PECB

BEYOND RECOGNITION

WHITEPAPER

GENERAL DATA PROTECTION REGULATION

GOVERNANCE, RISK AND COMPLIANCE

www.pecb.com

Principal Authors

- Eric LACHAPELLE, PECB
- Faton ALIU, PECB
- Donika MUÇOLLI, PECB

Contributors

- Henri Haenni, Abilene Advisors sàrl (Switzerland)
- Luc PERNET, Fidens (France)
- Joffrey GOUMET, Mielabelo Consulting (Belgium)
- Chris PAYNE, Advanced Cyber Solutions (United Kingdom)
- David SUPPLE, Barclays (United Kingdom)
- Taoufik SAMAKA, Telia Sverige (Sweden)
- Pierre GERODEZ, Devoteam (Belgium)
- Michel Boutin, In Fidem (Canada)
- David NUNN, trust-hub Ltd (United Kingdom)
- Taulanta KRYEZIU VITIA, PECB
- Artan MUSTAFA, PECB
- Arrita HASANI, PECB
- Endrita MUHAXHERI, PECB

CONTENT

INTRODUCTION

The European Union Directive 95/46/EC adopted in 1995 by the European Commission is an important component of the union wide privacy and human rights law. The directive is a set of rules implemented differently by each member state with the aim of individual data protection and data movement.

The General Data Protection Regulation will replace the Data Protection Directive and will be effective starting on 25th of May, 2018. This is occurring due to the European Commission aim at to unifying data protection laws across the union via one regulation such as the GDPR.

The EU parliament has approved the publication of the General Data Protection Regulation, proposed by the European Commission, for the protection of fundamental rights of natural persons with regard to processing of data.

The protection of personal and organizational data is ever crucial in a constantly growing cross border market environment. The General Data Protection Regulation requires safeguards and measures for protecting personal data, ensuring safe data processing and managing notifications of potential breaches. The need for safeguards and measures that enable security of personal data is expected to constantly increase; organizations are required to comply with the regulation to ensure protection of the fundamental rights and freedoms of the natural persons in regards to the processing of personal data.

GENERAL PROVISIONS OF THE GDPR

The GDPR objectives protect and provide control to natural persons over their personal data. Encouraging "The free movement of personal data" within Europe is a key objective of the GDPR. The GDPR clarifies the regulatory environment for international business by unifying the regulations within the EU. Further, the need for security is also a consequence of this objective.

The GDPR's fundamental conditions which organizations must follow when processing, collecting or managing a subject's personal data are categorized into six privacy principles:

1. **Lawfulness, fairness and transparency** – data subjects should be informed what data will be processed.
2. **Purpose limitations** – Data subject's data can only be used for the processing purpose for which the data subject is aware of. Without consent from the data subject, no further processing of data is allowed.
3. **Data minimization** – The GDPR specifies the amount of data that should be kept for processing.
4. **Accuracy** – The data subject shall have the right to obtain, without undue delay, the rectification of inaccurate personal data concerning him or her.
5. **Storage limitations**– The GPDR constraints the period of time for which personal data can be stored.
6. Integrity and confidentiality– The GDPR specifies that data must be protected against any unlawful or unauthorized processing, data loss or damage.

The GDPR applies to organizations collecting, processing and storing of EU citizen's personal data or EEA. This regulatory also applies to:

- Organizations with a physical presence in at least one-member state of the European Union.
-
- Organizations located outside of the EU, if they offer services, monitor or processes data subjects which belong in the European Union, even if the company location is not in the European Union.

There are special cases where the GDPR does not apply, such as: processing of personal data for national security activities or law enforcement (Law Enforcement Directive) or processing of data collected solely for personal purposes.

The GDPR introduces a set of definitions, which ease the understanding and responsibilities for the organizations affected by it.

Data subject

The data subject is a neutral person whose personal data processed by a processor or controller

Personal Data

Information that is an attribute or can directly/indirectly identify a data subject

Data Processor

The entity or individual that processes personal data on behalf of the data controller

Data Processing

Operation performed on data subject's personal data no matter if the data is processed automatically or not wholly automated

Profiling

The recording and analysis of data which is intended to evaluate Data Subject's behavior

Data Controller

The entity that determines the purpose of processing data subject's data

Personal Data Breach

refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, transmitted, stored, processed

DPO

The DPO is a person who will administer the organization's compliance with their data protection processing activities

Other definitions or more detailed information can be found in the official GDPR regulation.

Strategic Objectives of the GDPR

The General Data Protection Regulation sets out the:

- Establishment of data privacy as a fundamental right of natural persons
- Defining a baseline for data protection
- Defining responsibilities for the individuals involved in the processing of personal data and security of personal data
- Establish and ensure the effectiveness of the data protection principles
- Ensure the protection of the data subject's rights
- Ensure safe transfer of personal data in third countries or international organizations
- Ensure the implementation of the regulation and protection of personal data considered as a fundamental right

WHY GDPR?

The EU has the Data Protection Directive 95/46/EC (DPD) effective since 1995. The DPD regulates and protects the personal data within EU. The Directive allows continual processing of data, unless the data subject opposes the processing. On other hand, the GDPR requires organizations to establish reasonable evidence for processing data, capacities that prove that the processing of data is within their legal rights. Importantly, the GDPR is an enforceable law compared to the Data Protection Directive, thus preventing possible different interpretations within EU.

The growing trends of sharing/collecting of personal data on the internet, has resulted in huge amounts of data being stored by companies around the world. This introduced the need for stricter rules to constrain the usage of personal data, and was a burden for each member state of EU. Having each state interpreting the Data Protection based on their regulations, implied more complexity. Therefore, the European Commission decided to unify the regulation within EU, so when the GDPR is adopted it will replace the Data Protection Directive 95/46/EC.

One of the changes between DPD and the GDPR is the definition of personal data. In the EU, the Data Protection Directive of the personal data was defined as a person's: name, email address, any photo, bank account, or any identification number. In the GDPR, personal data is defined much broader; it includes Biometric-data (finger print), IP addresses, etc...

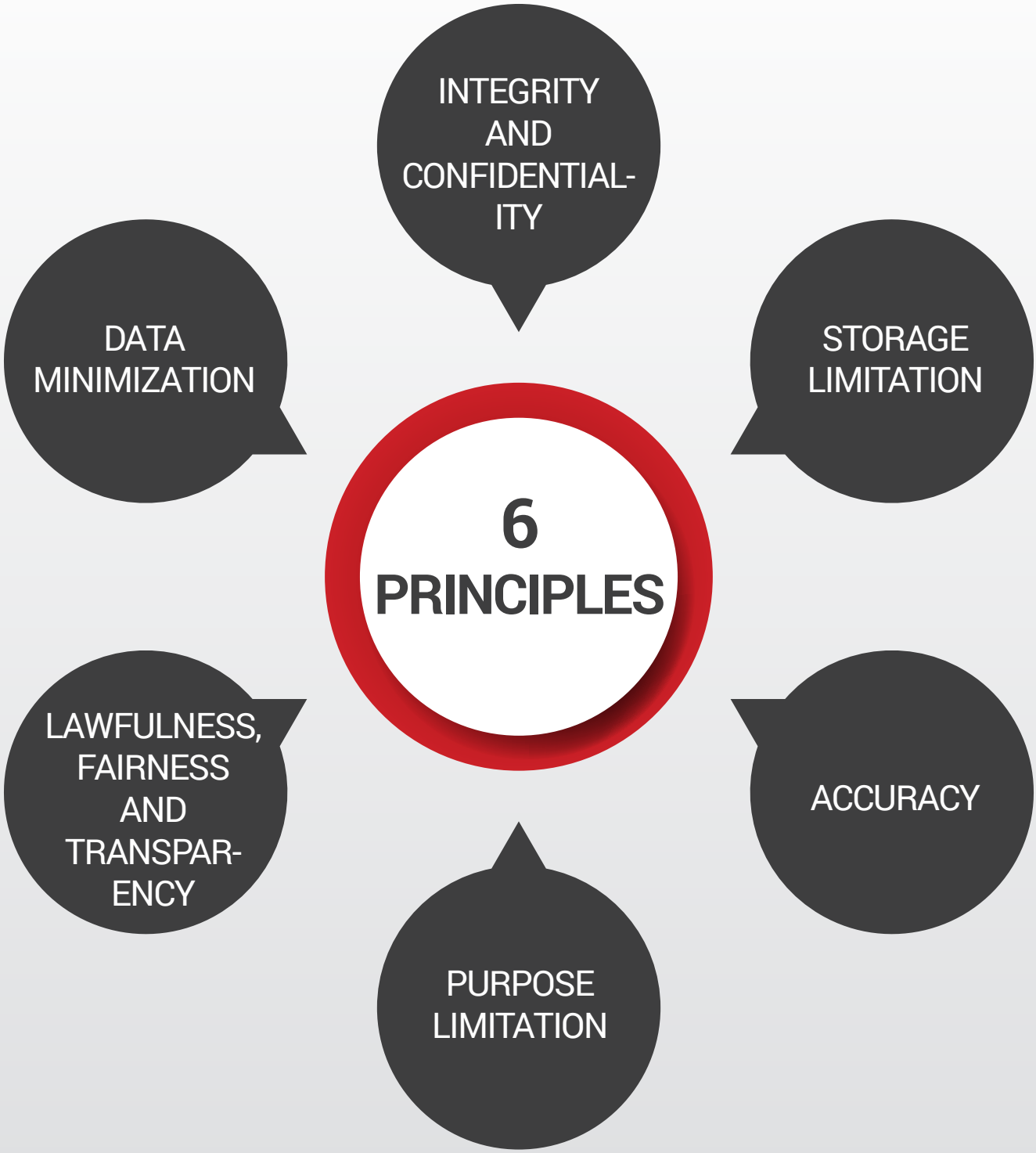
In contrast to the Directive, the GDPR does not exempt controllers from liability in case of an unavoidable accident.

Another difference is that the EU Data Protection Directive does not define what a data breach is; the GDPR includes a very broad definition:

A data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data protection principles

The General Data Protection Regulation provides six principles relating to the processing of personal data. The reason for providing such principles is to ensure that any processing of personal data is lawful and fair



1. Lawfulness, fairness and transparency

Transparency stands for: Informing the subject what type of data processing will be done.

Fair: The processed data must match with its description.

Lawful: Processing shall fulfil the described tests in the GDPR [article 5, clause 1(a)].

The principle of the lawfulness of processing indicates that processing of personal data shall be lawful only if and to the extent that at least one of the followings applies:

- If the data subject has given consent to the processing of his/her personal data for one or more specific purposes
- If processing is necessary for the performance of a contract to which the data subject is involved,
- If processing is necessary for compliance with a legal obligation to which the controller is subject,
- If processing is necessary in order to protect the vital interests of the data subject or of another natural person,
- If processing is necessary for the performance of a task carried out in the public interest, or
- If processing is necessary for the purpose of the legitimate interests pursued by the controller or 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.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

2. Purpose limitation

Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Personal data can be acquired only for the following: "specified, explicit and legitimate purposes" [article 5, clause 1(b)].

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.

Collected data on a subject shall be: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)].

In other words, only the minimum amount of data is to be kept for the purposes of specific processing.

4. Accuracy

Data shall be "accurate and where necessary kept up to date" [article 5, clause 1(d)]. Proper protection and measures against identity theft can be taken through baselining. Holders of data have to build processes for recertification into data management / archiving activities regarding the subject data.

5. Storage limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

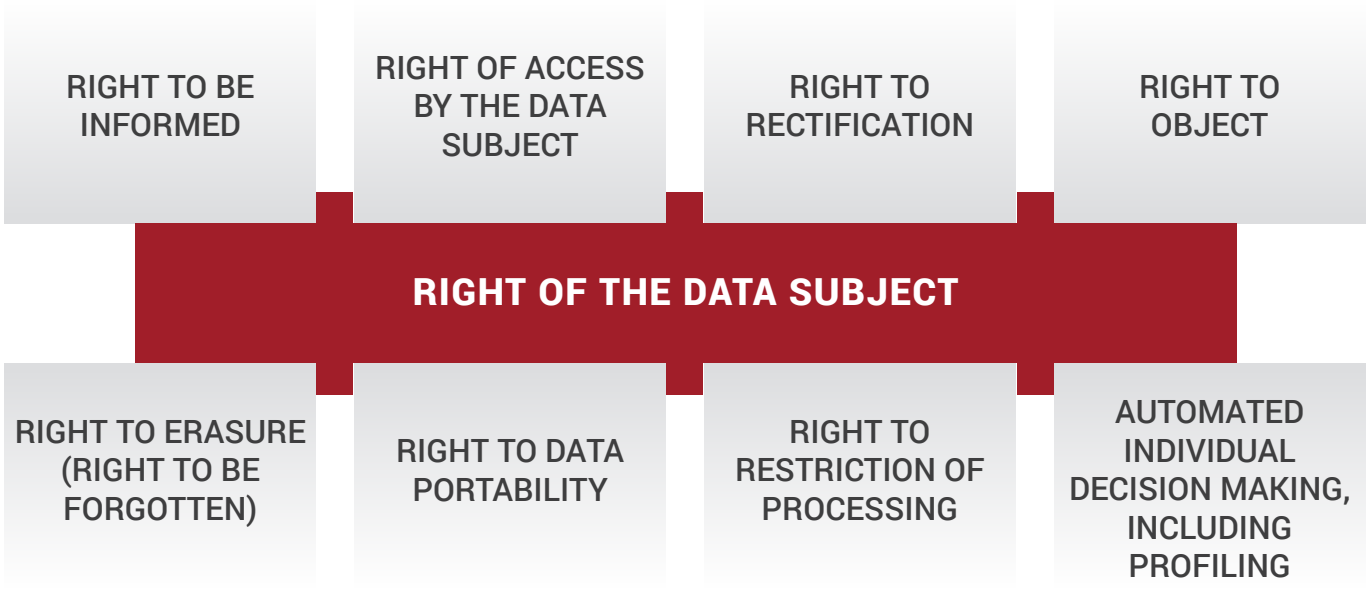
It is expected by the regulator that personal data is "kept in a form which permits identification of data subjects for no longer than necessary" [article 5, clause 1(e)]. To recap, the data that is no longer required should be deleted.

6. Integrity and confidentiality

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

Rights of the data subject

The General Data Protection Regulation has established rights for the data subjects including:



1. Right to be informed (Information and access to personal data)

The data subject has the right to be informed on how his/her data is being used. To respect transparency of personal data usage, the General Data Protection Regulation requires that "Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with information such as":

- The identity and the contact details of the controller
- The controllers representative
- The contact details of the person responsible for data protection.
- The purposes of the processing
- Legal basis for the processing

The controller is also required to provide the data subject with the necessary information, even when the personal data has not been obtained from the data subject.

2. Right of access by the data subject

This requirement enables the data subject to obtain confirmation from the controller as to whether or not personal data concerning him/her is being processed. The data subject's request must be completed within 30-days and the data controller cannot request payment of an administrative fee from the data subject. This is marked change from the Data Protection Directive which permitted 40-days and administrative fees.

Data subject access requests, according to the GDPR are entitled to an expanded set of categories of information. Therefore, organizations face a greater administrative burden as they are expected to handle these requests.

The right of access by the data subject enables the data subject to obtain from the controller confirmation as to whether or not personal data concerning him/her is being processed. Moreover, if the controller confirms that personal data is being processed, the data subject has the right to access the personal data and obtain information such as:

- The purposes and reasons of processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations
- 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;
- The right to lodge a complaint with a supervisory authority.

3. Right to rectification

The data subject shall have the right to obtain, from the controller, without undue delay, the rectification of inaccurate personal data concerning him or her. Moreover, this right enables the data subject to complete the incomplete personal data.

4. Right to erasure (right to be forgotten)

The right to erasure enables the data subject to obtain from the controller the erasure of personal data concerning him/her without undue delay. The controller is also required to erase the personal data of the data subject, if the personal data is no longer necessary in relation to the purposes for which they were collected or processed, if the data subject withdraws the consent on which the processing was based or if the personal data has been unlawfully processed.

5. Right to restriction of processing

The right to the restriction of processing indicates that the data subject has the right to obtain from the controller restriction of processing; this right is actuated if the accuracy of personal data is contested by the data subject until the controller verifies the accuracy of the personal data. Moreover, the data subject has the right to obtain restriction of processing, if the processing is unlawful. The data subject has the right to oppose the erasure of the personal data and request the restriction of their use instead.

6. Right to data portability

The right to data portability enables the data subject to receive his/her personal data which he/she has provided to a controller. Based on this right, the received personal data shall be structured in a machine-readable format. The data subject has the right to transmit personal data to another controller without any interruption from the controller to whom the personal data has been provided before.

This right allows data subjects to request an existing data controller to transmit personal data to another data controller. It does not have to be transmitted by the data subject. Mobile phone service providers and other utilities in Europe already have a system for this, whereby an entire account can be moved between companies via online forms. However, you are not required to adopt or maintain processing systems that are technically compatible with other organizations.

7. Right to object

The right to object enables the data subject to object at any time, the processing of his/her personal data. Therefore, the controller shall not process the objected personal data unless he/she demonstrates compelling legitimate grounds for the processing which override the interest, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

Moreover, the data subject has the right to object processing of his/her personal data, if the data is being processed for direct marketing purposes.

8. Automated individual decision making, including profiling

GDPR provides the data subject with the right to not be subject to a decision based only on automated processing, including profiling, which produces legal effects concerning the data subject (e.g. grocery store sale discounts, premium offers).

This requirement may become a worry for any organization which provides automated online quotes, for example insurance. These providers may have to change their quoting systems based on specific questions only about the conditions of driving/safety/etc.

Controller and processor

The controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Controllers play a crucial role for ensuring compliance with EU data protection law. The GDPR clearly defines how organizations should maintain lawfulness of their processing activities. The processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The processor and controller shall be liable and accountable for their roles and shall be held liable in case of a data breach as a result of the infringement of the regulation while processing personal data.

The controller and the processor shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing of data is performed in accordance with the General Data Protection Regulation. When implementing the technical and organizational measures, the controller shall take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The reason for implementing appropriate technical and organizational measures is to ensure that, by default, only personal data which is necessary to be processed, is processed. The GDPR recommends measuring all these through a risk assessment or DPIA (data privacy impact assessment). The main objective of Data Protection Impact Assessment is to support organizations in measuring the level of privacy. Thus, DPIA assist organizations in designing their systems with appropriate data protection levels. Basically DPIA can be considered as a risk-based tool to measure and review the privacy level and when mandatory, propose different design changes.

In the case of processing special categories, large quantities of personal data or in situations where processing could impact the rights and freedoms of data subjects, a DPIA is mandatory and could be requested in the event of a breach.

The General Data Protection Regulation sets requirements for joint controllers as well. Joint controllers are referred as two or more controllers that jointly determine the purposes and means of processing. They shall determine their responsibilities for compliance with the GDPR in a transparent manner.

In order for the processing to meet the requirements of the regulation and to ensure the protection of the rights and freedoms of the data subject, the controller shall use only processors that provide sufficient guarantees to implement technical and organizational measures. The processor shall have the authorization of the controller to process data or to engage another processor in processing. Meet certain conditions if the processor is not based in an EU/EEA member state. There is a list of friendly countries in which there are no restrictions, these countries are considered by the EU to have adequate or better data protection rules when compared to the GDPR. Processors based in a country not on this list can still process EU data subject personal data; however the rights and protections of data subjects must be guaranteed by a modal binding contract between data controller and processor.

Processing by a processor shall take place only if it is governed by a contract or other legal act under the Union or Member State. This contract shall have some specifications that shall be considered by the processor such as:

- Only act on the controller's documented instructions;
- Abide by the rules regarding international data transfers;
- Impose confidentiality obligations on all personnel who process the relevant data;
- Implement technical and organizational measures to ensure a level of security appropriate to the risk related to processing;
- Abide by the rules regarding appointment of sub-processors;

- Implement measures to assist the controller in complying with the rights of data subjects;
- Assist the controller in regards to activities that ensure security of processing e.g. data breach notification and data protection impact assessments;
- At the controller's decision, either return or destroy the personal data at the end of the relationship;
- Allow for and contribute to audits and inspections (including also an access to records of processing); and
- Provide the controller with all information necessary to demonstrate compliance with GDPR.

In order to keep track of the processing activities, GDPR requires the recording of these activities. The General Data Protection Regulation specifies that the record shall contain all of the following information:

1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
2. the purposes of the processing;
3. a description of the categories of data subjects and of the categories of personal data;
4. The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
5. Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
6. Where possible, the envisaged time limits for erasure of the different categories of data;
7. Where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

Each controller or controller's representative is required to maintain record of processing activities under its responsibility. Some of the information that shall be included in these records include the name and contact details of the controller, controller's representative and/or data protection officer, the purpose of the processing, categories of recipients to whom the personal data have been or will be disclosed including the recipients in third countries, categories of data subjects and categories of personal data.

Security of personal data

The General Data Protection Regulation requires the controller and the processor to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, by considering the cost of implementation, the nature, scope, context, purposes of processing and the likelihood and severity of the rights and freedoms of natural persons. The technical and organizational measures recommended to ensure the security of personal data include pseudonymisation through encryption of personal data. Implemented measures shall have the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in the event of a physical and technical incident. GDPR encourages use of the state-of-the-art technology to protect against latest threats. In order to ensure the security of the processing, the controller and the processor shall set in place a system for regularly testing, assessing and evaluating the effectiveness of technical and organization measures.

The controller and the processor can face different risks while processing. Therefore, when assessing the level of security, they shall consider the risks that have been faced or might be faced in the future processing activities. Some of the risks include the accidental or unlawful destruction of data, loss of data, alteration of data and unauthorized disclosure of, or access to transmitted, stored or processed personal data.

GDPR requires the controller and the processor to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk identified, assessed and evaluated previously. Some of the measures are: Privacy Impact Assessment (PIA) to assess risk related to the acidity and the processor, Data Protection Impact Assessment, DPIA (in case of high risk processing (special category of personal data)).

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

The General Data Protection Regulation has unquestionably enhanced the necessity for a holistic review of security strategies. The information security management system aims to not only protect the companies against technological malfunctions, but also prevent security issues that arise due to a lack of staff awareness.

ISO 27001, as the international standard on information security management, is employed to encompass three main security related aspects, namely:

- People - Given that data security is the responsibility of every person who is part of an organization, it is essential that all people are educated on data protection. Executive, users, developers should all be part of the solution, and attempts should be made to create a culture of security and design within the organization.
- Processes - Security and business processes should be subject to regular reviews for applicability. Such reviews should consist of a careful look on data collection, information flows, processing, and storage, because by doing so the scope of the problem is better understood.
- Technology - Individuals establishing an effective security strategy, in compliance with the requirements of the GDPR, should review their current technology strategies. Additionally, determine whether the technologies in place deliver the effectiveness needed to deal with new threats.

Everyday business dynamics require a recovery plan that is adaptable to specific conditions of the organization. The establishment of a business continuity plan yields several benefits, such as:

- Improved reputation
- Improved competitiveness
- Recognized commitment to maintain productivity and meet customer demands regardless of operational difficulties
- Enhanced profitability
- Lower financial volatility
- Enhanced customer trust and confidence

GDPR encourages the implementation of ISO/IEC 27001 as an approach to ensure easier GDPR compliance. The ISO/IEC 27001 certification supports organizations in creating better business efficiency, safeguards the valuable assets such as personal data, protects staff and organization's reputation, and simultaneously facilitates the attainment of compliance objectives. Some of the GDPR requirements are not directly covered in ISO/IEC 27001; however, ISO/IEC 27001 provides the means to push you one step closer to accomplishing conformity to the regulation. If you already have an ISO/IEC 27001 framework in place, you will not face duplication of effort, cost and time to comply with GDPR requirements.

GDPR puts a requirement on all companies to have effective business continuity plans in place. ISO 22301 defines the business continuity requirements and provides recommendations on how to address them, and how to develop procedures to manage disruptive incidents.

Notification of a personal data breach to the supervisory authority

The processor shall notify the controller in case personal data has been breached, without undue delay. Then, the controller is obliged to notify the personal data breach to the supervisory authorities, without undue delay, not later than 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the natural person. In case the supervisory authority has not been notified within 72 hours, the controller shall state the reasons for providing the information later that requested.

Both Controllers and Processors must have in place a form of incident management in order to understand, respond and control a breach; otherwise they cannot make the risk determination about the breach and notification to data subjects.

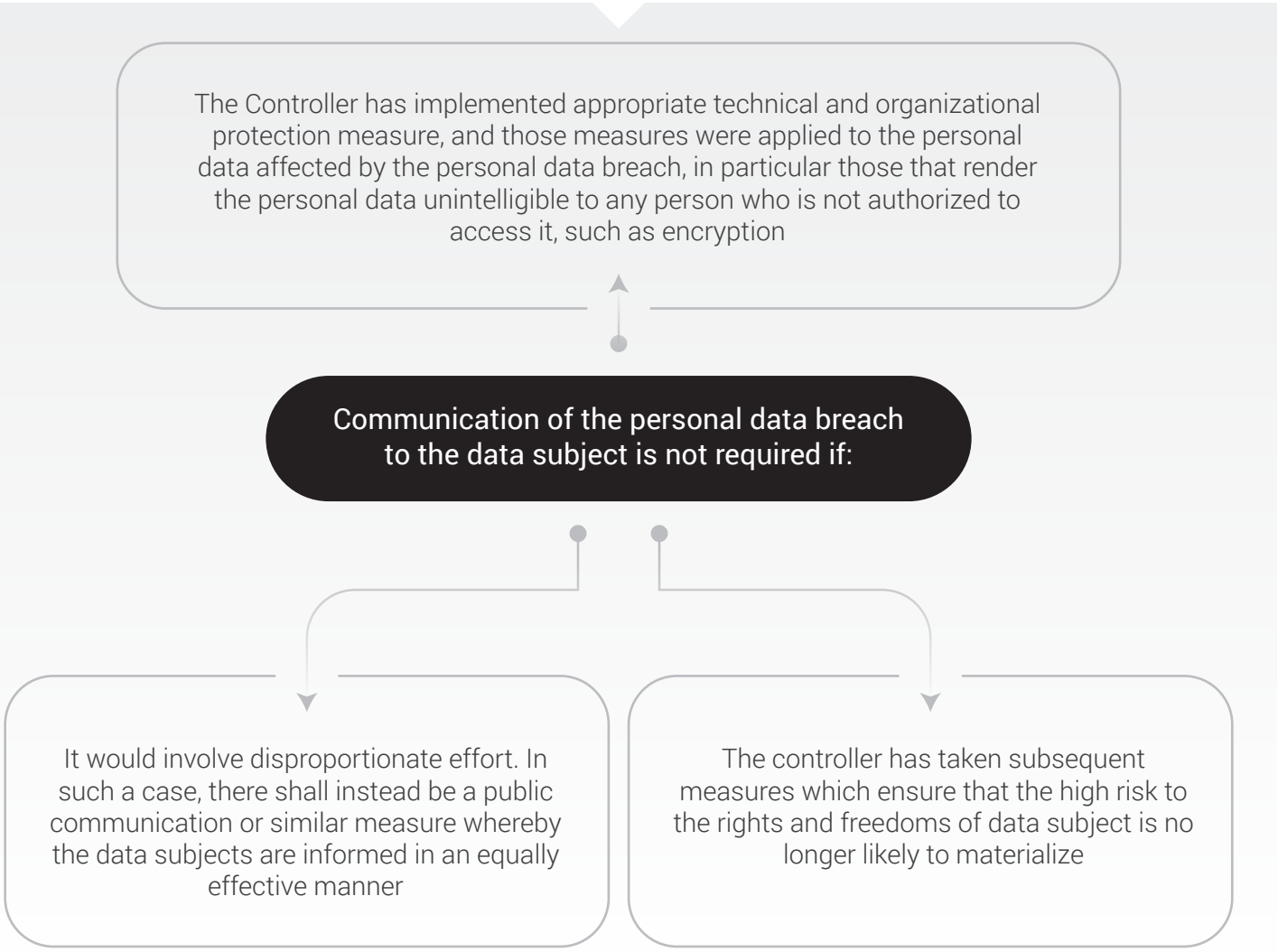
NOTIFICATION OF A PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The controller should communicate to the data subject the occurrence of a personal data breach, without delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions.

The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects.

This requirement extends a significant load on organizations, especially for those that have to process large amounts of personal data. Because they will need to make significant investments in order to properly inform data subjects in case of a personal data breach (e.g. if data subject's credit card details have leaked, the organization is responsible for notifying all affected data subjects to replace their credit cards).



Data Protection Officer

The General Data Protection regulation requires the designation of a data protection officer by the controller and the processor if:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- 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 and offences
- The organization has over 250 employees

The DPO can be:

- An existing internal employee but that employee's current roles and tasks must not impact their ability to be a DPO.
- Someone who is has expert knowledge of data privacy and protection.
- DPOs can be shared amongst organizations or bodies of organizations

After assigning a data protection officer, the controller and the processor shall ensure that the data protection officer is involved properly and in a timely manner, in all issues which relate to the protection of personal data. DPOs must report to the highest levels of management and the board. According to GDPR, the assigned data protection officer shall at least have tasks such as:

- **Informing and advising the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions**
- **Monitoring compliance with the GDPR**
- **Providing advice where requests as regards the Data Protection Impact Assessment and monitor its performance**
- **Cooperating with the supervisory authority**
- **Act as the contact point for the supervisory authority on issues related to processing**

The controller and the processor shall support the data protection officer in performing the above mentioned tasks.

Transfers of personal data to third countries or international organizations

The General Data Protection Regulation sets requirements on what should be considered when assessing the adequacy level of protection when transferring personal data to third countries or international organizations.

If a particular third country has requested to receive certain data, the transfer of such data can be conducted without the obtainment of any authorization, for as long as the Commission has concluded that this country has in place an adequate level of data protection (Adequate Jurisdiction). The list of Adequate Jurisdictions include: Andorra, Argentina, Canada (for organizations that are subject to Canada's PIPEDA law), Switzerland, the Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, and Uruguay.

Some of the elements that shall be considered when assessing the adequacy level of protection, provided by the GDPR, include:

- The rule of law
- Respect for human rights and fundamental freedoms
- National security, criminal law and the access of public authorities to personal data
- Data protection rules
- Existence and effective functioning of one or more independent supervisory authorities
- Ensure if the implementation of data protection rules are enforced and effective in the third country or international organization

It is possible that the Adequate Jurisdiction conditions may be subject to change, and as a result the jurisdiction no longer assures proper data protection. Consequently, the decisions taken by the Commission should be evaluated and reviewed periodically. By taking into consideration the potential developments, reviews are conducted at least every four years.

International cooperation for the protection of personal data

According to GDPR, the supervisory authorities and the Commission shall take appropriate steps to:

- Develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data
- Provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms
- Engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data
- Promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries

Remedies, liabilities and penalties

Right to lodge a complaint with a supervisory authority

The General Data Protection Regulation enables each data subject to lodge a complaint with a supervisory authority if he/she considers that the processing of his/her personal data infringes the regulation.

This requirement allows for the clarification that data subjects can lodge a complaint to different DPAs depending on their location or where the infringement happened. Yet, this does not mean that the DPA which received the complaint will directly deal with the pertinent data controller.

Right to an effective judicial remedy against a supervisory authority

The General Data Protection Regulation gives each data subject, without prejudice to administrative or non-judicial remedy, the right to an effective judicial remedy against a legally binding decision of supervisory authority concerning them.

Moreover, all processing against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority has been established.

Right to an effective judicial remedy against a controller or processor

The General Data Protection Regulation gives each data subject, without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, the right to an effective judicial remedy where he/she considers that his/her rights have been infringed because the processing of personal data did not comply with the GDPR.

Any proceeding against a controller or a processor shall be brought to courts of the Member States where the controller or the processor has an establishment. Moreover, such proceeding can be brought to courts of the Member States where the data subject has his/her residence unless the controller or processor is a public authority of the Member State.

Right to compensation and liability

The GDPR outlines that the controller and processor should be liable for the compensation to data subjects in incidents where unlawful processing of their personal data has occurred.

The data subject has the right to be provided with compensation from the controller or processor as the victim that has suffered harm as a result of unlawful processing of their personal data.

GDPR requires that any controller or processor involved in the processing that has caused damage as a result of non-compliance be held liable. If both the controller and the processor are responsible for the same damage suffered by the data subject, they are both required to ensure effective compensation to the data subject. The only way that the controller and the processor shall be exempt from liability is if they prove that they are not in any way responsible for the damage.

Imposing administrative fines

Supervisory authorities shall ensure that the imposition of administrative fines in case of non-compliance is effective, proportionate and dissuasive

for each individual case. These administrative fines depend on the circumstance of the case.

When deciding whether to impose an administrative fine and deciding the amount of the administrative fine (article 83) due regard shall be given to the nature, gravity and duration of the infringement taking into account the nature of the scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them. Moreover, due regard shall be given to the intention of the infringement, to the actions taken by the processor and the controller to mitigate the damage of the data subject and to categories of personal data affected by the infringement.

Infringement of the GDPR provisions can be up to 10 000 000 EUR, or in the case of an undertaking up to 2% of the total worldwide turnover of the preceding financial year. These fines apply if the following provisions have been infringed, and whichever is higher:

The obligations of the controller and the processor:

- Conditions applicable to child's consent in relation to information society services
- Processing which does not require identification
- Tasks of the data protection officer

The obligations of the certification body

- Certification
- Certification bodies

The obligations of the monitoring body

- Monitoring of approved codes of conduct

Infringement of the GDPR provisions can be up to 20 000 000 EUR, or in the case of an undertaking up to 4% of the total worldwide turnover of the preceding financial year. These fines apply if the following provisions have been infringed, and whichever is higher:

The basic principles for processing:

- Principles relating to processing of personal data
- Lawfulness of processing
- Conditions for consent
- Processing of special categories of personal data

The data subject rights:

- Transparent information, communication and modalities for the exercise of the rights of the data subject
- Information to be provided where personal data are collected from the data subject
- Information to be provided where personal data have not been obtained from the data subject
- Right of access by the data subject
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Right to data portability
- Right to object
- Automated individual decision-making including profiling

The transfer of personal data to a recipient in a third country or an international organization

- General principle for transfers
- Transfers on the basis of an adequacy decision
- Transfers subject to appropriate safeguards
- Biding corporate rules
- Transfers or disclosures not authorized by the Union law
- Derogations for specific situations

Any obligation related to delegated acts and implementing acts

- Exercise of the delegation
- Committee procedure

Noncompliance with an order or temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority or failure to provide access in violation

- Powers (ph. 1 and 2)

PECB

+1-844-426-7322

customer@pecb.com

Help Center

www.pecb.com