ISCTE IUL
REPOSITÓRIO
INSTITUTO UNIVERSITÁRIO DE LISBOA

Repositório ISCTE-IUL

Deposited in *Repositório ISCTE-IUL*:
2024-02-09

Deposited version:
Publisher Version

Peer-review status of attached file:
Peer-reviewed

Citation for published item:
Costa, N., Silva, J., Almeida, I. & Möhring, M. (2019). PRIvacy management responsibility on a scrutinized environment (primrose): A management method to address privacy challenges. In Gyöngyi Kovács, Markku Kuula (Ed.), Proceedings of the 26th EurOMA Conference - Operations Adding Value to Society. Helsinki: EurOMA.

Further information on publisher's website:
http://euroma2019.org/

Publisher's copyright statement:
This is the peer reviewed version of the following article: Costa, N., Silva, J., Almeida, I. & Möhring, M. (2019). PRIvacy management responsibility on a scrutinized environment (primrose): A management method to address privacy challenges. In Gyöngyi Kovács, Markku Kuula (Ed.), Proceedings of the 26th EurOMA Conference - Operations Adding Value to Society. Helsinki: EurOMA.. This article may be used for non-commercial purposes in accordance with the Publisher's Terms and Conditions for self-archiving.

Use policy

Creative Commons CC BY 4.0
The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in the Repository
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Serviços de Informação e Documentação, Instituto Universitário de Lisboa (ISCTE-IUL)
Av. das Forças Armadas, Edifício II, 1649-026 Lisboa Portugal
Phone: +(351) 217 903 024 | e-mail: administrador.repositorio@iscte-iul.pt
https://repositorio.iscte-iul.pt

PRIvacy Management Responsibility On a Scrutinized Environment (PRIMROSE) - A management method to address privacy challenges

Nuno Alexandre Costa (ncaou@iscte-iul.pt)
Instituto Universitário de Lisboa (ISCTE-IUL), Business Research Unit (BRU-IUL), Lisboa, Portugal

J. M. Vilas-Boas da Silva (jmvbs@iscte.pt)
Instituto Universitário de Lisboa (ISCTE-IUL), Business Research Unit (BRU-IUL), Lisboa, Portugal

Isabel Duarte de Almeida (isabel.dalmeida@edu.ulusiada.pt)
Universidade Lusíada, (CLISSIS-UL), Lisboa, Portugal
Instituto Universitário de Lisboa (ISCTE-IUL), Lisboa, Portugal

Monika Maria Möhring (monika.moehring@muk.thm.de)
Management und Kommunikation, Technische Hochschule Mittelhessen (THM), Friedberg, Germany

Abstract

This paper's theoretical contribution is in reporting an innovative privacy management method designated as PRIMROSE - PRIvacy Management Responsibility On a Scrutinized Environment. Research contribution is in introducing a supported process concerning the effective efficient management of privacy requirements occurring in organizations. PRIMROSE was the outcome of deductive reasoning subjected to a focus group and eight DPO interviewees scrutiny. Practical contribution is in setting the missing link regarding a generally recognized privacy management method to guide practitioners in which the elements originate from the qualitative research supporting root definitions semantics, considering, among others, principles, stages, processes, enablers and composite requirements.

Keywords: PRIMROSE, privacy management method, data protection.

Introduction

The European Union's General Data Protection Regulation (GDPR) was enforced on 25 May 2018 and demands that organizations, i.e. data controllers and processors "implement appropriate technical and organizational measures" to safeguard the "ongoing confidentiality, integrity, availability and resilience of processing systems and services" (Regulation EU, 2016), regarding the management of personal information of EU citizens (Costa et al., 2018).

In this context, the research sponsor, i.e. the DATASHIELD DPBCS is a company that provides consultancy services and solutions for data protection. It supports the investigation of a holistic privacy management method, designated as PRIMROSE. As trained facilitators of strategic privacy thinking, the research sponsor follows a predetermined process and uses predesigned techniques and practices to keep organizations on track regarding the privacy forum and brings in objectivity to clients and to the discussion of legal and regulatory issues and concerns of data protection.

If we consider the analysis and implementation of privacy and data protection solutions alone, the issue itself is complex in nature. Combined with the legal imperative, the challenge is increased. For example, the US approach to privacy is sectoral, different from the approach of the European Union (EU) countries, which has a comprehensive Regulation for member states. Another jurisdictional example, the General Law of Protection of Personal Data from Brazil, inspired in the GDPR also imposes a set of rules that have to be fulfilled. If we take the example of an organization that performs in these three geographical areas, the management of privacy and data protection include a specific and demanding use of resources that must be managed effectively and efficiently. In addition, organizations have different forms and configurations of management.

So, what organizations want is a method that involves the strategic thinking of their own people that are part of the overall privacy solution (Robert, 1998). Moreover, the terms of reference coming from the Regulation to set what should be done, designated as the "permanent enablers" (Costa et al., 2017), are thoroughly examined in order to address the needed requirements. Depending on their timescales, organisations are either permanent or temporary. Thus, projects are temporary.

Therefore, this investigation presents a summary of the PRIvacy Management Responsibility On a Scrutinized Environment (PRIMROSE), a privacy management method for addressing the following research questions: [RQ1] *What are the high-level requirements of the permanent organization to be GDPR compliant?* and [RQ2] *How should the GDPR requirements be managed in the permanent organisation?* PRIMROSE is expected to keep the data protection requirements on track, to bring objectivity to privacy work and, simultaneously, to involve all relevant interested parties to the discussion. Moreover, PRIMROSE principles, strategy, stages, processes, enablers, composite requirements and continuous service improvement, developed as a function of the privacy environment, are described in this paper.

The required organizational changes will not occur overnight. This qualitative investigation revealed that, for organizations to be effective and efficient in the matter of data protection throughout time, specifically in what concerns the Regulation requirements, its variables should be managed through a privacy method to ease the achievement of their planned benefits. Thus, the following section describes PRIMROSE, a holistic and multidisciplinary method for privacy management. The elements of the method are detailed and described. Finally, the theoretical, practical and managerial implications of the model are examined.

Proposal of a method for privacy management

PRIMROSE is a rival approach of *OASIS Privacy Management Reference Model and Methodology* that has not become enough widespread and popular. Rival approaches compete to explain the same phenomenon and cannot be mixed.

Privacy and data protection issues are complex to deal with. Therefore, PRIMROSE's first goal is to make the complex and irreducible privacy elements as simple as possible, by: (i) contributing to support privacy by design and by default (Cavoukian, 2013), (ii) addressing organizational privacy factors and mechanisms with effectiveness and

efficiency, and (iii) considering the respect for user privacy and utility as quality components.

By doing so, PRIMROSE contributes to privacy management holistically, supported by the reasoning that privacy has multiple dimensions.

Moreover, these multiple dimensions exhibit cross-impacts that may require an interrelated analysis. For example, the dimension of privacy concerning "behaviour and action" (ISACA, 2016), put together with the dimension of privacy concerning "data and image" (ISACA, 2016) may enable the identification of someone' specific lifestyle pattern. So, an increasing number of commercial apps might be used to register and disclose a broad variety of their users' individual behaviours.

Thus, these dimensions can be used to classify privacy issues, concerns and problems, according to shared qualities or characteristics, e.g. of behaviour and action, of communication, of data and image (i.e. information), of thoughts and feelings, of location and space, and of association (ISACA, 2016).

Privacy dimensions are therefore examined as a synergetic interaction that intend to prevent harm to individuals by investigating the relations of two or more privacy dimensions, to produce a combined privacy solution greater than the sum of their separate parts. This interpretation recognizes that dimensions are multivalent in their nature and complex in their dynamics. Moreover, PRIMROSE considers processing, i.e. "any operation or set of operations which is performed on personal data or on sets of personal data" (Regulation EU, 2016), as well as the impact of that processing on individuals that use any "service" (Vargo and Lusch, 2004) provided by the organisation. So, organisations role and accountability in protecting people, processes, and technology are strengthen by rationalizing and managing privacy and data protection requirements.

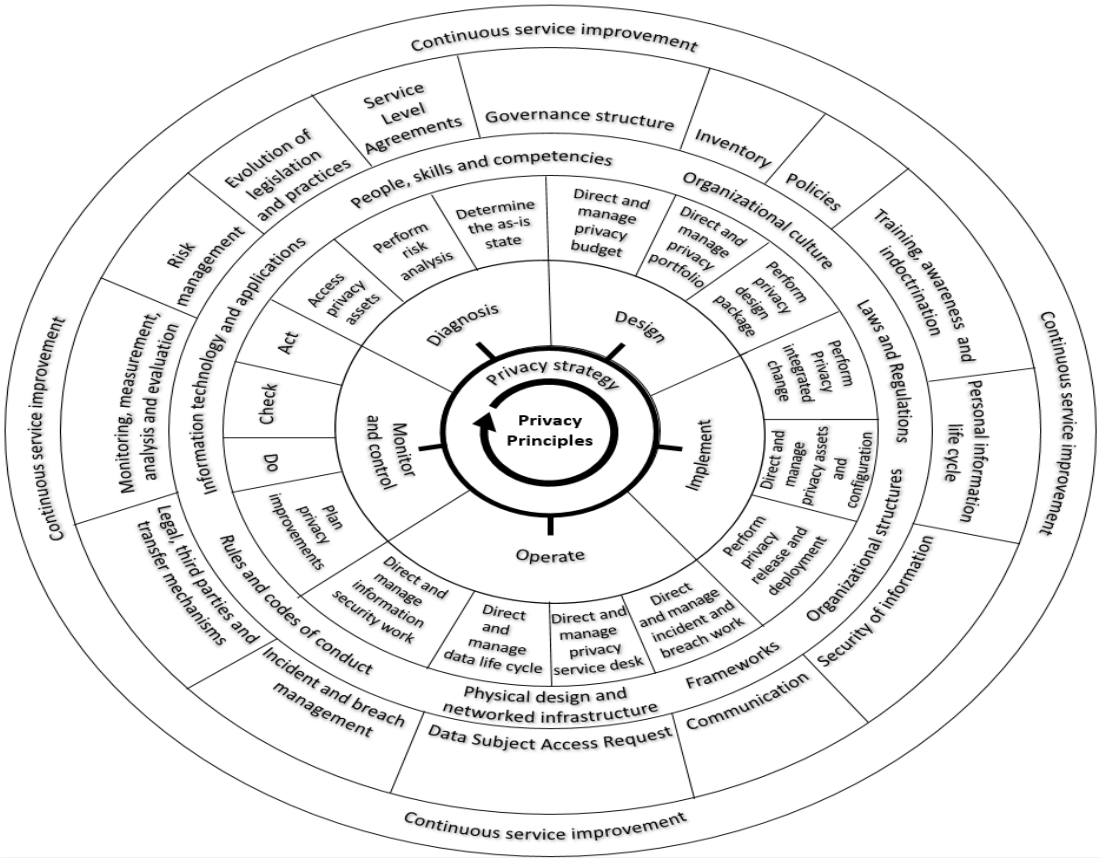

Figure 1 – PRIvacy Management Responsibility On a Scrutinized Environment (PRIMROSE)

Therefore, scrutinizing, examining or inspecting privacy issues and concerns, closely and thoroughly, in a complex privacy environment characterized by a diversity of laws and regulations, in different social-cultural and organizational configurations that are challenged every day, is of paramount importance.

For the reasons mentioned above, PRIMROSE considers relevant interested parties, internal and external, and encompass in a holistically, integrated and multidisciplinary way, principles, strategy, stages, processes, permanent and temporary enablers, composite (Ohnishi and Agusa, 1993) requirements, and continuous service improvement, in order to support organizational privacy strategic objectives, risk appetite and tolerance (*vide* Figure 1).

Principles

The first integrated layer of the method encompasses the fourteen PRIMROSE core principles. Together, they are the "strategic heartbeat" of the method and act as a "driving force or strategic drive" (Robert, 1998) that pushes or propels the organization toward certain privacy results, maturity level or profile. Moreover, they form the foundation base that the rest of the method adheres to.

These privacy principles have existing standards and principles as a foundation support. Therefore, the privacy principles are described in Table 1. Moreover, the standards and principles that supported the PRIMROSE principles were obtained from the BS10012:2017, GDPR, ISACA privacy principles, OECD 2013, ISO/IEC 29100:2011 (last reviewed and confirmed in 2017), APEC and GAPP (in Table 1).

Table 1 – Detail and source of the PRIMROSE privacy principles

PRIMROSE Privacy Principles	BS 10012	GDPR	ISACA	OECD 2013	ISO 29100	APEC	GAPP
1. Choice, decision and consent	N/A	N/A	✓	N/A	✓	✓	✓
2. Openness, lawfulness, fairness and transparency of processing	✓	✓	✓	✓	✓	N/A	N/A
3. Purpose limitation	✓	✓	✓	✓	✓	✓	✓
4. Personal information lifecycle	✓	✓	✓	✓	✓	✓	✓
5. Accuracy and quality	✓	✓	✓	✓	✓	✓	✓
6. Participation on individual rights and capabilities	N/A	N/A	✓	✓	✓	✓	✓
7. Accountability	✓	✓	✓	✓	✓	✓	✓
8. Security safeguards	✓	✓	✓	✓	✓	✓	✓
9. Preventing harm	N/A	N/A	✓	N/A	N/A	✓	N/A
10. Privacy by design	N/A	N/A	✓	N/A	N/A	N/A	N/A
11. Privacy by default	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12. Free flow of personal information	N/A	N/A	✓	✓	N/A	N/A	N/A
13. Interoperability	N/A	N/A	N/A	N/A	N/A	N/A	N/A
14. Trust	N/A	N/A	N/A	N/A	N/A	N/A	N/A

It is important to underline that certain privacy principles, for example, regarding the ISACA privacy principles, namely monitoring, measuring and reporting, third-party/vendor management, and breach management were not considered principles in its true sense. Instead, the aforementioned principles are reasoned and described as management work. Therefore, they are organized in one of a reasoned set of composite requirements of the PRIMROSE method, and, among which, all variables having a determined number of characteristics might be distributed and put together.

In short, the PRIMROSE privacy principles set the tone and provide orientation towards the privacy goals, and indicate what your organization should do to protect personal information.

Privacy strategy

According to Mintzberg (1979) strategy may be viewed as a mediating strength between two dynamic variables; the organization and its environment. The conception of strategy, includes the "interpretation of the environment and the development of consistent patterns in streams of organizational decisions ("strategies") to deal with it" (Mintzberg, 1979). The fundamental question has to do with "strategic thinking" (Robert, 1998) and it boils down to elicit from peoples thoughts and reasoning's, who lead or manage the business, their finest rational judgment regarding what is indeed happening in the organization; what conditions, events or circumstances are taking place or occurring in the organization external environment, and "what should be the position of the business in view of highly qualitative variables" in order to "produce a vision, a profile, of what an organization wants to become" (Robert, 1998). Thus, PRIMROSE provides a method for privacy professionals interfacing with the organisation, as well as aligning its culture, processes, methods and strategic orientation with privacy and data protection requirements.

Stages

PRIMROSE stages ensure interested parties commitment and organizational assets, as well as authority to apply organizational resources and capabilities. Moreover, stages provide a significant way to help the privacy steering committee monitor privacy work at C-Level. At the end of each PRIMROSE stage, the privacy board can review the organizational privacy work and decide whether to commit assets to the next stage. Two benefits are highlighted: first benefit is planning, because there is, at all times, a planning horizon; secondly, there is no need for the c-level executives that are taking on roles in the privacy steering committee to get involved with the everyday's management of the stages, however, they can maintain the power to influence or direct people's behavior or the course of events of privacy work, by giving official permission for or approval to progress. PRIMROSE stages can be described as follows (in Table 2):

Table 2 – PRIMROSE privacy stages

Stages	Description
Diagnosis	To "move forward, it is crucial that we understand the current state" (Kerzner, 2017). Therefore, this stage provides a formal examination and reasoning, e.g. through privacy impact assessments, regarding privacy assets, i.e. "any resource or capability" (TSO, 2012) to determine where the organization is at, i.e. to ascertain the privacy maturity level.
Design	It is the stage in the PRIMROSE lifecycle that turns a privacy "strategy into a plan for delivering the business objectives" (TSO, 2012).

Implement	It is the stage where all approved privacy assets change requests are implemented, e.g. may be through privacy programs and projects to address privacy requirements, issues and concerns.
Operate	Privacy objectives are lastly fulfilled through the “operate stage”, calling for an effective and efficient support of the organizational services to simultaneously ensure privacy and business practices.
Monitor and control	The “monitor and control stage” enables "tracking, reviewing, and reporting the progress to meet the [privacy] performance objectives defined" (PMI, 2017) in the business case and in the privacy management plan.

Each stage logically selects and organizes the privacy processes that concur to achieve the fulfillment of one or multiple objectives and requirements.

Processes

PRIMROSE processes comprise an organized set of inputs, practices, activities, techniques, that concur for the achievement of certain privacy requirements and objectives (ISACA, 2016). Moreover, they are undertaken to produce a set of required outputs, e.g. products, services, results (PMI, 2017). Therefore, circumstances that form the setting for a specific privacy commitment, and in which permanent or temporary organization they occur, aim at obtaining privacy requirements that provide value for the organization. Thus, privacy requirements should be fully understood, assessed, and clearly defined from the outset. However, they may be subject to change, but this variation must be formally controlled and managed.

Processes cover distinct needs and responsibilities which may co-exist simultaneously in any organization. Since, “becoming privacy compliant is a journey” (AICPA/CICA, 2009), they are iterative and may or may not occur in different timescales in which the organizations are required to whether diagnosis, design, implement, operate, and continuously improve their privacy requirements, as well as their intrinsic challenges.
In addition, these processes are meant to construct a more manageable and increasingly optimized organizational privacy environment. The seventeen PRIMROSE processes can be described as follows (in Table 3):

Table 3 – PRIMROSE privacy processes

Stage	Processes	Description
Diagnosis	Access privacy assets	Assess privacy gaps and vulnerabilities in the organization assets as compared to corporate strategy and policies, applicable laws and regulations, and data impacted.
	Perform risk analysis	Risk analysis is the “process to comprehend the nature of risk and to determine the level of risk” (ISO31000, 2009).
	Determine the “as-is” state	The “as-is” state has to be determined in order to represent the current situation that might need to be changed according to laws and regulations requirements.
Design	Direct and manage privacy budget	Budget concerns must be examined. Contingency and management reserves must be scrutinized and decisions about including them in the cost baseline should be made.
	Direct and manage privacy portfolio	This process describes the solutions currently being considered and being developed by the organization, along with its present contractual commitments, and retired solutions (TSO, 2012).
	Perform privacy design package	Defines all aspects of a privacy product, service, or result and its requirements through each stage of its lifecycle. A privacy design package is produced for each new privacy

		product, service, or result, major change, or privacy solutions retirement (TSO, 2012).
Implement	Perform privacy integrated change	It is the process where all approved privacy assets change requests are implemented and communicated (PMI, 2017).
	Direct and manage privacy assets and configuration	The purpose is to guarantee that the assets required to deliver products, services, or results are controlled in a truthful and correct way, "and that accurate and reliable information about those assets is available when and where it is needed" (TSO, 2012).
	Perform privacy release and deployment	The purpose is to "plan, schedule and control the build, test and deployment of releases, and to deliver new functionalities required by the business while protecting the integrity of existing" (TSO, 2012) products, services, or results.
Operate	Direct and manage incident and breach work	The purpose is to decrease the harmful impact on individuals and, on organization reputation, image and its assets, satisfy communication requirements to interested parties, and reinstate normal service operation as swiftly as possible (TSO, 2012).
	Direct and manage privacy service desk	As the single point of contact for Data Subject Access Requests (DSARs) both for employees as for customers on a daily basis, the purpose is to direct and manage this organizational interface.
	Direct and manage data life cycle	It is the process that organizations use to direct and manage the flow of data and information throughout its life cycle, i.e. from collection, use, share, retention, and deletion.
	Direct and manage information security work	This process is focal for all information security controls. It ensures that the information security policy is communicated and enforced, enabling an adequate management of the organization's data and information regarding its confidentiality, availability and integrity (TSO, 2012).
Monitor and control	Plan privacy improvements	Provides guidance and instructions regarding intended privacy improvements.
	Do	This process deals with the execution of the plan.
	Check	This process works toward the monitoring and measurement of progress against the privacy improvement plan.
	Act	The purpose is to identify deviations against the plan and act in accordance with its prevention or correctness definition.

Each stage and process address risks and opportunities and may have internal and external interested parties, which are shown in a responsibility assignment matrix (RAM), e.g. the use of a RACI (responsible, accountable, consult and inform) chart may be useful to ensure explicit and unequivocal assignment of roles and their essential responsibilities. Moreover, "RAMs can be developed at various levels" (PMI, 2017).

Enablers

Organizational "enablers are all that [singly or jointly] contribute and seek to construct the purpose in a positive-sum manner" (Costa et al., 2018). Thus, it includes "any [assets, i.e.] resources or capabilities" (TSO, 2012) that could contribute to the achievement of privacy requirements. The literature review has showed that there is a commonly agreed-upon definition and categorization of organizational enablers, e.g. Müller et al. (2016);

ISACA (2016); Costa et al. (2017); leading us to adopt and adjust existing categories for PRIMROSE use. Therefore, privacy enablers are grouped into eight categories: (i) people, skills and competencies, (ii) organizational culture, (iii) laws and regulations, (iv) organizational structures, (v) frameworks, (vi) physical design and networked infrastructure, (vii) rules and codes of conduct, (viii) information technology and applications. These privacy enablers can be organized into two parts: process facilitators and discursive abilities (in Table 4).

Table 4 – Privacy enablers (After Costa et al., 2017; Müller et al., 2016)

	Privacy Enablers	
	Process Facilitators	Discursive Abilities
Factors	Touchable characteristics, conditions, and variables that directly impact the effectiveness, efficiency, and viability, e.g., laws, regulations, standards	Effective communication and interpersonal skills that influence the mindset and behaviors of individuals, e.g., people, skills and competencies
Mechanisms	Trigger or accumulate actions in organizations to increase the likelihood of a certain output, outcome and benefits, e.g., structures, rules and codes of conduct	Structures that support effective communication (discourse), e.g., synchronized communication structures, dedicated network structures, e.g., shared beliefs, corporate culture

According to Costa et al. (2018), whilst effectiveness is defined as the expected organizational satisfaction of the privacy requirements (permanent enablers), efficiency has to do with the employees and collaborators of the organization, seeing that if they are educated and trained in privacy, data protection and security of processing, to what extent can they rapidly perform activities towards the resolution of privacy issues, concerns and problems, i.e. to be effective (temporary enablers).

Composite requirements

Composite requirements, i.e. high-level requirements "does not have its own testable fit criteria, but it rather "summarizes" a number of other individually testable requirements" (Robertson and Robertson, 2006). Therefore, the privacy composite requirements or themes are, as follows: (i) Governance structure, (ii) Inventory, (iii) Policies, (iv) Training, awareness and indoctrination, (v) Personal information life cycle, (vi) Security of information, (vii) Communication, (viii) Data subject access request, (ix) Incident and breach management, (x) Legal, third parties and transfers mechanisms, (xi) Monitoring, measurement, analysis and evaluation, (xii) Risk management, (xiii) Evolution of legislation and practices, and (xiv) Service level agreements. Moreover, they should coherently group several fundamental and distinct requirements. There are controls associated with these requirements that can be obtained from the Regulation, the BS10012 and the ISO27001.

Continuous service improvement

The purpose of the service improvement layer of the PRIMROSE method is to align privacy related business services with variable environment requirements, e.g. new laws and regulations, making the bridge between the external environment and the organization and, its internal environment, by acknowledging and communicating legislation updates to interested parties. These alignment activities support the PRIMROSE lifecycle approach through diagnosis, design, implement, operate, monitor

and control, constantly searching for ways to improve the "effectiveness, process effectiveness and cost effectiveness" (TSO, 2012) of privacy related services.

Method

The pursued research purpose is exploratory mainly because the scope of the study focus on the situation under analysis and no concerns for generalization are made explicit at this stage.

In addition, the presented research questions were used to guide a literature review, which supported the definition of the questions to be asked in two exploratory qualitative data collection situations, as follows: (i) one focus group made up by four participants and one moderator, one of the researchers. All participants are part of the sponsor company, i.e. the DATASHIELD DPBCS, and they act professionally as Data Protection Officers (DPO); (ii) eight semi-structured interviews led by the same researcher made to DPO working within the Portuguese context. DPO are individuals designated by the organization on the basis of professional competencies and, in particular, of expert knowledge on data protection law and practices (Regulation EU, 2016).

Data treatment and analysis was positioned under an interpretivist stance. It was supported by the use of the Vivo12 Plus software. In addition, visual representations were used adding more meaning to the findings. Moreover, the data analysis process occurred in the following steps: to produce audio transcriptions and to become familiar with the data, coding, and searching for themes, patterns and relationships. Chosen themes will be strongly justified by extant research. Finally, the themes were refined in order to be able to progress towards valid and firm foundation conclusions regarding the initial research questions.

Illustrative results and conclusions

This research addresses the [RQ1] *What are the high-level requirements of the permanent organization to be GDPR compliant? and* [RQ2] *How should be the GDPR requirements managed in the permanent organisation?* Thus, a qualitative study was carried out. An interdisciplinary literature review on the General Data Protection Regulation (GDPR) recitals and articles, on the data protection and privacy body of knowledge, and on security of processing was pursued. The interdisciplinary approach resulted into the melding the aforementioned knowledge with the literature related to privacy management. Outcomes are, as follows: (i) privacy requirements are supported by privacy principles and by privacy strategy [RQ1], (ii) organizational enablers (permanent and temporary) contribute and seek to construct the privacy purpose in a positive-sum manner [RQ2], (iii) privacy maturity models are acknowledged as a means by which organizational privacy progress can be measured against their organizational and technical implemented measures [RQ2], (iv) there is a gap regarding a generally recognized privacy management method [RQ2], i.e. a means by which the elements of the method described are applicable to most organizations most of the time, and there is agreement about its value and utility. The authors argue for PRIMROSE as an organised way to decrease the probability of risk occurrence, as well as its negative impacts, that are associated with this privacy management gap [RQ2].

Moreover, the focus group that was put together and eight semi-structured interviews confirmed these findings from the literature review. In addition, interviewees added new perspectives, namely: (1) they referred the existence of a common set of requirements on a relevant number of organizations most of the time. However, they also raised the need for specific descriptions of sectoral sets of requirements, e.g. health, education, insurances and so on; it is recognised that this sectoral set of requirements should be developed as

extensions of PRIMROSE, by interpreting additional specific issues and risks and by expanding the precepts of privacy management defined in PRIMROSE to specific sector needs [RQ1]. (2) Interviewees confirmation also allowed to explore and develop the semantics of the method root definitions, e.g. the proposed principles, stages, processes, enablers and high-level requirements elaborated as a function of the privacy environment [RQ1;RQ2]. (3) *Multidisciplinarity* [RQ2] was required to face the challenges that privacy and data protection demands. However, findings from the focus group brought forward for reflection *interdisciplinarity* instead [RQ2], in order to draw a bridge between disciplines and to become a truly integrated and coherent whole. Further research reflections also suggest *transdisciplinarity* as a required configuration of knowledge in the privacy and data protection curriculum to be analysed. (4) At the time of this investigation, the lack of national legislation, i.e. in Portugal, both in the public and private sectors, is often highlighted as an argument for the organizational leaders and executives postpone and not allocate the necessary resources to satisfy the privacy requirements in their business. (5) Interviewees clearly expressed that the State should give the example. (6) Careful consideration should be made regarding the primacy of the European Union law, as it functions as a principle aiming to assure uniform appliance of European Union legislation within the Member States.

As recommendation for further work, this investigation suggests that the pursued paths should be improved and further extended. The method should be progressively more elaborated, as far as optimizations and adjustments might occur, and as details and relationships become clearer. Moreover, it is expected that the presented descriptive model should generate several analytical ones with more limited scopes.

Finally, the meaning of what constitutes the success of data protection or privacy measures should be further investigated from the perceptions of the relevant interested parties, i.e. the stakeholders (Costa et al. 2017; Costa et al. 2018).

In summary, this assignment operationalised an exploratory research to address the general high-level requirements for organizational privacy resilience by proposing an innovative privacy management method positioned within the scope of an original conceptual model previously introduced by the authors (please *vide* Costa et al., 2017; Costa et al., 2018). It is believed that this might suggest a relevant contribution to the practitioner, because guidance to a more systematic diagnosis, design, implementation, operation, monitoring and controlling procedure concerning privacy management might come out. This method is also considered as an advancement to data privacy theory due to its originality. In addition, research as a path to avoid abusive prescriptions to real world problem-situations has also been valued through the outlined investigation.

Main references[1]

BS10012:2017, *Data protection - Specification for a personal information management system. Specification for a personal information management system*, The British Standards Institution.

Cavoukian, A. (2013), "Privacy by design", *Inf. and Privacy Commissioner of Ontario*, Canada, Available at: https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf. Accessed on 11/04/2018.

Costa, N., Vilas-Boas, J., Almeida, I. (2017), "Key drivers of project management success when applied to temporary multi-organizations", in *24th EurOMA Proceedings*, Heriot Watt University, Edinburgh.

Costa, N., Vilas-Boas, J., Möhring, M., Almeida, I. (2018), "Definition of key drivers for project success regarding the General Data Protection Regulation (GDPR)", in *25th Annual EurOMA Proceedings*, Hungarian Academy of Sciences, Budapest, Hungary.

[1] The complete list of references supporting the text can be found at the following address: https://bibliographyprimrose.wordpress.com/, despite it might also be supplied by the authors, on demand.