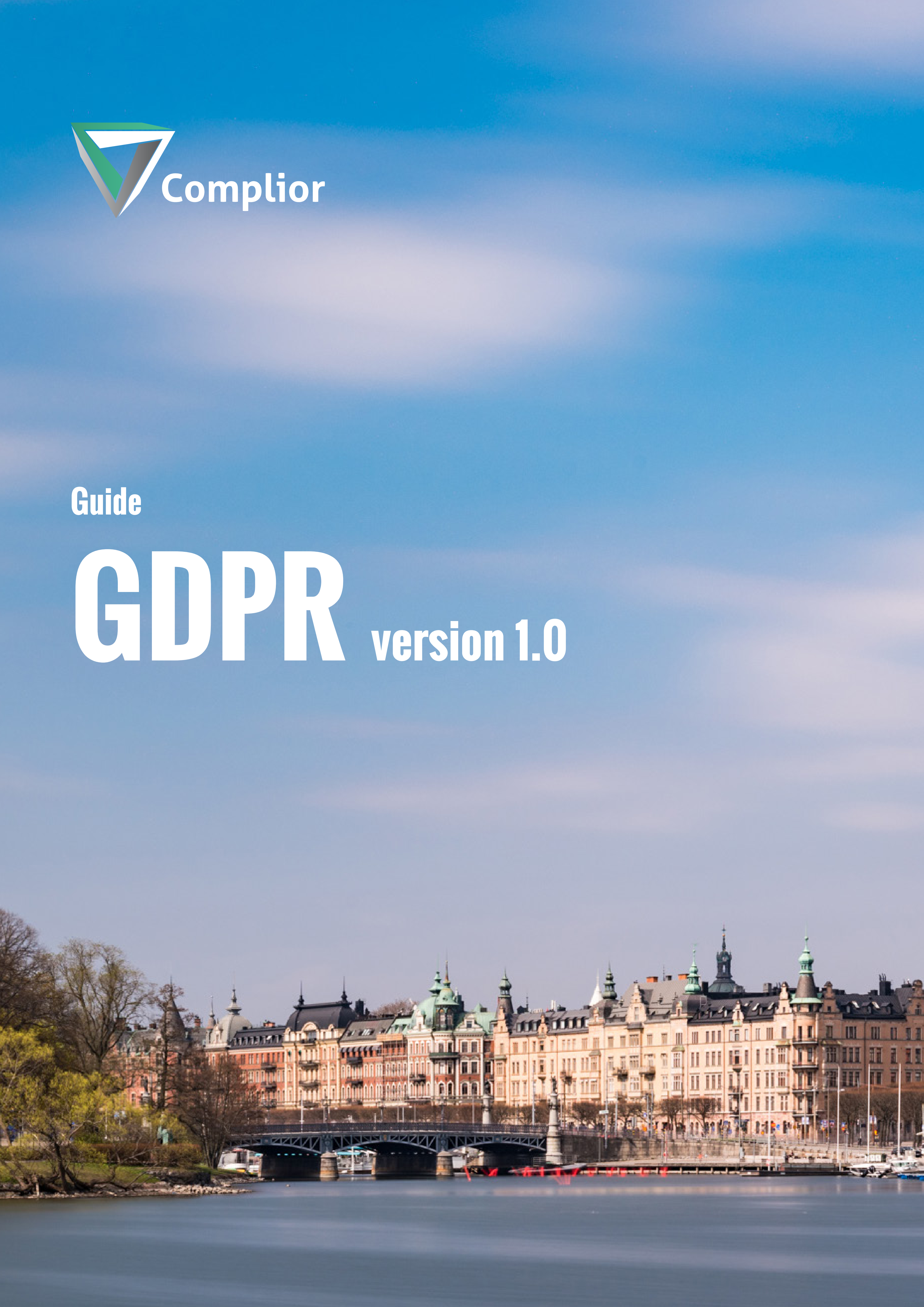

Complior

Guide

GDPR version 1.0

Table of content

Foreword

This guide is intended as an easy-to-understand, educational and comprehensive tool for those who are responsible for their organization's compliance with the new General Data Protection Regulation (GDPR). The guide can also be of use to those who have academic or other interests. The Data Protection Regulation will be the most important issue for many management teams in 2017/2018.

This guide will provide you with much more than just a basic insight into the subject. It provides concrete examples and guides you through the difficult legal jargon and the unique concepts of the regulation.

It is less than one year left until the regulation is applied in member state law, and this guide will be updated continuously as more information about the regulation is published. In the next version of this guide, the following sections will be added: Profiling, Data Privacy Impact Assessment, Transfer of Personal Data to Third Countries, Access Control, GDPR Log Management, Privacy by Design and the Right to Data Portability.

I wish you good luck with your GDPR compliance.

Jonas Gharanfoli,
Security consultant

1. Background

On May 25th, 2018, the General Data Protection Regulation (GDPR) will apply in member state law. The regulation affects all organizations that process personal data of EU/EEA-citizens, such as companies and public authorities. The purpose of the regulation is to extend and ensure the privacy rights of all EU/EEA-citizens. For example, if your organization has a CRM-system or an employee register, your organization will need to comply with the General Data Protection Regulation.

Prior to GDPR, member states were regulated by the Data Protection Directive, enforced in 1995. A lot has happened since 1995; the digital world we live in today has changed the conditions of how personal data can be collected, disseminated and analyzed. The development of Big Data analytics, marketing and the deployment of services such as Facebook have fueled the privacy debate in Europe. In January 2012, the European Commission presented a proposal to thoroughly reform the Data Protection Directive. As a consequence, the Data Protection Directive was expanded and converted into a regulation.

GDPR is a regulation and not a directive.

Both regulations and directives are called ‘legislative acts’ in EU law. Directives are goals given to member states. It is up to each member state to decide how to achieve the goals by incorporating the directive into new or existing laws. This means that laws created by directives may differ significantly between member states. By contrast, regulations are basically complete laws that will apply directly in full to all member states on a predetermined date. Regulations thus lead to much stronger harmonization within the EU/EEA.

The burden of compliance will be immense for many orga- nizations, however, an organization that prepares in time can get a significant competitive advantage. In addition to improved privacy protection, many service providers and customers will require your organization to comply with the GDPR as they may be put at risk if you do not.

Member States and regulatory authorities are also encouraged by the regu- lation to introduce certification mechanisms for the GDPR. In the same way as organizations can certify themselves to demonstrate their environmental responsibility, organizations will be able to demonstrate their privacy and cyber security responsibilities.

1.1 Which organizations are affected?

GDPR applies to all organizations that “process” personal data belonging to EU/EEA citizens, even if their base of operations is outside the EU/EEA. The regulation may cause a global uproar as there are many organizations outside of the EU/EEA that process personal data belonging to EU/EEA citizens. The public sector will also be affected because public bodies must comply with the regulation as well. The regulation regulates those who control the processing of personal data (contro lers) along with service providers (processors) that process personal data on controllers’ behalf.
The organizations that are excluded from the regulation are law enforcement agencies like the police. They have a new directive from the Euro- pean Commission that is similar to the GDPR.

1.2 Key differences between the GDPR and the DPD

- The privacy-rights of data subjects are enhanced.
- The supervisory authorities can impose harsher administrative fines – maximum administrative fines up to 20 000 000 EUR or up to 4 % of the total worldwide annual turnover, whichever is higher.
- Privacy by design - privacy protection should be incorporated into systems from the very beginning and permeate their entire life cycle.
- More requirements concerning assessments, processes and documentation.
- Consent must be gathered in a more transparent manner and is required under more circumstances.
- ”The right to be forgotten” will be enforced. This means that organizations must, in certain circumstances, delete all personal data of data subjects if they wish.
- The processing of children’s personal data will require the consent from the holder of parental responsibility over the child for “information society services” (e.g. Facebook, Instagram).
- New requirements for marketing (profiling / selection).
- Your organization must, under certain circumstances, retain a Data Protection Officer.
- Service providers (processors) are liable under GDPR. In the DPD, only controllers were liable, now both processors and controllers can suffer penalties if they violate the GDPR.
- More requirements concerning processing agreements, which will need to be rewritten.

2. Key Concepts

The regulation contains unique terms, definitions and concepts that the reader must know before explaining the more complex aspects of the regulation.

2.1 What is personal data?

According to the regulation, 'personal data' is:

"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, loca- tion data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4(1))

An identified or identifiable natural person means a living person in the regulation (it is up to each individual member state to decide whether it must be a living person or if personal data of the dead should be covered).

*"... an identifiable natural person is one who can be identified, **directly** or **indirectly**..."*

You can directly identify someone by, e.g., their full name or social security number. If someone has a very rare first and/ or last name, this can suffice to directly identify someone. You can indirectly identify someone by combining information such as occupation, location, physical characteristics, and social status. For example, "cyber security consultant + brown hair + Frösunda (a small area in Sweden)" is personal data because this information can be indirectly linked to a very few identifiable natural persons in Frösunda. A guideline used by statisticians in the domain of PII (Personal Identifiable Information), is if the information can be linked to less than seven people, it is considered PII or personal data.

"Identifier such as a name, an identification number, a location or online identifiers ..."

Online identifiers such as IP addresses and cookies are also considered personal data. Location data such as GPS coordinates are considered personal data if they are linked to a person.

Are dynamic IP addresses personal data?

Today, it is very common for people visiting websites to have their IP address stored by the owner of the site. A dynamic IP address, together with the time and the ISP's customer directory, can identify exactly which computer visited a webpage at a certain time; this information can thus be attributed to an identifiable physical person. According to a verdict from the European Court of Justice (The Breyer-verdict), dynamic IP addresses are considered personal data if the owner of the website has "legal means" to request third-party information, such as ISP information, and it should not be "Impossible to implement in practice".

2.2 Processing

The term 'processing' is very broadly defined in the regulation, it basically includes everything you could possibly do with personal data. The full definition from the regulation reads as follows:

"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, orga- nisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restric- tion, erasure or destruction" (Article 4(2))

2.3 Supervisory authority

In each member state a supervisory authority has been appointed. A supervisory authority is an independent public authority whose function it is to ensure compliance of the GDPR in their jurisdiction. In Sweden, the supervisory authority is Datainspektionen. Each supervisory authority will, among other things, have the following obligations:

- Conduct audits
- Can issue warnings
- Can temporarily restrict or completely prohibit processing of personal data
- May issue administrative fines
- Must receive notifications under major breaches
- Can issue certifications and revoke certifications

The GDPR's goal with the supervisory authorities is that organizations operating internationally should answer to a single lead supervisory authority. Which lead supervisory authority the controller or processer must answer to depends on where the organization has its main establishment, i.e., the place of its central administration.

2.4 Controllers, processors and processing agreements

The new data protection regulation imposes new requirements on controllers and processors. The controller is the legal person (public authority or company) that controls what personal data is processed and the purpose of the processing. Controllers are not a physical person such as the CEO, CTO or Data Protection Officer. Even if an employee decides to set up an illegal registry of personal data, it will be the organization that pays the administrative fine. Keep in mind that the con- troller has the greatest responsibilities in the GDPR.

A processor is a legal person who processes personal data on behalf of the controller. A processor is often a supplier or service provider. The processing does not only apply to storage but also to remote access for service, support, development, maintenance and the like. For example, a processor may be a cloud service provider. A novelty in the GDPR is that both controllers and processors must comply with the GDPR. Processors were not previously liable in the DPD.

The big question here is: if a processor violates GDPR, will the controller also be liable and vice versa?

The short answer is - it will differ on a case-by-case basis. What is important is to comply with the principle of accountability in the regulation – to clearly document exactly what obligations the controller has and what obligations the processor has. This must be governed by a written contract, a "processing agreement". If one party fails to comply with the contract, that party will suffer the penalties. Processing agreements must follow the requirements in article 28 and should be created with the help of a legal consultant. There is a pos- sibility that supervisory authorities will create standardized agreements to facilitate this process in due time.

***Note**: A processor is almost always also a controller. This is be- cause they have, e.g., employees and suppliers of their own. I emphasize that the entire chain of suppliers and subcontractors are liable in the GDPR, which means that if a subcontractor makes a mistake, there may be legal consequences for all within the supply chain, including the controller.*

2.5 Special categories of personal data

'Special categories' of personal data or sensitive categories of personal data are defined in article 9(1), and include the following:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union Membership
- Health
- Sex life or sexual orientation
- Genetic or biometric data

There are also cases where the processing itself can be considered sensitive. There are organizations that can process information that is not sensitive by itself, but by using different models and algorithms they can disclose sensitive personal data. For example, there are companies that can detect if a person is prone to diabetes just by analyzing their purchase history of food products. This processing is therefore sensitive because health-related information belongs to a special cate- gory of personal data.

***Note**: It is difficult to get a legal basis for the processing of sensitive personal data in the regulation. If an organization processes sensitive personal data illegally, it can suffer major penalties. For legal processing of sensitive personal data, additional protection measures will need to be implemented in most cases, such as pseudonymization.*

2.6 Protection-worthy personal data

Then we have categories of personal data that are not defined as "special categories" in the regulation, but will still need to be processed with extra caution. This is because, as with the special categories, there is a great risk of violating the rights and freedoms of data subjects. The processing could also lead to psychological and/or material damage if the data is disclosed to unauthorized individuals. I have chosen to call this category of personal data 'protection-worthy' personal data.

This information includes:

- Professional secrecy / protected personal data
- Social security number
- Passport Number
- Certain financial information
- Other information related to people's private life
- Information related to children
- Authentication credentials
- Cardholder data (credit-/debit card data)

Note: Processing of personal data relating to criminal convictions and offences can only be carried out under the control of official authority or when the processing is authorized by Union or Member State law. Any comprehensive register of criminal convictions can only be kept under the control of official autho- rity.

2.7 Pseudonymization and data anonymization

Pseudonymization:

This means that personal data is exchanged for non-identifiable information. To restore the original information, additional information is required which is kept separately, e.g., by using encryption or substitution techniques. Pseudonymized personal data is still considered personal data by the regulation.

Anonymization:

Personal data is exchanged for non-identifying information. Unlike pseudonymization, there is no additional information that can restore the original information, e.g., if you delete or mask the "key" that allows the information to be linked to a person. Anonymized personal data is no longer covered by the regulation.

2.8 Data Protection Officer

The Data Protection Officer's tasks are defined in Article 39(1). In summary, the Data Protection Officer will monitor the or- ganization's compliance with the GDPR, inform and advise the organization, collaborate with and be the contact point for the supervisory authority. All organizations do not need to hire a Data Protection Officer, but the organizations that meet one of the following criteria in Article 37(1) must hire a Data Protection Officer:

a) the processing is carried out by a public authority or body.

b) the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale Guide

c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions.

Article 37(5) requires the organization to hire the Data Protec- tion Officer on the basis of professional qualifications and, in particular, expertise in data protection legislation and practi- ces. In other words, the Data Protection Officer needs to have very good understanding of the GDPR and data protection. It is permissible to hire someone from within or outside of the organization as a Data Protection Officer. It is, however, essen- tial that there is no conflict of interest, i.e., the Data Protection Officer may not be the CEO, CTO or CIO.

2.9 Personal data breach

The regulation has the following definition of a personal data breach:

"'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Article 4(12))

This could, e.g., be a hacker attack where personal data has been stolen, changed or made unavailable. Here it is important to have procedures in place so that those responsible can respond quickly and correctly. A data protection policy should be implemented that includes a documented incident management process. Processors are obliged to inform controllers in the event of a personal data breach that occurs in their environment. Controllers may in turn be required to report personal data breaches to the supervisory authority and/or the affected data subjects.

When do controllers need to report personal data breaches to the supervisory authority?

The personal data breach must be reported to the supervisory authority if it is likely that the breach will endanger the rights and freedoms of the data subject. The responsible managers should consult each other immediately after the incident and determine if this is the case. In addition, the regulation requires that the controller reports to the supervisory authority ”without undue delay” and, if possible, no later than 72 hours after being informed of the breach. The breach report must include the information described in Article 33(3).

When must affected data subjects be informed?

The affected data subjects must be informed ”without undue delay” if the breach is likely to pose a high risk regarding rights and freedoms of the data subjects. The regulation basically states that for very serious breaches, a breach report must be sent to the supervisory authority and the affected data subjects must be informed. For serious breaches, just reporting the breach to the supervisory authority can some- times be sufficient. For less serious breaches, the Data Protec- tion Officer only needs to record the incident internally.

Article 34(3) contains circumstances when the affected data subjects do not need to be informed:

If the controller has implemented appropriate technical and organizational protection measures "that render the personal data unintelligible to any person who is not authorized to access it, such as encryption" then the affected data subjects need not be informed. This is one of the many benefits of usingpseudonymization.

2.10 Administrative fines

There is a great commotion about the notoriously large fines that the GDPR allows the supervisory authorities to issue. Many media outlets have been quick to point out that organizations can face fines up to 20,000,000 EUR or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In their urge to report this, most have forgotten to clarify that this is the maximum fine that regulatory authorities are allowed to issue. Since there are many conditions in the regulation that affect the size of the fine, it is not likely that an organization will need to pay the absolute maximum amount. The organization must have grossly neglected all of stated conditions in order to receive the maximum fine. Article 83(2) lists the conditions and they are many, for example, the supervisory authority will take into account: the nature, gravity, duration, number of data subjects affected and the level of damage suffered by them, the degree of cooperation with the supervisory authority and the intentional or negligent character of the infringement, only to name a few.

The administrative fines have been assigned two different levels:

Level 1: Maximum fine up to 10,000,000 EUR or up to 2% of the total worldwide annual turnover, whichever is higher.

As a general rule, violations concerning controller or processor obligations will impose fines at the first level. This includes Articles 8, 11, 25-39, 42 and 43. These violations include: data protection by design and by default, records of processing activities and notification of a personal data breach to the supervisory authority.

Level 2: Maximum fine up to 20,000,000 EUR or up to 4% of the total worldwide annual turnover, whichever is higher.

The largest fines will be issued to organizations that violate the rights of the data subject (Articles 12-22), lawfulness of processing (Article 6), basic principles (Article 5), conditions for consent (Article 7), processing of special categories of personal data (Article 9), transfer of personal data to third countries (44-49).

Organizations do not only risk administrative fines for potential violations, the regulation gives data subjects a right to claim compensation for suffering caused as a consequence of the organization's violation. In other words, the organization can be sued. The regulation also gives data subjects a right to invoke class action lawsuits, making it easier for large groups of affected data subjects to receive monetary compensation.

2.11 Exceptions

Not all processing of personal data is covered by the regulation. These are the exceptions:

Processing of personal data for private purposes:

Processing of personal data in the private sphere is not covered by the regulation, e.g., a birthday party list containing personal data about attendees is not covered by the regulation. On the other hand, all processing done in the context of the professional sphere is covered by the regulation.

Freedom of expression and freedom of press:

Processing for journalistic purposes and academic, artistic or literary expression, are exempt from all chapters in the regulation, except chapter 8 (remedies, liability and penalties).

3. Lawfulness of processing

Before the organization can process personal data, there must be a legal basis for the processing. There is a lot of misunderstanding concerning the extent to which GDPR will require consent from data subjects. Many believe that consent will be required for all processing of personal data. This is incorrect, since there are many other legal bases to justify the processing of personal data. Many controllers use consent when it isn't really needed, as a sort of safe haven when they are not really sure what to do. If the organization does not utilize the correct legal basis, their processing may not be lawful.

The following section goes through Article 6(1) and describes all the different legal bases for processing personal data:

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Even though consent it mentioned first in the regulation, it should generally be the last legal basis that the controller considers. The downside with consent is that it will require a clear, affirmative action by the data subject, can be withdrawn at any time, and it is not valid if the imbalance of power is too great between the data subject and the one requesting consent, e.g., between employer and employee. This means that consent is not valid if the data subject is pressured to consent or can suffer negative consequences for refusing to consent. There must always be a way to revoke consent for it to be valid. A person cannot consent to the pro- cessing of another individual's personal data, although there are some minor exceptions, for example when parents provi- de consent for their children.

As mentioned previously, consent requires a clear, affirmative action from the data subject. Silence or pre-ticked boxes do not constitute valid consent. For example, consent is valid if the data subject ticks a box with a text in close proximity that states: "By ticking the box you agree to our terms and have read our Privacy Policy (link)". This example illustrates what the regulation calls explicit consent. Explicit consent can sometimes provide the controller with a legal basis for sensitive processing.

Consent does not have to be explicit when processing non-sensitive personal data; implied consent is not explicitly granted by a person, but rather implicitly granted by a person's actions and the facts and circumstances of a particular situation. For example, if a data subject visits a company and writes his name and title into the 'visitor computer,' he implicitly gives consent to the company to send this information to the person that he wants to meet.

b) 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.

A typical example is an employment contract. An employer can legally process personal data from its employees if the processing is relevant to fulfill the terms of the employment contract. This means that employers do not have to run around and obtain consent from employees when GDPR is put into practice.

c) processing is necessary for compliance with a legal obligation to which the controller is subject.

Organizations have other legal obligations apart from the GDPR, e.g., accounting laws require the organization to store personal data for a certain amount of time. The organization can utilize this legal basis for legal obligations that supersede the GDPR.

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

In the Data Protection Directive, it was standard for many public authorities to use the 'legitimate interest' basis for their processing. However, this is no longer permissible.

f) processing is necessary for the purposes of the legitimate inte- rests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

In many cases an organization can justify their processing if the benefits of the processing outweigh the risk for the data subject. In recital (47), direct marketing is explicitly stated as a possible legitimate interest. This means that direct marketing can be used without consent in certain cases.

4. Principles relating to processing of personal data

The regulation includes general principles relating to processing of personal data in Article 5. The message from these principles permeates the entire regulation and violating these principles can lead to the largest fines.

4.1 Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

It may appear obvious that personal data shall be processed lawfully, but it means that the processing needs a legal basis from Article 6. Fair processing means that personal data is not processed in ways that have unjustified adverse effects on the individuals concerned or that it is collected using misleading tactics. Transparency means that the organization has to be open to stakeholders about its processing, e.g., it should be clearly stated in a Privacy Policy which personal data that is processed, how it is processed and for what purpose. The principle of transparency requires that any information and communication relating to the processing of personal data is easily accessible and easy to understand, and that clear and plain language is used.

4.2 Purpose limitation

The purpose limitation contains two parts:

1) Personal data must be collected for specified, explicit and legitimate purposes:

Specified and explicit purpose means that the purpose may not be too vague or unspecific, e.g., the phrase ”We collect the information for marketing purposes” is not sufficiently specific or explicitly stated. Legitimate purpose refers to one of the legal grounds in Article 6.

2) Personal data may not be processed in a manner that is incompatible with the original purpose.

If the organization has collected personal data for a particular purpose, they cannot process the personal data for another purpose incompatible with the original purpose at a later time. What does ”incompatible” mean in this context? It is discussed in recital (50). In summary, these criteria should be taken into account for the new purpose to be compatible with the original:

The link between the original purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expecta- tions of data subjects; nature of the personal data; the consequ- ences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operation.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, is not considered to be incompatible with the initial purposes as stated in article 5(1).

Example:

A company owns an e-commerce website that sells organic food that is delivered to customers once a week. For this purpose, the company processes cardholder data, shipping addresses and email addresses of customers. So far the processing is legal. The personal data is only processed because it is necessary for the service to be completed. At a later time, the company decides to send information via email to each customer about a big sale of organic food. This is arguably legal, there is a clear link between the original purpose and the new purpose and the customer should not be unpleasantly surprised about the new sale offer. The company then archives the personal data for statistical purposes. This is also legal, but it needs to be pseudonymized and the cardholder data can't be archived.

4.3 Data minimization

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed Organizations shall not process more personal data than is necessary to fulfill a specific purpose and it is not allowed to process personal data that is not relevant to a specific pur- pose. For example, some organizations store personal data thinking that it might be useful in the indefinite future; this violates the principle.

4.4 Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

There are obvious risks to data subjects if inaccurate personal data is being processed. For an insurance company, it may mean that a customer receives an incorrect insurance premi- um. Personal data must therefore be accurate and kept up to date. According to article 5(1), ”every reasonable step must be taken” to rectify or remove inaccurate personal data.

4.5 Storage limitation

Personal data shall not be kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.

When personal data is no longer necessary for the original purpose for which it was collected, it should be deleted. There must be a review process in place for removing personal data. Time periods for which personal data can be retained until it is removed shall also be documented if possible. As mentioned, one can archive personal data for, e.g., statistical purposes if it is stored in a pseudonymized form. Instead of deleting personal data, it can be anonymized. If the organiza- tion stores personal data from old customers in the systems, where the purpose of the processing is no longer relevant, it must be deleted.

4.6 Integrity and confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Integrity and confidentiality are two cornerstones in information security. Integrity means that only authorized persons can change personal data; write permission. Confidentiality means that only authorized persons can view personal data; read permission. ”Appropriate technical or organizational measures” include access control, log management, physical security, firewalls, antivirus, data protection policy, pseudonymization, etc.

4.7 Accountability

The controller shall be responsible for, and be able to demonstrate compliance with above mentioned principles.

Demonstrating compliance will require documentation, assessments and in some cases the hiring of a Data Protection Officer. Article 30 requires the organization to maintain records of processing activities. A Privacy Policy and a data protection policy should be implemented. A Privacy Policy is a document addressed to external stakeholders in order to inform them how and why personal data is processed. A data protection policy contains documented requirements and processes that everyone in the organization should know and adhere to.

5. Rights of the data subject

5.1 The right to be informed

Controllers are required to provide information to data subjects when collecting personal data from them. Article 13 lists all the information that needs to be provided; such as identity and contact details of the controller, the period for which the personal data will be stored, the purpose of the processing and the legal basis that is claimed. Keep in mind that the requirements are slightly different if the controller collects personal data directly from the data subjects or receives them from a third party.

5.2 The right of access

The data subject shall have the right to obtain confirmation from the controller as to whether or not personal data concerning him or her is being processed, and, if that is the case, access to the personal data. This means that the controller must implement processes for providing data subjects with copies of the personal data but also processes that ensures that it is the right owner of the personal data that requests the data. Article 15(1) requires the controller to also provide the data subject, inter alia, with the following information:

The purposes of the processing; the categories of personal data concerned; the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organizations; where possible, the envisaged period for which the personal data will be stored; the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.

If the controller shares personal data with other organizations, there is no need to name all organizations by name; it is enough to say which categories these organizations belong to, such as marketing companies or cloud service providers. The controller can not charge the data subject for access to the copy.

However, the controller can request payment feasible in relation to the administrative cost should the data subject repetitively request copies and it is unreasonable to provide a copy for free.

5.3 Right to rectification

The data subject has the right to obtain, “without undue delay”, the rectification of inaccurate personal data concerning him or her from the controller. This right is greatly connected to the principle of accuracy.

5.4 Right to erasure ('right to be forgotten')

The data subject is entitled to have his or her personal data deleted upon request "without undue delay" by the controller.

This is one of the most controversial parts of the regulation and has been given the nickname "the delete button". The right to erasure has caused quite the commotion in the IT world because systems are not really designed to properly delete personal data from databases. I would like to point out that organizations don't have to delete their backups in order to satisfy this right. There is a widespread misconcep- tion that it is enough to encrypt the personal data and then delete the key. This will not be enough, because encrypted personal data is categorized as pseudonymized personal data and is still covered by the regulation. Encrypted data follows a mathematical pattern and the key can be restored through brute force attacks that systematically check all pos- sible key combinations until the correct key is found. On the other hand, it is acceptable to anonymize personal data and thus fulfill the right to be forgotten. Controllers may also re- tain personal data for archiving purposes.

Article 17 lists conditions when the controller does NOT need or should delete personal data even if the data subject requests the deletion:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority;

c) for reasons of public interest in the area of public health.

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

e) for the establishment, exercise or defense of legal claims.

For example, there might be a legal claim where a customer owes the controller money for unpaid invoices. Then this customer cannot call and ask for their personal data to be deleted. Accounting law also requires that personal data remain stored for a certain period of time.

6. Checklist for the GDPR-compliance-project

The GDPR will require new organizational and technical mea- sures in your organization. The board of directors should initiate the GDPR compliance project and allocate responsibilities and the necessary resources. It is important that all relevant departments of the organization cooperate and pursue the same goal; this is NOT just an IT project that only concerns the IT department.

There are two sides of a GDPR compliance project:

1. The soft part – Management, documentation, policy, education, administration

2. The hard part – Technical measures

Soft Requirements:

1. A flow diagram of personal data should be created. The organization needs to know where, why, how and for how long personal data is stored, the flow of personal data, who can access it etc. Article 30 demands that the controller starts documenting processing activities and this document will give both the controller and the supervisory authority an overview of the processing.

2. Determine which legal basis from Article 6 the organization will utilize to justify the processing.

3. Determine if the organization complies with the principles from Article 5.

4. Determine whether the organization can ensure the rights of the data subject in chapter III of the regulation.

5. Determine if the organization needs to hire a Data Protection Officer. (Article 37)

6. Review and Update the processing agreements – Determine what your organization's GDPR obligations are those of your customers and service providers. The terms and the scope of the processing may need renegotiation, as well as potential penalties for violating the contract in light of the new administrative fines. (Article 28)

Hard Requirements:

1. Privacy by design – privacy protection should be incorporated into systems from the very beginning and permeate their entire life cycle.

2. Pseudonymization and encryption – Processing of sensitive personal data will require stronger privacy protection.

3. Erasure of personal data – Implement technical solutions for the removal of personal data.

4. Access control – Only employees with the assigned privileges shall have access to personal data. Distribute roles within the organization and assign relevant privileges.

5. Log management – Logs must provide adequate traceability. During a personal data breach, it is essential that the system can gather as much information and evidence as possible.

6. Penetration tests and vulnerability scans – penetration tests and vulnerability scans can map vulnerabilities in the systems.

7. Other technical measures – SNTP, hardening, monitoring systems, firewalls and antivirus.

Complior