Chapter 18
EU GDPR: Toward a Regulatory Initiative for Deploying a Private Digital Era

Vasiliki Diamantopoulou, Costas Lambrinoudakis, Jennifer King, and Stefanos Gritzalis

Abstract Nowadays, people and enterprises put effort in protecting systems and applications that handle personal data and also in protecting digital footprints, and they realize that the concept of privacy protection is continuously evolving, depending on each environment. Admittedly, there is a plethora of digital products or services that necessitates the provision of personal data.

The GDPR came into effect to establish a more concrete framework for the protection of EU citizens' personal data. The impact of this regulation goes beyond the boundaries of EU in two ways. Firstly, the GDPR acts as a facilitator of non-EU enterprises that wish to do business and interact with EU citizens. Secondly, the GDPR, due to its wide applicability and generality, can be used as a basis and inspiration for other countries to establish their own data protection regulations and legal frameworks.

This chapter consists of guidance for organizations to be able to reach compliance with the GDPR, regarding the protection of the personal information they process. Also, this chapter presents the impact that the GDPR has brought to the global landscape, because of its wide territorial scope and the expanded approach of the various definitions of data protection concepts being used.

V. Diamantopoulou (✉)
Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece
e-mail: vdiamant@aegean.gr

C. Lambrinoudakis · S. Gritzalis
Department of Digital Systems, University of Piraeus, Piraeus, Greece
e-mail: clam@unipi.gr; sgritz@unipi.gr

J. King
Stanford Institute for Human-Centered Artificial Intelligence, Stanford University, Stanford, CA, USA
e-mail: kingjen@stanford.edu

B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy*,
https://doi.org/10.1007/978-3-030-82786-1_18

18.1 Introduction

The necessity of preserving individuals' privacy is becoming of utmost importance as technology advances [1, 2]. Organizations serving every sector must respect the personal data they process, demonstrating compliance with the corresponding regulatory schemas, according to the territory they act and to the individuals' origins. However, the concept of the protection of privacy is treated differently according to the specific context in which it is applied. The legal sector, like the Information Technologies (IT) sector, also has to deal with the problem of defining and dealing with the concept of personal data protection. The global landscape is changing step by step, developing regulatory frameworks aligned with the dramatically increased technological advances [3–5]. The European General Data Protection Regulation (GDPR) [6] is the "golden standard" in Data Protection Law globally, with various countries around the world implementing or amending local legislation in the areas of data protection and privacy, based on a core set of principles in common with the GDPR. We expect that the regulatory schemas around the world will contribute toward a harmonized addressing of the protection of personal data.

This chapter concerns both the scope of privacy protection and the policies and regulatory framework that ensure it. Personal data, which concerns every piece of information that is related to a natural person, has received increased attention lately, mainly regarding its protection. The level of protection that is demanded is determined by the type of processing applied to the data, its combination with other information, and by the environment in which it is used and evaluated. Today, the possibilities of collecting, processing, disseminating, and correlating the information generated by the information and communication systems in general- as well as the possibility of using, exchanging, and correlating the data collected for multiple and different purposes than those for which they were collected. This directly affects the life and communication of individuals, their personality, and their habits, and has also highlighted the qualitative dimension for the risks of natural persons. We are now aware that the increase in the processing capabilities of personal information is related inversely proportional to the ability of the person to supervise the use of information relating to them.

The issue of privacy is not a new matter of concern for the "Information Society," nor is it a unique one. It is related to the social environment; its size, structure, and nature; and the emergence of new social spaces and fields of activity of people [7, 8]. New communication technologies change the reality and the notion of "private" and "public." These new technological advances include the Internet of Things, behavioral marketing, the use of Big Data, and blockchain technology. In addition to the above, and to a much greater extent, the available communication and expression platforms offered through Web 2.0 have been enriched, with platforms such as social platforms, e-participation platforms, consultation sites, and more.

This chapter presents the impact that the GDPR has brought to the global landscape. In many cases (countries), it is obvious that the GDPR acts as an inspiration

for the development of other legal frameworks, being used as an international model, due to its wide territorial scope as well as the expanded definitions of data protection concepts (being used). From a business perspective, the GDPR has strengthened the control of the consumers over their data, adding rights that they can exercise to protect their personal data and helping in raising awareness on the use of this data. Also, the GDPR puts in place requirements for data controllers and data processors, such as data protection-by-design and data protection-by-default, implementation of appropriate technical and organizational controls that ensure the security of their information systems, and recording of processing activities, to name a few. Finally, the GDPR activates the "consent" that the data subject/consumer has to provide to the data controller in order for the latter to process the personal data of the first. All these requirements act as control elements for every data subject that is related to the EU. Consequently, organizations that act on a worldwide scale are enforced to apply all the privacy requirements enforced by the GDPR, making GDPR a facilitator for the protection of data subjects' personal data in a broader level of applicability.

This chapter aims at the analysis of privacy concerns from the legal perspective in order for organizations, private or public ones, to be able to be compliant with the GDPR, regarding the protection of the personal information they process. To this end, we proceed in the next sections with the analysis of the GDPR, and specifically, by focusing on the main changes of the regulation compared with the previous European Directive 95/46/EC [9], highlighting the major changes in the legal framework. Moreover, we provide a "to do list" describing ten discrete steps for compliance of data processors and data controllers who process EU citizens' personal data. Finally, we present the current status of the global legal perspective, emphasizing the influence of the GDPR to other legal frameworks around the world.

18.2 Data Protection in EU

To further government protection of individual privacy, more than 20 years ago, the European Union aligned data protection standards within the countries—Member States in order to facilitate cross-border data transfers internally in the EU. At that time, national data protection laws provided considerably different levels of protection and could not offer legal certainty neither for individuals nor for data controllers and processors. In 1995, the European Community therefore adopted Directive 95/46/EC [9] of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter, Data Protection Directive). The aim of this directive was the harmonization of the protection of fundamental rights of individuals with regard to data processing activities, ensuring, in parallel, the flow of personal data between EU Member States in a free and unobstructed way. However, the continuous growth and evolution of technology have taken place at such a pace that the existing legal frameworks had become obsolete, calling for an adaptation of the corresponding legislation. The GDPR that

replaces Directive 95/46/EC builds on the principles and rules of the pre-existing Directive, but it is differentiated in the volume of the enhancement of the rights of the Data Subjects, it appoints responsibility to the data controllers and processors for the protection of personal data they keep, by bringing forth the concept of self-regulation and accountability, and it increases the sanctions related to the violations of its provisions. Detailed analysis of the new concepts the GDRP brings is provided in Sect. 18.2.2.

In addition to the Data Protection Directive, the ePrivacy Directive 2002/58/EC provides data protection rules for telecommunications networks and internet services. This Directive is due to be repealed by the ePrivacy Regulation. The European Commission adopted a proposal for ePrivacy Regulation on 10 January 2017; it is currently under discussion in the European Parliament and the Council of the European Union. These Directives have emerged as necessary tools to use in the internal market in which goods, services, capital, and people should move freely.

18.2.1 General Data Protection Regulation (EU) 2016/679

The GDPR is a new regulation, which brings new obligations, new rights to the world formed by Information and Communication Technologies, and the globalization of information flows and services. The orientation of the Regulation is to support the security of personal data so that it can then support citizens' rights. It lays down the requirements for the protection of individuals with regard to the processing of personal data and the free movement of such data. It is mandatory for public and private organizations that manage personal data of European citizens. The aim is for citizens in the European Union to gain (more) control of their personal data.

18.2.2 Introduction of the New Concepts of the GDPR

The new Regulation is based on the concept of privacy as a fundamental human right [10, 11]. The EU's landmark in the evolution of its privacy framework is an attempt to change data controllers' and data processors' mentality about the uncontrolled processing of individuals' personal data they process. Additionally, the use of IS's for unknown (i.e. other than those clearly stated) purposes is a major problem for democracy in an information society. Consequently, the implementation of the GDPR is not tertiary, and it is of major importance for the citizens' own life; this orientation was given by the European Parliament.

Many of the concepts of the GDPR are not new ones but have their origin in the replaced Directive 95/46/EC. One of the main drivers of the new regulation can be considered the need for modernization. The use of new technological achievements has invaded individuals' lives and threaten their privacy. New or advanced online

services and technologies have been introduced, such as social networks, location-based services, cloud computing, data processing, and storage capabilities, to name a few. As an outcome of this technological invasion, decisions can be taken based on the automated processing of personal data, ignoring transparency and fairness. Another driver for the GDPR can be considered the control over individuals' personal data and the self-regulation of organizations, as an answer to the complexity of the previous regulatory environment (e.g. notification to several data protection authorities). Additionally, the territorial scope of the GDPR has changed, since its applicability concerns not only EU countries but every organization that processes EU residents' personal data. All these issues have been taken into consideration in the various articles of the GDPR, and appropriate actions are enforced in order to protect individuals' personalities.

In particular, the major breakthroughs of the GDPR are summarized in the following list:

- **Definition of Personal Data**. Additionally to the definition of personal data presented in Directive 95/46/EC which mentions that it is any information relating to an identified or identifiable natural person (i.e. the data subject), the GDPR has added *location data*, *an online identifier*, as well as factors specific to the *genetic identity* of a natural person, besides physical, physiological, mental, economic, cultural, or social identity, already included in Directive 95/46/EC.
- **Definition of Special Categories of Personal Data**. In special categories of personal data, GDPR includes the processing of *genetic data* and *biometric data for the purpose of uniquely identifying a natural person*, apart from personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation, already included in Directive 95/46/EC.
- **Data Controller's responsibilities**: The GDPR describes precisely the term of the data controller as well as its roles and responsibilities. Compared with Directive 95/46/EC, where they are the ones who must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, and unauthorized disclosure or access, the data controller shall now implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed taking 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*. Moreover, data controller shall implement appropriate data protection policies, in relation to processing activities.
- **Jurisdiction**: This point presents another dimension in the territorial scope of the application of the Regulation, since it applies, now, to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, *regardless of whether the processing takes place in the Union or not*. This requirement relates with processing regarding *the offering of goods or services, or the monitoring of their behavior as far as their*

behavior takes place within the Union. To this end, every organization around the world that processes personal data of EU citizens must comply with the GDPR, regardless of their place of establishment.

- **Consent Management**: The way the data subject is providing their consent to anyone asking to process their personal data has now changed: consent should be freely given, specific, informed, and unambiguous. Consent should be given *by a statement or by a clear affirmative action*. In this way, the data subjects are given the opportunity/ability to gain control over the management of their data, and the controllers can manage the provided consent as a proof for their legal processing. It is worth noting in this point that the consent should concern a specific data processing activity, clearly described to the data subject. If, for any reason, the data controller wishes to use a data subject's personal data for a different data processing activity, this should be described as a consent related to the new processing activity.
- **Breach notification**: In Directive 95/46/EC, there wasn't any reference regarding the notification of the supervisory authorities when a data breach occurs. The GDPR describes this process as an obligation assigned to the data controller, highlighting the short time period that they should react, by informing the supervisory authorities *without undue delay and, where feasible, not later than 72 h after having become aware of it*. Reference is also made to the notification of data subjects, if there is a risk for their rights and freedoms.

The GDPR does not introduce many substantially new concepts, but it increases the compliance requirements of data controllers and data processors. Moreover, this regulation encourages the use of certification schemes like ISO 27001 [12] to serve the purpose of demonstrating that the organization is actively managing its data security in line with international best practices.

18.2.3 Ten Steps for Compliance of Data Processors and Data Controllers

GDPR extends the scope of existing legislation to all EU or non-EU controllers who process personal data of citizens of the EU Member States and imposes compliance on a sufficiently rigorous legislative framework. With the enforcement of the Regulation, companies face new data protection obligations, as well as a reinforcement of pre-existing obligations under the GDPR. The very wide scope of application of the GDPR is based mainly on the intention to capture the challenges of the global economy, the new emerging technologies, and the new business models that organizations apply [13].

Moreover, the impending fines imposed by the GDPR have been significantly increased, reaching up to €20,000,000.00 or up to 4% of the total worldwide annual turnover (GDPR/Art. 83, Sec. 5) Thus, it is imperative for the companies to carefully

reorganize their internal data protection procedures in order to reach compliance with the GDPR [14].

The following ten steps can be considered as the basis to achieve compliance with the requirements of the regulation:

1. **Privacy awareness—readiness of the organization**. Probably this is the most critical point. Organizations should consider compliance with the GDPR as a systematic action, that is supported by appropriate for the needs, the volume, and the culture of the organization planning. In this step, focus should be given to the human resources of the organization as the success of it is based on the awareness that will have been achieved among the employees, the third parties, and any other associate of the organization. Moreover, organizations have to be prepared that the project of compliance with the GDPR is an ongoing process that potentially can increase the workload.

   - All business processes associated with personal data have to be assessed and potentially redesigned based on the preservation of individuals' privacy.
   - The organization should implement an organizational framework according to which there will be roles with responsibilities for the protection of personal data. The framework should include at least the roles of the data protection officer, the information systems' lead developer, the information technology (IT) manager, and the information systems auditor.
   - The organization should conduct an assessment of all important "gaps" related to the requirements of the GDPR, taking into account the required data protection policies, documentation, and implemented security measures.

2. **Develop and maintain Record of Processing Activities** The organization should recognize the processing purposes that it serves and all related processing activities, paying attention to the fact that many of them may not be immediately visible, such as document archive, staff file, customer file, electronic application files, contact files for communication purposes, security files-camera material, online access logs, etc. Each processing activity should be distinguished per processing purpose.
   Then the organization should explore whether there is an obligation to maintain a record of processing activities (GDPR/Art. 30), although it is certainly a good practice to do it. An obligation exists if the organization employs more than 250 persons or if processing poses a risk to the rights of the data subjects or if it involves special categories of personal data (i.e., "sensitive" data) or data relating to criminal convictions. The development of a comprehensive inventory of enterprise information resources (data inventory) and the implementation of an appropriate data classification scheme are proposed. The information to be kept includes:

   - Contact details of the Data Controller, its representative, and the appointed DPO-if any
   - The processing purposes

- A description of the categories of Data Subjects
- A description of the categories of personal data
- Whether the organization transfers data to non-EU countries
- The deletion deadline for each data category and the legal basis for this decision
- A general description of the technical and organizational security measures taken by the organization

3. **Designate a Data Protection Officer (DPO)** The obligation to designate a Data Protection Officer applies to:

   - All public authorities or bodies, except for courts acting in their judicial capacity (GDPR/Art. 37a). Examples of this category are ministries, hospitals, telecommunications, and transport.
   - Organizations that perform regular and systematic monitoring[1] of data subjects on a large scale (GDPR/Art. 37b). Examples of this category are security service providing companies, call centers, marketing companies, etc.
   - The core activities of the organization consist of large-scale processing of special data categories (GDPR/Art. 37c). Examples of this category are clinical studies companies and research centers.

   The senior management designates a Data Protection Officer, a competent person reporting directly to the senior management without receiving any instructions on how to perform their tasks as a Data Protection Officer. The senior management shall ensure that the Data Protection Officer is not dismissed or penalized for performing their tasks. The Data Protection Officer should have direct access to the senior management, and the data subjects of the personal data should have clear access to the Data Protection Officer. The Data Protection Officer may also have other responsibilities, but the organization ensures that no "conflict of interests" arises due to these additional professional duties and obligations. The Data Protection Officer is responsible for all matters relating to the protection of personal data in the organization. Therefore, he/she must have access to all databases and organization's systems. The Data Protection Officer is bound by terms of confidentiality.
   The role of the Data Protection Officer is to advice the data controller/processor, organize training/awareness programs, act as an internal auditor on personal data issues, and monitor compliance with legal requirements. Furthermore, the Data Protection Officer is the point of contact with the data protection authorities as well as with the data subjects.

[1] This activity can refer either to online monitoring, such as location tracking services, or processing that aims to define a particular behavior or the subject of the personal data for advertising purposes, such as behavioral advertising, and data subject's profiling based on specific personal data, such as identification of consumer identity, preferences, favorite stores (profiling).

The Data Protection Officer should have the following knowledge and skills:

- Specialized knowledge of the legal framework for the protection of personal data at national and European level.
- Basic knowledge of Information Security and Information Systems in order to be able to understand, design, and supervise the implementation of a personal data protection program.
- Communication skills and persuasion in order to be able to report directly to senior management and persuade them to support the compliance and personal data protection program.
- Appropriate experience to coordinate the internal team dealing with the personal data protection program, as the team leader.

The specialization level of the Data Protection Officer is not explicitly defined in the GDPR but it should be proportional to the risk level of the organization, as well as to the level of complexity of the organization's business processes and the volume of the processing of personal data.

The organization assigns to the Data Protection Officer the following responsibilities:

- To represent the organization vis-à-vis the authorities, national and European.
- To advise the senior management on data protection issues.
- To suggest the appropriate data protection policies directly to senior management.
- To monitor and harmonize the operation of the organization, when acting either as a Data Controller or as a Data Processor with regard to the policies, practices, and methodologies of processing, storing, and transferring personal data.
- To protect the organization when acting either as a Data Controller or as a Data Processor from the risks of getting penalized with the substantial and heavy administrative fines provided by the Regulation.
- To ensure the support of the senior management and the required budget for implementing the data protection program.
- To develop the data protection program and the data protection policy and supervise their implementation, to evaluate the degree of participation and success, and to make the necessary corrections where necessary.
- To establish an inventory of Personal Data categories that relates to the type of personal data, the way the data is stored and processed, the time allowed for their retention, and the methodology for deleting or destroying them.
- To assess and advise on a case-by-case basis for establishing a Data Protection Impact Assessment Method and performing Privacy Impact Assessment.
- To coordinate the interdepartmental collaboration with the Human Resources, Information Security, Information Systems, Legal and Regulatory Compliance, and Marketing and Procurement departments to

create a sustained corporate data protection culture as a valuable corporate asset.
- To design and implement internal training programs and maintain the required training completion records by department/group of employees.

Finally, the organizational structure of the organization should reflect the distinct role of the Data Protection Officer.

4. **Ensure consent of data subjects when necessary** The organization must record the legal basis for the processing of the data. When consent is the legal basis for the processing of personal data, it must be provided by the Data Subject. The data controller must be able to prove that:

   - They have obtained the consent of the data subjects.
   - The consent is "free."
   - The consent is specific and explicit for a well-defined processing purpose.
   - The consent has been obtained with a clear positive action (e.g., filling in a box when visiting a website, selecting desired technical settings for a service, etc.). Silence, pre-filled boxes, or inactivity should not be taken as consent.
   - For underage persons the consent is considered to be "valid" when the child is at least 16 years of age. Otherwise, consent must be given by the person who has parental responsibility.

   Prior to the consent process, the organization must inform the Data Subject, at least for all the essential elements of the processing:

   - The identity and contact details of the Data Controller
   - The identity and contact details of the Data Protection Officer
   - Third parties and recipients potentially involved in data processing
   - The purposes and legal basis of the processing
   - The period of data retention
   - The intention of cross-border transfer
   - The Data Subject's rights

   This information should be in visible form, easily accessible, and understandable so that the Data Subject has a real choice. Moreover, the consent procedure must be user-friendly to avoid ambiguities. The Data Subject must be able to withdraw its consent at any time. However, it must be ensured that the Data Subjects have access to their current status of consent at any time and can change their settings or withdraw their consent completely. So far, numerous fines have been imposed on various organizations across Europe and beyond, because of their inadequacy to prove that they have obtained the consent of the data subject in a free and unambiguous way.[2] For example, consent should not be requested via a document that also includes other matters (e.g., general Terms and Conditions) as this should be regarded as "blurring" the consent.

[2] https://gdpr-fines.inplp.com/list/.

An entity must be capable of providing a proof of validity of obtained consent, otherwise the legal requirement for GDPR compliance is not met [15].

5. **Apply privacy-by-design and privacy-by-default principles** The protection of personal data and privacy can be improved and enhanced by designing information systems in a way that reduces the degree of invasion in privacy. Privacy by design, or Data Protection by Design (GDPR/Art. 25), is an approach that requires the integration of the key protection parameters by the controller into existing wider project management and risk management methodologies and policies. GDPR provisions facilitate this direction by requiring controllers (companies, organizations, etc.) to ensure that the protection of users' privacy is a basic parameter in the early stages of each project and then throughout its life cycle [16, 17]. To achieve that it is important to consider issues like state-of-the-art technology developments, cost of implementing the protection measures, nature—scope—context and purposes of processing, and minimization of threats against the rights and freedoms of individuals from processing. In this area belong a series of methodological frameworks [18–22] and tools [19, 23–25] that help analysts, designers, and developers to develop IS's that privacy will be a built-in and not an add-on feature as it happens many times.
Privacy, in order to be included as a concept in the software development cycle, should be transformed into a technical requirement. Thus, during the development of new IT systems, the organization should identify technical ways for the protection of personal data. To this respect, the Information Systems Development Officer consults the Data Protection Officer and opts for a development method that supports the identification and modelling of data protection mechanisms during the analysis of the overall system's specifications prior to the implementation.
As far as the privacy by default approach, it requires to ensure that, by definition, only the personal data necessary for the specific purpose is processed, and at the same time it is necessary that the "default" settings of the applications be as privacy-friendly as possible.
Based on the above, the organization shall ensure, when procuring new systems, that appropriate technical ways for the protection of personal data are followed. The Information Systems' Lead Developer seeks advice from the Data Protection Officer and ensures that each procurement notice for a new IT system includes in the obligations of the contractor the identification and modelling of personal data protection standards and the integration of specifications into the new system during development. The organization's Information Systems vendors must demonstrate that they have applied the principles that the law requires in the solutions to be used by the organization. This requires special attention when recording specifications and evaluation criteria for the acquisition of a new Information System.

6. **Protect processing of personal data—conduct Data Protection Impact Assessment**
The organization must plan the protection of personal data, taking into account the risk of processing to the rights and freedoms of natural persons, and the nature, scope, context, and purposes of the processing. While Directive 95/46/EC implies the requirement for risk management procedures, GDPR clearly proposes the implementation of management processes that will facilitate the objective assessment of risks in order to determine whether the data processing operations involve a risk or a high risk for the natural persons (GDPR/Art. 35).
A data protection impact assessment, and hence, the criticality of data shall (in accordance with the GDPR) particularly be required in the case of:

- A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g., user profiling by web search activity monitoring for targeted advertising and promotion of products and services (hotels, restaurants, etc.))
- Processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10 (e.g., processing of patients' medical records (special category of personal data) from healthcare organizations, including medical history, illnesses, and patient care)
- A systematic monitoring of a publicly accessible area on a large scale (e.g., traffic monitoring for informing drivers of the fastest route, residence entries' monitoring, and public transport entrance)

The concept of risk management becomes even more clear in GDPR since it imposes the requirement for an impact assessment (when a type of processing, in particular using new technologies and taking into account nature, scope, context, and processing purposes, is likely to cause a high risk to the rights and freedoms of natural persons), a very risk-centric process.
In general, Impact Assessment is one of the most useful tools for identifying and assessing risks to privacy when a controller employs new technologies, products, or services. To this end, a variety of methodologies have been proposed, several of which are also included in the guidelines of the Article 29 Working Party [26]. However, data protection impact assessment processes are not included in most risk management standards, are often not embedded in an organization's broader risk management framework, and are even less relevant to an organization's internal business processes [27]. Taking into account the systems' and threats' continuous evolution, risk management "necessitates" the identification of appropriate controls. The processing of personal data, hierarchy, and the management of risks have to be examined in a way that optimizes the cost and contributes to the most suitable decision-making, aiming at protecting personal data. Impact assessment contributes to the application of

privacy principles, in a way that the data subjects are able to preserve control of their personal data.

An integrated risk management process should support the ability to control and limit the risk at all levels, while assessing how the impact of a specific risk compares with the consequences that may be caused by some other risk. Risk management, in the framework of privacy protection, can have many common elements with risk management for the protection of personal data in an organization (e.g., security, information systems, etc.). Their successful combination allows optimization of resources (human and technical) and better risk management [28].

The Data Protection Impact Assessment (DPIA) should provide:

- A systematic description of the processing activities envisaged, the purposes of the processing and its legal basis
- An assessment of the necessity and proportionality of the processing activities
- A risk assessment on the rights and freedoms of data subjects
- The anticipated risk mitigation measures

while in terms of the protection (security) of the processing activities it is necessary for the organization to propose the appropriate/suitable technical and organizational measures. Indicatively:

– Pseudo-anonymization and encryption
– Ensuring privacy, integrity, availability, and reliability
– Restoration of availability and access in the event of an incident
– Testing, assessing, and continually evaluating the effectiveness of the protection measures

7. **Develop Data Protection Policy** Organizations need to update/enhance their data protection policies in relation to the existing legal framework. The data protection policy generally includes the purpose and the objectives set by the management with regard to the protection of personal data, as well as the instructions, procedures, rules, roles, and responsibilities related to the protection of such data. The implementation of the data protection policy is binding for all employees and associates of the organization. This means that compliance with the procedures and directives it provides is mandatory for all employees and associates of the organization directly or indirectly involved in the operational processes involving the processing of personal data. With the help of the data protection policy, the organization seeks to achieve the following goals:

- The protection of natural persons whose personal data is processed by the organization.
- The identification of the risks involved in the processing of personal data by the organization.

- The implementation of rules and techniques in order to satisfy the legitimate rights of the natural persons whose personal data is processed by the organization.
- The compliance with the requirements set by the European and national legal framework.

The data protection policy attempts to define commonly accepted principles, ways, and responsibilities governing the processing of personal data. The data protection policy is not only about technical or organizational issues, but it treats both categories with the same attention.
A data protection policy should provide information on:

- The legal basis for the processing (which "complicates" the information as it requires legal analysis)
- The time frame that the processing/storage will take place
- The existence of any automated decision-making process, including profiling, with information on possible consequences
- Data collected from other sources
- The Data Protection Officer's data
- The procedures employed in order to satisfy all data subjects' rights

The data protection policy is not a static document but should be kept as up to date as possible and adjusted in line with the changes of IS and the technical and social environment. It is also updated in the event of major changes to the organization or its IT systems.

8. **Data breach** The organization is considered as being aware of a data breach after it is has been confirmed that an event that results in undermining of personal data has occurred. The timely detection and evaluation of a data breach incident are extremely crucial. It should be noted that the Data Controller is considered aware of the breach only after the initial investigation of the event (which must begin as soon as possible) and upon its classification as an incident. Whether it is immediately clear that personal data is at stake or whether this conclusion takes some time to achieve, emphasis must be given to direct action to investigate the incident in order to determine whether there has actually been a violation of personal data. As soon as the short investigation period has passed, and the Data Controller has confirmed the incident, it is deemed to be aware and then notification to the supervisory Authority is required (GDPR/Art. 33). When the Data Processor detects the breach, it should promptly notify the Data Controller of the violations. This notice must be "immediate" to help the Data Controller comply with the time commitments. Moreover, if the Data Processor offers services to more than one Data Controllers, it must report the incident and details about it, to each of them.
A prerequisite to achieve the timely detection of a breach is to make clear what constitutes it, since what may be considered a breach for one organization may not for another. It will be beneficial for an organization to have a list of events that are considered as breaches so as not to lose time by investigating these

events in real time. For example, any successful SQL connection from an IP outside a known and pre-defined IP range, or if any file is being accessed from a file server outside business hours.

When a potential data breach occurs, and provided there is a risk for natural persons, the organization, when acting as a Data Controller, must inform the competent supervisory authority *without delay and, if possible, no later than 72 h from the time it occurred*.

The organization must design procedures that describe how it communicates with the Supervisory Authority and the information that will be communicated to them. The organization must state:

- The nature of the violation, including, if possible, the categories and number of affected Data Subjects, and the categories of data
- The name and contact details of the Data Protection Officer
- The possible impact of the violation
- The controls taken or proposed to be taken to address the breach

In addition, the organization must inform the Data Subjects for the violation of their data, if the data breach may pose a high risk to their rights and freedoms. Thus, the organization must design procedures that describe how it communicates with the Data Subjects and the information that will be communicated to them. This information must be concise, transparent, comprehensible, and easily accessible. The organization must use clear and plain language, especially when the information concerns children. The procedures should include providing information through hardcopy forms, electronic announcements, or even orally once the identity of the Data Subject has been confirmed.

9. **Organizations operate in more than one EU Member States**

If the controller is active in more than one Member States, the country of the main establishment should be designated (GDPR/Art. 51). This article spares the organization the requirement to get to grips with several different laws of the various countries of the organization's activity. Thus, in the case of cross-border processing, the "one-stop-shop" mechanism [29, 30] is supported by the implementation of the GDPR, ensuring the cooperation between the corresponding Data Protection Authorities of each country.

The data protection authority of the country that the organization has its main establishment is considered as the Lead Supervisory Authority for the organization. This is identified as the organization's central administration in the EU unless decisions about the purposes and means of processing of personal data are taken in another establishment and that establishment has the power to implement those decisions. If the organization processes data in order to fulfill an obligation under the national law of an EU Member State, only the DPA of that EU Member State is competent.

For the identification of the above, it is therefore important for the organization to clearly determine:

- The place/country of the main establishment (headquarters)
- Potential other facilities within EU
- The place/country where the basic decisions for processing are taken (in the headquarters or not)
- The existence of joint data controllers

10. **Transfer personal data to non-EU countries**
In cases where the data controller must transfer personal data to non-EU countries, it is required to ensure that this transfer is conducted with respect to the legal requirements being imposed by the GDPR (GDPR/Art. 44). Transfer of personal data to a third country or an international organization is realized under the following conditions:

- Transfers subject to appropriate safeguards: EC has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection (GDPR/Art. 45). EC has already recognized the appropriateness of some countries around the world,[3] with this list being updated.
- Transfers subject to appropriate safeguards: The data controller or data processor has provided appropriate safeguards (GDPR/Art. 46), and on condition that enforceable data subject rights and effective legal remedies for data subjects are available:
  - Binding corporate rules (GDPR/Art. 47)
  - Standard data protection clauses (EC) (GDPR/Art. 46)
  - Codes of conduct (GDPR/Art. 40)
  - Certification mechanism (GDPR/Art. 42)

Then it is important to assess and select an appropriate transmission mechanism and also to explore whether it has an obligation to inform the persons whose data will be is transferred.

18.3 Global Privacy Landscape

The demand for the protection of personal data is not limited to Europe. Citizens and consumers around the world are increasingly demanding privacy. And in turn, companies are recognizing that providing strong privacy protection gives them a competitive advantage as confidence in their services increases. Many, especially those with global reach, are under pressure to align their policies with the GDPR,

[3] https://bit.ly/2XR5TSE.

not only because they want to do business in Europe, but also because the GDPR has become the "golden standard" in Data Protection Law globally.

The quintessence of the global impact of the GDPR is encapsulated in this rule: the GDPR applies to any entity doing business in the EU regardless of whether the service provider has a presence in the EU or the recipient of the service is an EU citizen or resident.[4]

The global significance of the GDPR is exemplified by the fine of 50 million Euros that the French National Data Protection Commission (CNIL) imposed for its violation on the global tech giant Google. The CNIL enforcement action focused in particular on the GDPR's transparency and consent requirements and at the same time provided useful guidance on how to design privacy policies.[5]

Furthermore, in recent years, increasing numbers of countries around the world have implemented new or amended legislation in the areas of data protection and privacy, based on a core set of principles in common with the GDPR. These include, inter alia, the recognition of data protection as a fundamental right; the adoption of overarching legislation in the field; the existence of enforceable individual privacy rights; and the setting up of an independent supervisory authority.[6] Of new or modernized laws that overlap up to 80% with the GDPR, a few have been enacted as recently as 2018, such as the Brazilian General Data Protection Law[7] that is very closely modeled on the GDPR or India's Personal Data Protection Bill[8] (to be enacted) that contains GDPR-inspired provisions around consent and the right to be forgotten.

On January 23, 2019, the EU Commission adopted its adequacy decision on Japan, allowing personal data to flow freely from the EU to Japan on the basis of mutually agreed data protection standards. In addition, and for the first time in the history of EU adequacy discussions, Japan is also granting an equivalent status to the EU, thus creating the first mutual system for data flows. This is also the first adequacy decision granted on the basis of the GDPR.[9]

[4] Article 3 GDPR. See also Recital 24 of the GDPR clarifies that tracking individuals on the Internet to analyze or predict their personal preferences—as many websites and apps do—will trigger the application of EU law.

[5] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[6] In 2015 the number of countries that had enacted data privacy laws stood at 109, a significant increase from 76 in mid-2011. As of May 2019, the number has climbed to more than 120 countries.

[7] The Brazilian General Data Protection Law "Lei Geral de Proteçao de Dados" (LGPD) was adopted on August 18th and will come into force in early 2020. See the English translation in https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.

[8] https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

[9] Commission Implementing Decision (EU) 2019/419 of January 23, 2019, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance), OJ L 76, 19.3.2019, p. 1–58 ELI.

Following a review of the Privacy Shield (the framework arrangement between the European Union and the USA to enable the transfer of personal data between the two) by the European Data Protection Board (EDPB)10 and a formal complaint by the French digital rights group, La Quadrature du Net, the General Court of the EU on July 1st and 2nd of 2019 struck down the Privacy Shield, ruling it insufficient in terms of data protection according to EU law. As such, international companies cannot rely merely on the Privacy Shield and must separately determine whether their data privacy practices adhere to the GDPR.

Privacy shield was meant as a placeholder (SCC) to allow for transfer to the USA in light of government surveillance. It got contested in Schrems I, Schrems II and La Quadrature du Net. In Schrems II, the CJEU decided that privacy shield did not apply because surveillance is not limited to strictly necessary and proportional, and there is no judicial redress. This means that companies cannot rely on privacy shield for transfer to USA and other countries as well, and must determine whether surveillance (or other practices) meets these limitations and requirements, set up legal export mechanisms. If not, additional protections are required (e.g. encryption), or transfer must be suspended.

Especially for countries with a surveillance regime that is incompatible with the GDPR requirements for privacy and due process. Get transparency from and control over the importer, so that the exporter can verify GDPR compliance.

Despite the worldwide influence of the GDPR, as of 2021 the USA remains disconnected from the global conversation on privacy. The California Consumer Privacy Act (CCPA), which went into effect in January 2020, was spurred by growing consumer unease with data collection. Like the GDPR, it provides certain rights to consumers-including the right to information and access to personal data, the right of erasure, and the right to opt-out-and, at the same time, greatly expands the definition of personal data.[10] However, the law is limited in its scope (it applies to businesses with a gross annual revenue of $25MM USD; or, drives 50% of their revenue from data sales of California residents; or, businesses that buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices) and only provides rights to California residents. While other US states have attempted to pass similar legislation, these efforts as of yet have been unsuccessful. These attempts also highlight the divergence of agreement in US discussions around data privacy. Despite widespread consumer interest and attention from legislators, discussions at the US federal level continue to stall. However, if enough US states are successful in their efforts to pass privacy legislation, this will put pressure on federal legislators to harmonize the varying laws. Additionally, a second California privacy law, the California Privacy Rights Act (CPRA) that was approved by voters in November of 2020 and set to go into effect in 2023, may further increase this urgency. The CPRA also establishes the first US state-level regulatory agency

[10] For the CCPA core requirements, see https://www.dataprotectionreport.com/2018/06/california-passes-major-privacy-legislation-expanding-consumer-privacy-rights/ or https://oag.ca.gov/privacy/ccpa.

devoted to overseeing California's privacy laws, and once established, may even exceed the size of the Federal Trade Commission's privacy and consumer protection division, responsible for enforcing consumer privacy protections across the entire USA.

Based on the recent examples referred to above, it is expected that the GDPR will continue to operate as a trigger for non-EU countries to adopt much higher data protection standards than they do today. This, in turn, should lead to greater upward convergence of data protection principles internationally, at both bilateral and multilateral levels—a goal which is in the interest and to the benefit of citizens and businesses alike wherever they are in the globalized world. Released from the bottle, the privacy genie isn't likely to be returned. Even companies that may not directly engage in business with the EU would be wise to be aware of the GDPR's provisions and consider proactive compliance in anticipation of continued international adoption of its core principles.

18.4 Conclusions

The protection of personal data is becoming an issue that now, more than ever, affects all organizations around the world. The global scene has changed dramatically during the last few years because of the vast technological advancements affecting every sector. To this end, the reforming of the existing regulatory schemas in order to capture the mechanisms and the technologies that are used for the processing of personal data was of utmost importance. European Commission with the GDPR aimed to define a harmonized framework of action with respect to individuals' privacy. Existing national laws were too difficult to be controlled, leaving room for derogations. After the establishment of the GDPR, other nations followed this example, either by being based on this regulation and developing their own (i.e., LGPD of Brazil), by establishing frameworks in alignment with the European regulation in order to be able to transfer personal data (i.e., Privacy Shield, between EU and USA), or by demonstrating that they have undertaken all the necessary actions,[11] ensuring an adequate level of protection.

[11] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

Compliance with the GDPR comprises a challenging project for organizations for a series of reasons; the complexity of business activities and the duplication of data (in different information flows or even entire departments within an organization) are the most important ones. However, even if organizations need to comply with the GDPR, they lack guidelines that could help them into reaching compliance. There are already products being developed that can be used toward this compliance; however, none of the current technical solutions is able to capture the current security status of an organization, identify the gaps, assess the criticality of the processing activities and the personal data that they use, provide concrete solutions tailored to each organization to finally fortify its processes, and guarantee the protection of individuals' personal data [31]. The "ten steps for compliance" list that is provided in this work aims to facilitate data processors/controllers toward their compliance. Of course, if organizations have already been certified under a specific certification schema (e.g., ISO 27001), they have already satisfied a part of the requirements that the GDPR requests, which means that less effort is required [32].

References

1. Solove, D.J. 2004. *The Digital Person: Technology and Privacy in the Information Age*. Vol. 1. NyU Press.
2. DeVries, W.T. 2003. Protecting privacy in the digital age. *Berkeley Technology Law Journal* 18: 283.
3. Goddard, M. 2017. The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research* 59 (6): 703–705.
4. Safari, B.A. 2016. Intangible privacy rights: How Europe's GDPR will set a new global standard for personal data protection. *Seton Hall Law Review* 47: 809.
5. Greengard, S. 2018. Weighing the impact of GDPR. *Communications of the ACM* 61 (11): 16–18.
6. European parliament. 2016. Regulation (EU) 2016/679 of the European parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation).
7. Acquisti, A., S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati. 2007. *Digital Privacy: Theory, Technologies, and Practices*. CRC Press.
8. Gritzalis, S. 2004. Enhancing web privacy and anonymity in the digital era. *Information Management & Computer Security* 12 (3): 255–287.
9. European commission. 2017. Directive 95/46/ec of the European parliament and of the council. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046, Accessed 14 May 2017.
10. Warren, S.D., and L.D. Brandeis. 1890. Right to privacy. *Harvard Law Review* 4: 193.
11. Westin, A.F. 1968. Privacy and freedom. *Washington and Lee Law Review* 25 (1): 166.
12. ISO/IEC. 2013. ISO 27001:2013 information technology—security techniques—information security management systems—requirements. Tech. Rep.
13. Voigt, P., and A. Von dem Bussche. 2017. The EU general data protection regulation (GDPR). A Practical Guide. 1st ed. Cham: Springer International Publishing.
14. Lambrinoudakis, C. 2018. The general data protection regulation (GDPR) era: Ten steps for compliance of data processors and data controllers. In *International Conference on Trust and Privacy in Digital Business*, 3–8. Springer.

15. Fatema, K., E. Hadziselimovic, H.J. Pandit, C. Debruyne, D. Lewis, and D. O'Sullivan. 2017. Compliance through informed consent: Semantic based consent permission and data management model. In *PrivOn@ ISWC*.
16. Cavoukian, A., et al. 2009. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada. Vol. 5.
17. Langheinrich, M. 2001. Privacy by design principles of privacy-aware ubiquitous systems. In *International Conference on Ubiquitous Computing*, 273–291. Springer.
18. Deng, M., K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen. 2011. A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering* 16 (1): 3–32.
19. Bijwe, A., and N.R. Mead. 2010. Adapting the square process for privacy requirements engineering. Technical Note.
20. Kalloniatis, C., E. Kavakli, and S. Gritzalis. 2008. Addressing privacy requirements in system design: The Pris method. *Requirements Engineering* 13 (3): 241–255.
21. Jensen, C., J. Tullio, C. Potts, and E.D. Mynatt. 2005. Strap: A structured analysis framework for privacy. Tech. Rep., Georgia Institute of Technology.
22. Islam, S., H. Mouratidis, C. Kalloniatis, A. Hudic, and L. Zechner. 2012. Model based process to support security and privacy requirements engineering. *International Journal of Secure Software Engineering (IJSSE)* 3 (3): 1–22.
23. Kalloniatis, C., E. Kavakli, and E. Kontellis. 2009. Pris tool: A case tool for privacy-oriented requirements engineering. In *MCIS*, 71.
24. He, Q., A.I. Antón, et al. 2003. A framework for modeling privacy requirements in role engineering. In *Proc. of REFSQ*, 137–146. Vol. 3.
25. Liu, L., E. Yu, and J. Mylopoulos. 2003. Security and privacy requirements analysis within a social setting. In *Proceedings of 11th IEEE International Requirements Engineering Conference*, 151–161. IEEE.
26. Party, D.P.W. 2017. Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679.
27. Wright, D., K. Wadhwa, M. Lagazio, C. Raab, and E. Charikane. 2014. Integrating privacy impact assessment in risk management. *International Data Privacy Law* 4 (2): 155–170.
28. Notario, N., A. Crespo, Martín, Y.S., Del Alamo, J.M., Le Métayer, D., T. Antignac, A. Kung, I. Kroener, and D. Wright. 2015. Pripare: Integrating privacy best practices into a privacy engineering methodology. In *2015 IEEE Security and Privacy Workshops*, 151–158. IEEE.
29. Tambouris, E., and M. Wimmer. 2005. Online one-stop government: a single point of access to public services. In *Electronic Government Strategies and Implementation*, 115–144. IGI Global.
30. Sedek, K.A., S. Sulaiman, and M.A. Omar. 2011. A systematic literature review of interoperable architecture for e-government portals. In *2011 Malaysian Conference in Software Engineering*, 82–87. IEEE.
31. IAAP. 2018. Privacy tech vendor report. Tech. Rep.
32. Diamantopoulou, V., A. Tsohou, and M. Karyda. 2019. General data protection regulation and iso/iec 27001:2013: Synergies of activities towards organisations' compliance. In *International Conference on Trust and Privacy in Digital Business*. Springer.