# Implementing privacy by design in practice

**Daniela Fábián Masoch**

March 25, 2019

**Table of contents**

# 1 Introduction

Data protection has become increasingly important in recent years. Not only have the EU and many countries around the world revised their data protection laws and introduced stricter rules to protect the rights of data subjects and significant sanctions for non-compliance with the law. The awareness and expectations of individuals, such as consumers, patients, employees, service providers and business partners, as well as public authorities, have also increased significantly. While until a few years ago data protection was hardly on the priority list of many companies and hardly any resources were spent on implementing the legal requirements, most companies have realized since the introduction of the EU General Data Protection Regulation (GDPR) that data protection is a serious issue.

The reason for the increased sensitivity to data protection is not only the threat of sanctions and the loss of reputation in the event of a breach of data protection regulations. Companies have understood that they can only take full advantage of new technologies such as Blockchain, Machine Learning, Artificial Intelligence, Internet of Things and Mobile Apps if they meet individuals' expectations, maintain their trust and respect their privacy. Today, data protection is no longer seen as just a compliance or information security issue, but as an essential factor in building and maintaining trust, competitiveness and success in the marketplace.

Organizations must know and foresee their risks and take appropriate measures to eliminate them, reduce them to an acceptable level or manage them. To this end, organizations must, first of all, know what personal data they store and process, in which business areas, in which systems and for what purposes. This knowledge is the fundamental prerequisite for active risk and data protection management.

Before processing personal data, companies must take into account the data protection aspects and principles as well as possible restrictions and risks in advance and take appropriate risk-minimizing measures. Such an assessment is necessary, for example, before the introduction of a new data-processing system or a health app or before the storage of particularly sensitive data in a cloud, the introduction of a monitoring system in the company or the outsourcing of data processing to a service provider in a country outside the EEA or Switzerland. With this approach, the company can not only ensure compliance with legal requirements, but also make strategic and operational decisions in advance and efficiently implement business processes. This can include, for example, storing data on servers in Switzerland instead of in the USA or purchasing software with integrated data protection principles. The company can also take the necessary steps to ensure that its privacy policies and applicable laws are implemented.

This procedure is nothing more than “privacy by design.”

# 2 Privacy by design: a new obligation for controllers

The EU General Data Protection Regulation (GDPR) has introduced a legal obligation for controllers referred to as “data protection by design and by default.” This principle requires the controller to implement appropriate technical and organizational measures designed to implement data protection principles into the processing of personal data in an effective manner. Failures to comply with this obligation are subject to significant fines following Art. 83 GDPR.

Further laws have introduced the concept of privacy by design, such as the Draft Swiss Federal Act on Data Protection, published on September 15, 2017 (D-FADP)[1] or the new Indian Personal Data Protection Bill which

[1] Art. 6.1, 2 D-FADP: Data Protection by Design: The controller must set up technical and organizational measures in order for the data processing to meet the data protection regulations and in particular the principles set out in Art. 5 (general principles of lawfulness, proportionality, purpose limitation, data minimization, transparency, retention, and quality). It considers this obligation from the planning of the processing.

The technical and organizational measures must be appropriate in particular with regard to the state of the art, the type and extent of processing, as well as the risks that the processing at hand poses to the personality and the fundamental rights of the data subjects.

was published in 2018.[2] The concept has further been introduced, although not explicitly, in the new Brazilian General Data Protection Law (Lei Geral de Proteção de Dados, LGPD) which will come into effect in early 2020.[3]

The concept of privacy by design is a fundamental requirement for the effective implementation of data protection. Privacy by design essentially requires controllers to take into account the privacy principles and requirements both, at the design stage of any IT system and technology, business practice, service or product and throughout the whole life cycle of the personal data, and to embed appropriate technical and organizational measures to implement the data protection requirements and to protect the rights of data subjects.

Although implementing data protection by design has become a new obligation under the GDPR, the concept is not new. It had existed for a long time as best practice and served as a practical approach to those organizations that had implemented data protection principles before the GDPR was even drafted.

The concept was already indirectly considered in EU Directive 95/46[4] and then introduced in 2009 as "Privacy by Design" by Ann Cavoukian, at that time the Information and Privacy Commissioner of Ontario, Canada, building on seven basic principles[5]:

1. **Be Proactive, not Reactive; Preventative not Remedial:** Being proactive and preventative anticipates and prevents privacy invasive events before they happen and privacy risks before they materialize.
2. **Privacy as the Default:** Privacy, in particular, transparency, data minimization, purpose limitation, confidentiality and data retention, is built into filing systems and business processes by default, automatically protecting personal data without the need for the data subjects to become active.
3. **Privacy Embedded into Design:** Privacy is embedded into the design and architecture of IT systems and business practices in a holistic and integrative way becoming an essential component of the core functionality being delivered. This means that privacy is integral to the system, without diminishing its functionality.
4. **Full Functionality – Positive-Sum, not Zero-Sum:** All legitimate interests and objectives, and not only the privacy goals, shall be accommodated without unnecessary trade-offs. Creative solutions shall be found that enable multifunctionality.
5. **End-to-End Security – Lifecycle Protection:** Personal data shall be secured, depending on their level of sensibility, from the collection throughout the entire lifecycle, by strong technical and organizational measures such as appropriate encryption, strong access controls and logging methods.
6. **Visibility and Transparency:** Visibility and transparency about the processing operations are essential to establishing accountability and trust.
7. **Respect for User Privacy:** The privacy of individuals should remain at the center of the interest and individuals should be offered measures such as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Art. 6.3 D-FADP: Data Protection by Default: The controller is additionally bound to ensure through appropriate predefined settings that the processing of the personal data is limited to the minimum required by the purpose, unless the data subject directs otherwise.

[2] Article 29 of the Personal Data Protection Bill, available here: https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

[3] Article 50 LGPD, unofficial English translation available here: http://portaldaprivacidade.com.br/wp-content/uploads/2018/08/LGPD-english-version.pdf

[4] Recital 46 Directive 95/46: Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected.

[5] Privacy by Design: The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices, from Ann Cavoukian, Ph.D.

Privacy by design was finally recognized by the 32nd International Conference of Data Protection and Privacy Commissioners in 2010 as "an essential component of fundamental privacy provisions[6]" and can also be found in various other documents, such as the FDPICs guide to technical and organizational measures for data protection of 2015.[7] A similar concept, "Security by Design" follows the same approach and can be found in standards such as ISO/IEC/27001.

By introducing the concept of privacy by design as a legal obligation, the legislator ultimately wants to make it clear that it is not enough to set standards, but that these standards must be implemented effectively and verifiably. The principle applies to the entire processing of personal data, whether in the development and implementation of new business processes, systems, services or products that process personal data in any way.

# 3 How to implement privacy by design in practice?

## 3.1 What does Article 25 GDPR say?

Article 25 GDPR describes the concept of privacy by design and covers the following questions:

- Who is obliged to implement privacy by design? The controller. Manufacturers of products and applications as well as service providers are only encouraged to consider privacy by design in recital 78 GDPR. In practice, however, manufacturers and service providers will have a keen interest in implementing the concept to remain competitive.
- What needs to be done? The controller must implement technical and organizational measures, so-called TOMs, such as the pseudonymization of personal data.
- How must the TOMs be? They must be adequate[8] and appropriate to implement data protection principles such as data minimization effectively and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR and to protect the rights of data subjects.
- When must TOMs be implemented? Both at the time of determining the means for processing and during the processing itself.

Article 25 GDPR does, however, not specify how this obligation is to be implemented in practice.

The mention of pseudonymization in Art. 25 GDPR can only be understood as an example of a technical measure. Further technical measures, such as access authorizations and restrictions, user authentication, access restrictions, encryption, logging, secure system configurations, protective measures against malware and data loss, physical protective measures, as well as a technical implementation of the right of objection and the correction or deletion of data or data portability must also be considered. Article 32 GDPR (and in Switzerland Art. 7 FADP) must be observed.

Furthermore, organizational measures must also be taken. These include, for example, policies, guidelines, instructions and manuals, records of processing activities, documentation of data breaches and data protection impact assessments, contracts with third parties and processors, training and controls, meaning all the elements that are necessary for a well-functioning data protection management system.

The technical and organizational measures must be suitable for implementing the data protection principles and safeguarding the rights of the data subjects, whereby data minimization is again only mentioned as one

[6] Resolution on privacy by design: https://icdppc.org/document-archive/adopted-resolutions/

[7] A Guide for technical and organizational measures, from The Federal Data Protection and Information Commissioner (FDPIC) published in August 2015, available here: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/dokumentation/guides/technical-and-organizational-measures.html

[8] Article 25.1 GDPR: "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing."

example. Of course, all other principles, such as lawfulness, transparency, confidentiality, purpose limitation, data integrity, storage duration and security, as well as the requirements concerning commissioned data processing and cross-border data transfers must also be taken into account.

## 3.2 How can Article 25 GDPR be implemented in practice?

One effective way to implement privacy by design in practice is to build a data management and risk assessment program with responsibilities and a process to identify systematically, evaluate, address and mitigate potential privacy and security risks associated with the collection and processing of personal data. The seven best practices principles described in Chapter 2 can serve as guidance for the implementation of data protection by design in the company. An effective data management and risk assessment program should include the following elements:

### 3.2.1 Data Protection Management System (Fig.1)

- A documented **commitment** by management to establish and enforce high standards of data protection for the company with the aim of integrating data protection into the corporate culture and embedding the data protection principles in the design and implementation of corporate policies, data protection management systems, business practices, services and products.
- The appointment of a data protection advisor and allocation of **responsibilities** at all levels of the organization, including management, business units and functions, for the effective implementation of data protection requirements.
- The establishment of a **data protection framework** with enforceable data protection policies and guidelines that attach appropriate importance to data protection and regulate the collection, processing, transfer, storage and deletion of data, as well as mechanisms to monitor implementation and compliance with standards and rules.
- The application of appropriate **processes** to ensure that data protection principles and requirements are adequately taken into account and integrated into data processing procedures and thus the principle of privacy by design is lived.
- The introduction of **records of processing activities.**
- **Risk management** with compliance checks and, where appropriate, data protection impact assessment.
- **Third-party management** and **data transfer governance**.
- Regular and documented awareness campaigns and performance of employee **training.**
- Regular and documented **monitoring and controls** through self-assessments and audits to verify the effective implementation of the data protection management program and compliance with legal requirements and internal policies and directives.

### 3.2.2 Processes

The processes, as mentioned above, include the following elements:

- The allocation of responsibilities in the relevant functions, such as Procurement, Legal and IT, which, as “gatekeepers,” ensure that the processes are adhered to.
- The identification of privacy risks relating to systems, websites, apps, business processes or products at the time of the design and throughout the lifecycle of the data, from collection to disposal.
- The documentation of the data processing activities (inventory).

- The performance of compliance and risk assessments and, where appropriate, DPIAs before personal data is collected and stored in systems, transferred or otherwise processed for business purposes of anticipating risks and adverse effects for the individuals concerned and to determine corrective actions.
- The implementation of the identified measures.

### 3.2.3 Risk Management

The conformity and risk assessment of data processing procedures is essential in the privacy by design process and answers questions such as:

- Is the purpose of the processing specifically described? How is it ensured that the data is not processed for other purposes?
- What is the legal basis for the processing of personal data? Is the consent of the data subjects required and, if so, how should it be obtained and documented? How can a withdrawal of consent be asserted and how is it handled and documented? If the controller has a legitimate business interest, were the interests of the controller weighed against the interests of the data subjects? Has this balancing test of interests been documented?
- Are all intended personal data necessary to fulfill the purpose or can specific data sets be omitted if necessary? Can the purpose also be accomplished with anonymous, pseudonymous or simply less data?
- Are the systems, websites, apps, business processes and products which store or process personal data, and which are developed or purchased by the company set up in such a way that only the necessary data for the purpose in question is stored and processed? How is the accuracy of the data ensured?
- Who should have access to which personal data and for what purposes? Is the group of people who should have access to the data defined and documented? Are these persons obliged to maintain confidentiality? How is access controlled and restricted?
- Have processors, if any, been audited to ensure that they can comply with data protection requirements?
- Are data processing agreements and other arrangements in place, where necessary, to govern the relationship with third parties?
- Is personal data accessed from abroad or transferred abroad? If so, have suitable legal measures been taken and documented to legitimize the data transfer? How are the measures implemented and compliance monitored?
- Are all necessary security measures planned and, if necessary, already implemented?
- What rights do the data subjects have? Are there any restrictions? How is it ensured that data subjects could exercise their rights effectively? Who is responsible for responding to data subjects requests? How are rights such as data portability, deletion or revocation of consent guaranteed?
- How long should personal data be stored and processed? Is there a retention and deletion concept?
- Are the data subjects informed about the processing of their personal data or is notice planned and how is it to be carried out? Is the data protection notice easily understandable and accessible?
- What technical and organizational measures are expected to secure the data and how are these measures to be implemented, verified and controlled?
- What security measures are taken to avoid security incidents? What is the process in the event of a security incident?

Fig.1


# 4 Conclusion

Consistent and sustainable compliance with data protection requires the strategic and conceptual integration of data protection principles in all business practices, in the organizational structure, in the development of rules, IT systems and products. It requires active cooperation between Business, Information Security / IT and Legal / Data Protection.

The concept privacy by design is not new and has been considered as best practice for years. New is the inclusion of the concept in the GDPR as a legal obligation for controllers, subject to sanctions if violated.

Privacy by design is, however, not only a legal obligation but also a fundamental prerequisite for the effective and sustainable implementation of data protection and the basis for a well-functioning data protection management.

**Daniela Fábián Masoch**
FABIAN PRIVACY LEGAL GmbH
Bäumleingasse 10, 4102 Basel, Switzerland
+41 61 544 44 01
daniela.fabian@privacylegal.ch
www.privacylegal.ch

Daniela is the founder and executive director of FABIAN PRIVACY LEGAL, a law firm specialized in international European and Swiss data protection laws, governance, legal compliance, risk management and program implementation. Daniela is an attorney at law, admitted to the bar in Switzerland, and a Certified Privacy Professional CIPP/E, CIPM, FIP with over 25 years of legal and practical experience in data protection, security and related matters. She advises multinational companies in a variety of sectors in the EU, Switzerland and the US in assessing, building and implementing privacy strategies, governance models and global privacy programs, with a pragmatic and commercial approach. Before commencing her own business in 2015, Daniela held various positions at Novartis, including the position of Global Head Data Privacy with the responsibility for setting the Group privacy strategic direction and for building, implementing and overseeing the global privacy function and group-wide privacy compliance program, including Binding Corporate Rules.