https://doi.org/10.3926/hdbr.179

Data protection by design: Organizational integration

Santiago Martín-Romo Romero
PhD in the Business Administration. Certified Information System Auditor from the ISACA Association. Author of several books and papers on the area of information systems with research activities focused in the security and privacy of business processes. Spain.

Carmen De-Pablos-Heredero
PhD in Economics & Business Organization. Director of the Master Degree in Business Organization and Master Degree in Logistic Business Processes SAP at the Rey Juan Carlos University, Madrid, Spain. Author of several books and articles in Business & Education. Spain.

santiago.martinromo@urjc.es, carmen.depablos@urjc.es

Received: October, 2017.
Accepted: June, 2018.
Published: December, 2018.

Abstract
Firms perform the processing of physical personal data and are obliged to protect them according to the Acts. In the European Union, the General Regulation for Data Protection (GDPR) obliges firms to be proactive in the protection of the personal data they process, through data protection from the design. In this research, a group of technical and organizational measures to include in processing, under the focus of data protection from the design is determined from the definition of the processes in which data are processed. These activities, realized by making use of different firm's profiles, promote the need to develop a proper organizational integration amongst participants. The activities done by different profiles at firms promote the need to develop an organizational integration amongst participants, activities performed by different agents, results interchanged and common products used.

Key words
European Regulation for Data Protection; personal data; processes, privacy by design; organizational integration.

How to cite this article
Martín-Romo Romero, S., & De-Pablos-Heredero, C. (2018). Data protection by design: Organizational integration. *Harvard Deusto Business Research,* VII(2), 60-71. https://doi.org/10.3926/hdbr.179

The management of personal data in relation to privacy requirements is critical for companies

1. Introduction

Companies use the data and information belonging to both the individuals and legal entities with whom they interact. As the owners of their personal data, individuals have a series of rights pertaining to how companies process said data, at different phases, from the collection of information and its processing to its deletion (Perera, Ranjan & Wang, 2015).

Personal data are considered to be "any information about an identified or identifiable individual" (European Parliament & Council of the European Union, 2016), and *identifiable individual* is understood to mean "any person whose identity can be determined, either directly or indirectly."

The collection, storage and processing of these personal data, manual or automated, enter into the sphere of privacy of their holders and, therefore, the companies responsible for these operations are required by law to protect them.

Privacy, and in particular the management of personal data, has become one of the most controversial and important aspects of the relationship between businesses and the agents with whom they interact and a priority for organizations, for both reasons related to their reputation and the potentially substantial fines by regulatory bodies in the event of any infraction (OASIS, 2012).

Until recently, companies in Spain only had to comply with the law on the protection of personal data contained in the LOPD and the RLOPD, which satisfied the corresponding European Directive (European Parliament & Council of the European Union, 1995). As of May 25, 2018, compliance is mandatory with the GDPR, and it overrides the aforementioned legislation in terms of anything that might contradict the new regulation.

Current legislation in this area in European countries, based on the above-mentioned directive, was rendered outdated, mainly due to the technological advances that have arisen in recent decades. When the directive was created, the use of the Internet had barely penetrated the business fabric and even less so in society. Email, electronic file exchange (ftp) and static websites were practically the only Internet services used (Fundación Telefónica, 2015; AIMC, 2015). Since that time, the power and storage capacity of computers have increased significantly, telecommunication networks have become more developed and new devices have emerged (smartphones, tablets, etc.), and as a result new services have appeared for data processing in general. Today, we have data capture through websites, social networks, cloud computing, the Internet of things and big data, mobile devices, tablets, smartphones, etc. that connect to the organization's IT processes. Moreover, the information and communications systems of companies have suffered threats and actual attacks (De Pablos, López-Hermoso, Martín-Romo & Medina, 2012; DPI, 2013; Fundación Telefónica, 2015; AIMC, 2015).

This technological evolution promoted change initiatives in Europe in terms of the regulations related to data protection. Accordingly, in 2012, the European Commission proposed a new regulation (European Commission, 2012; European Parliament, 2014), that would be directly applied in each country (without the need to be transposed), for the protection of personal data. This regulation was approved by the European Union in 2016, thus resulting in the General Data Protection Regulation (GDPR) (European Parliament & Council of the European Union, 2016), which took effect in May 2016 and the application of which was mandatory as of May 25, 2018 for member states.

Taking into account the regulatory background, the present study deals with privacy from the design perspective, through the definition of business processes, i.e. at a level prior to the

Technological progress has promoted the emergence of new legislation at the European level

creation of the information systems. The proposal is that businesses, from the very moment they create a business activity, must incorporate the appropriate requirements in relation to privacy that they will have to comply with in that particular business activity.

2. Data protection by design

The concept of privacy by design (PbD) is recognized as a philosophy that helps to improve the privacy of individuals (Poullet, 2010; Antignac & Le Métayer, 2014).

The term PbD was included among the proposals in the new Regulation (European Commission, 2012; European Parliament, 2014) and was replaced in the final version (European Parliament & Council of the European Union, in its Article 25), by the expression data protection by design.

PbD is a concept created at the turn of the century by Canadian Ann Cavoukian, ex-Commissioner for Information and Privacy of Ontario. Her initial goal was to preserve the privacy by implementing measures that integrate the fundamental aspects of data protection within the technological system used for information processing. This focus was later expanded (Cavoukian, 2012) to include three areas of application, including business practices (organizations), technology and the physical design (infrastructures).

Since PbD was included in the GDPR, many statements have been made in favor of this philosophy. ICO (2017) states: "The basis of the privacy by design approach is that if a privacy risk with a particular project is identified, this can be an opportunity to find creative technical solutions that can deliver the real benefits of the project while protecting privacy." ICDPPC (2016) indicated the importance of PbD: "Not only engineers, but also researchers need to start considering privacy engineering principles like *privacy by default* and *privacy by design* in new research, products and services." However, works such as that by Colesky, Hoepman and Hillen (2016) indicate that in and of itself, PbD lacks the specific tools to aid software developers in designing and implementing privacy-friendly systems and there are also no clear guidelines on how to map the specific legal data protection requirements to system requirements.

Some authors, such as Bygrave (2017), believe that PbD has a number of deficiencies in the GDPR, particularly in terms of the lack of clarity on the parameters and methodologies to be applied to reach its objectives, the lack of clear, direct communication with those who are engaged in information systems engineering and the lack of necessary incentives to stimulate privacy-related interests.

In recent years, privacy by design has gained recognition, acceptance and notoriety. Companies, in order to comply with the PbD obligation, must use methods, techniques and tools that make it possible to apply it with a certain degree of order.

In the area of information systems development, these methods of support have begun to appear for implementing the concept of privacy by design, as seen in Compagna, Khoury, Krausová, Massacci and Zannone (2009); Tschantz and Wing (2009); Deng, Wuyts, Scandariato, Preneel and Joosen (2011); Gürses Troncoso and Diaz (2011); Rubenstein and Good (2013); Hoepman (2014), Luna, Suri and Krontiris (2012); and Le Métayer (2013). Different European projects have been undertaken or are underway with the aim of helping to apply concepts related to PbD, including EuroPriSe (2007), PICOS (2009), PRISMS (2012), SurPRISE (2012), PACT (2012), CAPPRIS (2013) and PRIPARE (2014). On an international level, this concept also appears in the ISO privacy framework standard ISO 29100 (ISO, 2011), in the confidentiality protection guide of the NIST (McCallister, Grance & Scarfone, 2010) and in the standard privacy protection method of the OASIS organization (2012).

Harvard Deusto Business Research. Volume VII. Issue 2. Pages 60-71. ISSN: 2254-6235

Privacy by design improves the management of personal data from a legal perspective

Almost from its origins, the practice of privacy by design has been analyzed from the perspective of risk management (Cavoukian, 2010; CNIL, 2012; ITU-T Technology Watch, 2012; ICO, 2013), which implies analyzing the threats to privacy, the possibility they will occur (vulnerability) and the impact that would result, calculating the risk to thus establish the necessary measures (security, organizational, etc.) that reduce, assume or transfer that risk.

Although the concept of PbD has acquired great importance in recent times, as indicated by Luna et al. (2012), the methods, techniques and tools that must accompany it have not kept pace, something which is also pointed out by Rachamadugu and Anderson (2008) and FTC (2010).

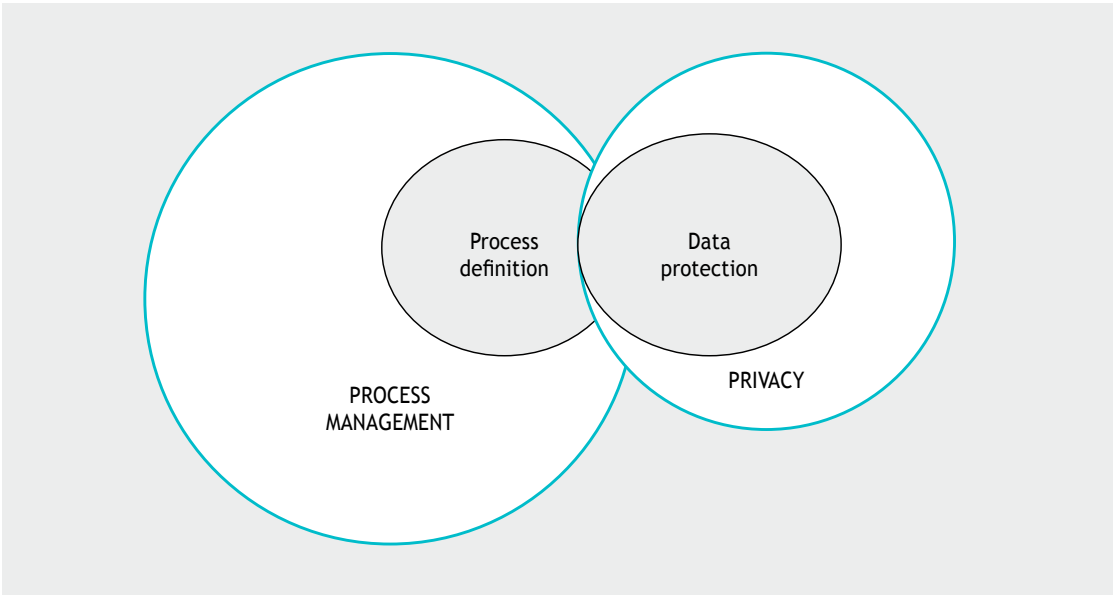
The potential benefits of applying the PDB have been recognized by both privacy regulators (European Parliament & Council of the European Union, 2016) and by data protection authorities (ICDPPC, 2010), although, as stressed by Notario, Crespo, Martin, Del Alamo, Le Métayer, Antignac, Kung, Kroener and Wright (2015), it is complicated to implement it, due to the lack of maturity of this discipline in its practical application.

3. Privacy by design through the definition of processes

Privacy from the perspective of business process management has received little attention in research and there is a gap in the current literature, as no studies are found in relation to methodologies to integrate privacy into business processes (Majdalawieh, 2013; Rachamadugu & Anderson, 2008; FTC, 2010). PbD is in and of itself a process that is closely linked to process design (Kroener & Wright, 2014).

This work studies data protection with a focus on PbD, as required by the European regulation on data protection (European Parliament & Council of the European Union, 2016), but starting with process management, injecting privacy so that it originates with it already built-in. Table 1 shows a diagram of the concepts involved and their relationship to one another.

Table 1
Concepts and their interrelation



Harvard Deusto Business Research. Volume VII. Issue 2. Pages 60-71. ISSN: 2254-6235

Companies need methods and tools that will help and guide them in the implementation of PbD

The integration of privacy in the process definition and from an organizational perspective is a different approach from other studies, as the closest would be those studies that are focused on linking privacy with the development of information systems.

The aspects to consider when integrating data protection into process definition are defined below.

4. Integration of data protection into process definition

4.1. Process definition

For process definition, it is suggested to use structuring in phases, activities and tasks according to MÉTRICA (2000), as well as its global orientation in terms of products, techniques and participants. We must bear in mind that it is a product-oriented methodology; in other words, it is used in the development of an information system, which bears some similarity to process development. Both must be defined and clarified, with the collaboration of users and the involvement of certain profiles that employ a range of techniques and tools.

The objective of this activity is to obtain a detailed specification of the defined process that meets the information needs of users and will serve as a basis for further development in information systems.

The initial description of the process to be defined is created based on the products generated in the global process planning. The scope of the process is established, the general requirements are designed and the process is described with the initial high-level models.

The users are also established who will define the process, delimiting their responsibilities, profiles and dedications. In addition, the planning of the following tasks is also carried out.

In the definition of new process requirements, a detailed catalog of requirements is also created that makes it possible to precisely describe the process and also serves as the basis for checking the completeness of the specification of the models that are being obtained throughout the activity.

Work sessions are conducted with the aim of gathering the information needed to obtain the detailed specification of the new process. In the work sessions, it is a good idea to use the usage case technique to establish the requirements. This technique facilitates communication between process analysts and users. The functions are then described that will be facilitated by the process and the restrictions that must be considered in terms of processing frequency, security, privacy and access control, performance, etc. This set of information is incorporated into the requirements catalog.

During the next activity, the process is divided into analytic subprocesses to obtain the detailed specification of the different models and the monitoring of requirements.

4.2. Data protection

In this activity, the aim is to study the privacy of an environment in five stages, which are consecutive and based on the structure of the MAGERIT methodology for risk management and analysis (2012).

Harvard Deusto Business Research. Volume VII. Issue 2. Pages 60-71. ISSN: 2254-6235

The integration of data protection in the definition of processes entails defining the processes

The stages are the following:

- Stage 1. Organization of the work, establishing the necessary considerations for starting the project to ensure privacy. The opportunity of implementing it is studied, the objectives that must be met are defined and its scope is determined, planning the material and human means for its performance, making it possible for the project to be launched.
- Stage 2. Analysis of the personal information processed, which makes it possible to identify and assess the personal data processed, obtain an assessment of the shortcomings in the protection of said data and estimate the need for a more in-depth study with a risk analysis.
- Stage 3A. Management of privacy requirements, which allows you to configure the possible requirements that must be met in order to eliminate the shortcomings detected in the previous stage and always with the fulfillment of the stated objectives from the first stage. This stage is performed when it is not necessary to carry out a risk analysis regarding privacy.
- Stage 3B. Evaluation of the impacts on privacy, which constitutes a risk analysis and management, and therefore entails the typical risk components and identifies and evaluates the assets, threats, vulnerabilities, impacts and thresholds pertaining to the risks. This is done when the study setting has some very specific characteristics.
- Stage 4. Selection of safeguard mechanisms to deploy, developing an orientation for the deployment plan for the selected mechanisms, establishing the means for monitoring the deployment, collecting work reports on the process to ensure privacy, obtaining the final project documents and making the presentations of the results in the organization.

According to the perceived intensity in terms of the risks to privacy, the user of the method will have to choose between following stage 3A or 3B. In the latter case (Stage 3B) is aimed at high-risk environments for privacy, a study referred to as the *Privacy Impact Assessment* (PIA).

4.3. Integration of both

The integration of data protection in the definition of business processes makes it possible to obtain appropriate privacy requirements during the definition of the business processes.

This proposal is based on the integration of some of the products obtained in the data protection with some of the products obtained in the process definition, so that the process is defined with privacy already built in. As indicated in ICO (2013), it is a matter of searching for open doors that allow information to be exchanged from one method to another, providing for a synergy between the two. Various methods in other areas related to information processing are integrated into one another, as can be seen in Hanouz (1993), Baskerville (1993), MÉTRICA (2000), GISSIP (2006), ENISA (2008), MAGERIT (2012) and ICO (2013).

The integration proposal seeks the incorporation of the contribution made by users to the privacy requirements and designing options via the modeling of processes with the use of collaborative work flow tools and modeling and expression conceptual languages that are flexible to represent and formalize said requirements, providing mutual understanding between the user, the legal side, the technical side and the government regulators involved.

The objective of the proposed integration is to assist specialists in processes to incorporate the user requirements and organizational requirements in terms of privacy and data protection

Harvard Deusto Business Research. Volume VII. Issue 2. Pages 60-71. ISSN: 2254-6235

The integration of data protection in the definition of processes implies protecting data

from the very beginning (i.e., the PbD philosophy) in the definition of processes and do so in a way that is coherent, iterative, systematic and assessable. The processes will be more reliable by taking privacy needs into consideration from the start, since later in their development, technological solutions will materialize the models designed with built-in privacy.

The recipients of this method of integration are both business analysts and privacy analysts, since it will serve as a reference guide to both for the exchange of information in their respective specialties.

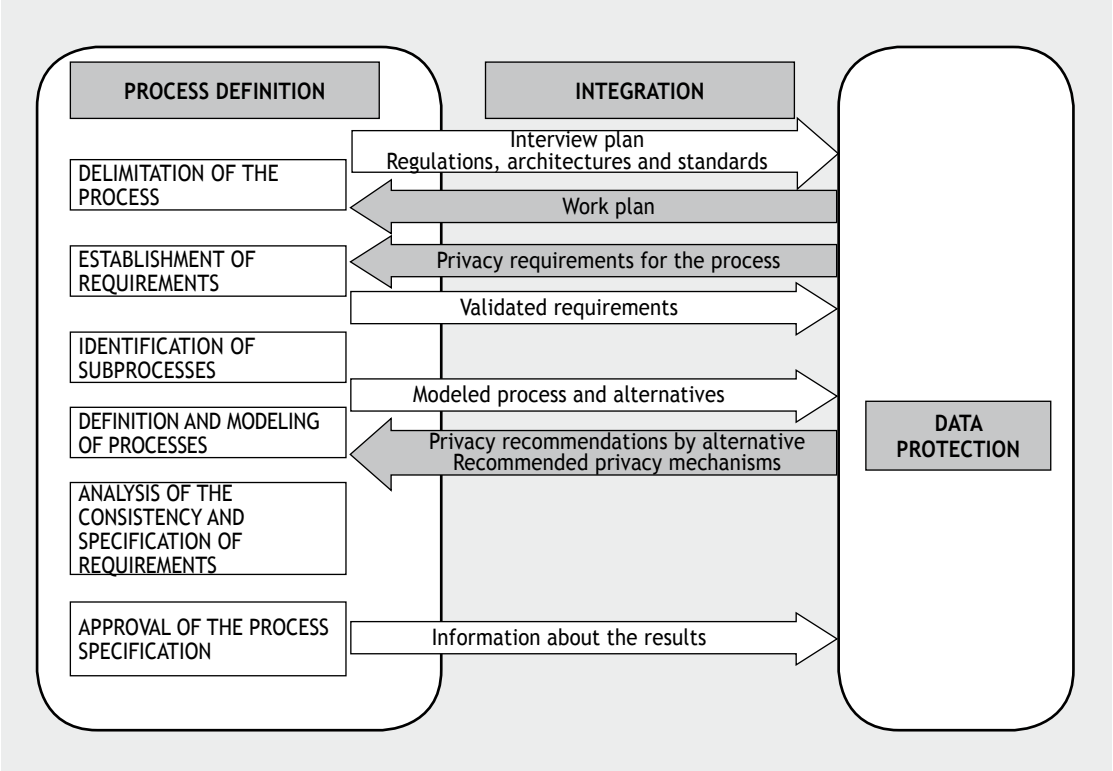
The data protection activities define a cycle of privacy analysis and management along two complementary lines:

- Integrating it into the proposed life cycle in the early stages of BPM methodologies, for the management of business processes, thus permitting the definition of several models of privacy in the processes, according to their level of abstraction.

- Establishing the activities to be carried out to obtain the corresponding evaluations and privacy requirements for each of these models. The corresponding interfaces with the phases, activities, tasks and techniques involved in the process definition are created.

With the data protection, the privacy safeguards are specified for each process, incorporating them as processes of quality assurance into the specification, in order to complete it and to be able to contrast it with the users, based on their roles, prototypes and functional definitions. Figure 2 shows the details of the integration.

Table 2
Integration of data protection into process definition



Harvard Deusto Business Research. Volume VII. Issue 2. Pages 60-71. ISSN: 2254-6235

The integration of data protection in the definition of processes implies integrating both of them

5. Organizational integration of the PbD into process definition

5.1. Integration of products

The products obtained in both types of tasks will be documentary in nature, and due to the different objectives, they will have little in common. The subject matter, methods and techniques used to get the products will barely coincide, due to the fact that they are applied in very different areas within the companies.

The activities involved in defining processes are oriented towards how to obtain the products and services provided by the company and the data protection activities seek to ensure the privacy of those involved in these products and services.

Those professionals who perform and/or use products of process definition or data protection activities must know and understand very well the products of both, as integrating the products of one into the other is complex.

The activities of process definition include a hierarchy, with a structure to obtain different products throughout the order in which they are performed. The products obtained in the data protection activities must be incorporated into this structure. The products generated for data protection activities (lists of recommended measures and management reports) will be introduced under the name of "data protection products." These products of data protection activities will generate some requirements that will affect other process definition products. Mylopoulos, Chung and Nixon (1992) already distinguished between the functional requirements (what the system does) and the non-functional requirements (those referring to restrictions, conditions, quality and others). In the latter case would be the privacy requirements.

The requirements generated by the data protection activities will be added to the requirements catalog generated in the process definition, and later adapted in the process development phases. A complete specification of the requirements at all levels is key for the correct development of the process.

There are two products that are the most important products of a data protection review:

1. The data protection management report.
2. The recommended protective measures (requirements) and the mechanisms to meet the requirements.

These products need to be interpreted and analyzed by the process definition team. The following key factors must be considered:

- The data protection analysts must discuss the requirements with the professionals defining the processes to create a list of new privacy-related proposals.
- The different types of protective measures should be incorporated in the detailed definition of the process phase.

5.2. Integration of participants

As Hitpass (2012) points out, the process definition activities are carried out by the process analyst with the collaboration of the process manager and the process participants (user, business executive). The data protection activities will be performed by the data protection analyst, in collaboration with the process manager and the process participants (user, business

Harvard Deusto Business Research. Volume VII. Issue 2. Pages 60-71. ISSN: 2254-6235

The proposed integration will help incorporate the requirements of both users and the organization

executive). Both teams will work in parallel, with the process definition team doing most of the work. Therefore, a careful plan is required to integrate the data protection activities with the process definition activities.

Once the product has been established that is to be obtained with the process definition, it is important to hold a series of management meetings to discuss the results of each data protection review. The number of meetings, their field of action and their frequency will depend on the scope of the project.

The integration for business process analysts has the following objectives:

- Ensuring an adequate understanding of the process definition method from the perspective of the privacy in the processes being defined.
- Providing a sufficient basis to prepare for the integration.
- Collaborating in establishing the optimal conditions to protect privacy in the newly defined processes.

In the process definition environment, the data protection analyst is faced with the challenge that much of the required information is merely theoretical, and quite vague.

5.3. Integration of activities

When integrating data protection within a process definition project, it is important to plan the activities required by both types of work at the same time to prevent unnecessary delays. It is therefore necessary to hold a series of meetings and interviews with the process definition project team and the data protection analysts at the start of the project to establish the basis for later development. It is very important to schedule all the work that is to be done by the data protection team in conjunction with the planning carried out by the process definition team. Furthermore, whenever data protection reviews are carried out, the process definition team will need fast results.

Both the process definition professionals and those reviewing the data protection need to conduct interviews with the profiles representing the process manager and the participants in the process. For the process definition professionals, these interviews are important to determine the business requirements needed to define the processes. For those reviewing data protection, on the other hand, these interviews are important to establish the processing of personal data and their sensitivity, as well as the evaluations of the threats and vulnerabilities related to privacy. Both types of interviews must be performed simultaneously to ensure the smooth running of the project and prevent wasted time by the users.

To summarize, the planning and preparation for these interviews must be a key point on which both the data protection reviewers and the process definition team must work together.

6. Conclusion

Data protection by design, as a new mandate of the GDPR, involves establishing the technical and organizational measures as soon as possible in the cycle in order to respect the rights of individuals when companies process their data. This paper proposes that the establishment of these privacy requirements be studied as soon as the processes are proposed that will process these data. In this way, by defining these processes with their functional requirements, the data protection requirements will be incorporated in such a way that they are described and implemented with the most appropriate mechanisms in later phases.

The proposal will allow you to check the consistency of data during the life cycle of the process

The definition of processes and the establishment of the data protection requirements are activities performed within companies by different profiles, which makes it necessary to establish proper organizational integration among the different agents, to coordinate the activities they will perform and to use the products obtained.

The following are the advantages of integrating data protection in the process definition:

- It provides an analysis of the protection of the data processed by the process in question prior to its development.
- It incorporates safeguards before it is completed (which is more effective and cheaper in the long run).
- It ensures consistency throughout the life cycle of the process.

7. Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

8. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

9. References

AIMC (Asociación para la Investigación de Medios de Comunicación) (2015). *Audiencia de Internet en el EGM.*

Antignac, T., & Le Métayer, D. (2014). Privacy by Design: From Technologies to Architectures. In B. Preneel & D. Ikonomou (eds.), *Privacy Technologies and Policy.* Second Annual Privacy Forum, APF 2014, 8450, 1-17. https://doi.org/10.1007/978-3-319-06749-0_1

Caves, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys,* 25(4), 375-414. https://doi.org/10.1145/162124.162127

Bygrave, L. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review,* 4(2), 105-120. https://doi.org/10.18261/issn.2387-3299-2017-02-03

CAPPRIS (2013). Collaborative Action on the Protection of Privacy Rights in the Information Society. Inria Project Lab.

Cavoukian, A. (2010). Privacy Risk Management. Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, *by default.* Information and Privacy Commissioner, Ontario, Canada.

Cavoukian, A. (2012). Privacy by Design. *IEEE Technology and Society Magazine,* 31(4), 18-19. https://doi.org/10.1109/MTS.2012.2225459

CNIL (Commission Nationale de l'Informatique et des Libertés) (2012). *Methodology for Privacy Risk Management.* Paris.

Colesky, M., Hoepman, J., & Hillen, C. (2016). A Critical Analysis of Privacy Design Strategies. *IEEE Symposium on Security and Privacy Workshops,* 33-40. https://doi.org/10.1109/SPW.2016.23

Compagna, L., Khoury, P. E., Krausová, A., Massacci, F., & Zannone, N. (2009). How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. *Artificial Intelligence and Law,* 17(1), 1-30. https://doi.org/10.1007/s10506-008-9067-3

De Pablos, C., López-Hermoso, J. J., Martín-Romo, S., & Medina, S. (2012). *Organización y transformación de los sistemas de información en la empresa.* ESIC.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering,* 16(1), 3-32. https://doi.org/10.1007/s00766-010-0115-7

DPI (Data Privacy Institute) (2013). *Reflexiones sobre el futuro de la Privacidad en Europa. II Edición del Estudio de la propuesta de Reglamento de Protección de Datos de la UE.* ISMS Forum Spain.

ENISA (European Network and Information Security Agency) (2008). *Integration of Risk Management with Operational IT Processes.*

European Commission (2012). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* COM(2012) 11 final. 2012/0011 (COD). Retrieved August 8, 2015, from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1419003505129&uri=CELEX:52012PC0011

European Parliament (2014). *European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading). Retrieved August 8, 2015, from http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402

European Parliament & Council of the European Union (1995). Directive 95/46/EC 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. *Official Journal of the European Communities,* No L 281, 31-50.

European Parliament & Council of the European Union (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). *Official Journal of the European Union,* L119, 59, 1-88. Retrieved June 18, 2018, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN

EuroPriSe (2007). *The European Privacy Seal.* Project promoted by the European Union.

FTC (Federal Trade Commission) (2010). *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers.* Retrieved September 23, 2015, from http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

Fundación Telefónica (2015). *La Sociedad de la Información en España 2014.*

GISSIP (2006). *Guide d'intégration de la sécurité des systèmes d'information dans les projets.* Secrétariat général de la défense nationale. Direction centrale de la sécurité des systèmes d'information.

Gürses, S., Troncoso, C., & Diaz, C. (2011). *Engineering Privacy by Design.* Paper presented at the Computers, Privacy & Data Protection Conference.

Hanouz, R. (1993). *Sécurité et qualité des systèmes d'information: La méthode INCAS-MESSIE.* Les éditions d'organisation.

Hitpass, B. (2012). *BPM: Business Process Management. Fundamentos y Conceptos de Implementación.* BHH Ltda.

Hoepman, J. H. (2014). Privacy Design Strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam & T. Sans (eds.), *ICT Systems Security and Privacy Protection,* 446-459. https://doi.org/10.1007/978-3-642-55415-5_38

ICDPPC (2010). *32nd International Conference of Data Protection and Privacy Commissioners. Resolution on Privacy by Design.* Jerusalem. Retrieved September 23, 2015, from https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

ICDPPC (2016). *Artificial Intelligence, Robotics, Privacy and Data Protection.* International Conference of Data Protection and Privacy Commissioners.

ICO (Information Commissioner's Office) (2013). *Privacy impact assessment and risk management.* Trilateral Research & Consulting.

ICO (Information Commissioner's Office) (2017). *Big data, artificial intelligence, machine learning and data protection.* Version: 2.2.

ISO (International Organization for Standardization) (2011). *ISO/IEC 29100:2011. Information technology – Security techniques – Privacy framework.* First edition. Geneva, 15 Dec 2011.

ITU-T Technology Watch (2012). *Privacy in Cloud Computing.*

Kroener, I., & Wright, D. (2014). A Strategy for Operationalizing Privacy by Design. *The Information Society,* 30(5), 355-365. https://doi.org/10.1080/01972243.2014.944730

Le Métayer, D. (2013). Privacy by Design: a Formal Framework for the Analysis of Architectural Choices. *ACM Conference on Data and Application Security and Privacy (CODASPY 2013),* 95-104. https://doi.org/10.1145/2435349.2435361

Luna, J., Suri, N., & Krontiris, I. (2012). Privacy-by-Design Based on Quantitative Threat Modeling. *Seventh International Conference on Risks and Security of Internet and Systems,* 1-8. https://doi.org/10.1109/CRISIS.2012.6378941

MAGERIT (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.* Ministerio de Hacienda y Administraciones Públicas.

Majdalawieh, M. (2013). Building a Privacy Model in the Business Processes of the Enterprise: An Information Systems Design Science Research. *Eurasian Journal of Business and Management,* 1(1), 2013, 15-31.

McCallister, E., Grance, T., & Scarfone, K. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* National Institute of Standards and Technology (NIST). Special Publication 800-122. https://doi.org/10.6028/NIST.SP.800-122

MÉTRICA (2000). *Metodología de Planificación, Desarrollo y Mantenimiento de Sistemas de Información.* Métrica versión 3. Consejo Superior de Informática y para el Impulso de la Administración Electrónica.

Mylopoulos, J., Chung, L., & Nixon, B. (1992). Representing and using nonfunctional requirements: a process-oriented approach. *IEEE Transactions on Software Engineering,* 18(6), 483-497. https://doi.org/10.1109/32.142871

Notario, N., Crespo, A., Martin, Y.-S., Del Alamo, J. M., Le Métayer, D., Antignac, Th., Kung, A., Kroener, I., & Wright, D. (2015). PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. *IEEE CS Security and Privacy Workshops,* 151-158. https://doi.org/10.1109/SPW.2015.22

OASIS (2012). *Privacy Management Reference Model and Methodology (PMRM).* OASIS Committee Specification Draft 01.

PACT (2012). *Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action.* International research project supported by the EU as a part of the Trust & Security Group within the 7th Research Framework Program.

Perera, C., Ranjan, R., & Wang, L. (2015). End-to-End Privacy for Open Big Data Markets. *IEEE Cloud Computing,* 2(4), 44-53. https://doi.org/10.1109/MCC.2015.78

PICOS (2009). *Privacy and identity management for community services.* International research project supported by the EU as a part of the Trust & Security Group within the 7th Research Framework Programm.

Poullet, Y. (2010). About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In S. Gutwirth, Y. Poullet & P. de Hert (eds.), *Data Protection in a Profiled World,* 3-30, Springer. https://doi.org/10.1007/978-90-481-8865-9_1

PRIPARE (2014). *D1.2 Privacy- and Security-by-design Methodology Handbook.* International research project supported by the EU as a part of the Trust & Security Group within the 7th Research Framework Programme.

PRISMS (2012). *The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making.* FP7 SEC-2011.6.5-2. International research project supported by the EU as a part of the Trust & Security Group within the 7th Research Framework Programme.

Rachamadugu, V., & Anderson, J. A. (2008). Managing Security and Privacy Integration across Enterprise Business Process and Infrastructure. *2008 IEEE International Conference on Services Computing,* 2, 351-358. https://doi.org/10.1109/SCC.2008.46

Rubenstein, I. S., & Good, N. (2013). Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkeley Technology Law Journal,* 28(2), 1333-1413.

SurPRISE (2012). *Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe.* FP7 SEC-2011.6.5-2. International research project supported by the EU as a part of the Trust & Security Group within the 7th Research Framework Programme.

Tschantz, M. C., & Wing, J. M. (2009). Formal Methods for Privacy. In A. Cavalcanti & D. R. Dams (eds.), *FM 2009: Formal Methods,* 5850, 1-15. https://doi.org/10.1007/978-3-642-05089-3_1