ISCTE IUL
Instituto Universitário de Lisboa

Department of Information Science and Technology

Information Security Frameworks Assisting GDPR Compliance in Bank Industry

João Filipe Virtuoso Serrado

Dissertation submitted as partial fulfilment of the requirements for the degree of

Master in Computer Engineering

Supervisor:
Doctor Rúben Filipe de Sousa Pereira, Assistant Professor
ISCTE-IUL

October, 2019

Acknowledges

I would like to thank my supervisor, Prof. Dr. Rúben Filipe de Sousa Pereira, for the amazing support during this research, the availability and incentives. Without his help, I believe I wouldn't finished it.

Thanks to all the interviewees and the banks who collaborated in this investigation. Their help was very useful to evaluate this research and how useful it is.

Finally, I big thank you to my family and friends. A very special thank you to my parents and my brother.

Resumo

Nos últimos anos com o consequente aumento do uso de Tecnologias de Informação (TI) pela população, assistimos a um aumento da recolha e tratamento dos dados por parte das organizações, destinando-se a diversos fins, como por exemplo, para a necessária prestação de serviços ou campanhas de *marketing*.

Como consequência do aumento de dados, têm existido diversas tentativas de roubo dos mesmos para se vender ou pedir resgates às organizações. Esta situação tem revelado que as organizações no que respeita à segurança e proteção de dados nem todas têm o mesmo grau de maturidade, sendo que um aspeto também determinante é a legislação existente não ser a mais adequada para o nível de utilização das TI nos dias de hoje.

Para colmatar estas falhas a União Europeia (UE) decidiu criar o Regulamento Geral de Proteção de Dados (RGPD), com entrada em vigor a 25 de maio de 2018, aplicável a todos as organizações que tratam dados pessoais de cidadãos residentes na União Europeia (EU). Com efeito as organizações conjugam todos os seus esforços para a implementação deste novo regulamento, de forma a que não sejam aplicadas multas por incumprimento ao mesmo.

À imagem do que foi descrito anteriormente e com base num conjunto de boas práticas e *frameworks* existentes sobre segurança da informação atualmente no mercado, esta tese propõe explorar como os *frameworks* de segurança da informação podem ajudar os bancos a cumprir com o RGPD, através do mapeamento dos requisitos do regulamento com as práticas dos *frameworks*. Numa segunda fase realizar-se-á entrevistas com responsáveis na matéria, num setor específico onde existe mais sensibilidade no que toca a estes temas, o setor da banca.

Palavras-Chave: GDPR, Proteção de Dados, Segurança de Informação, *Frameworks*.

Abstract

In the last years, with the consequent increase use of Information Technology (IT) by the population, we watched an increase in the collection and processing of data by the organizations, for various purposes, such as for example the necessary provision of services or marketing campaigns.

As a result of the increase of data, there have been several attempts to steal the data to sell or request redemptions from organizations. This situation has shown that organizations as regards data protection and security do not all have the same degree of maturity, and a determining aspect is also that the existing legislation is not the most adequate for the level of IT use in the days of today.

To address these issues, the European Union (EU) decided to create the General Data Protection Regulation (GDPR), which entered into force on May 25, 2018, applicable to all organizations dealing with personal data of citizens residing in the European Union. In effect, the organizations combine all their efforts for the implementation of this new regulation, so that fines for non-compliance are not applied.

Based on the previous description and with base on a set of best practices and existing frameworks of information security existent currently in the market, this thesis aims to explore how can current IS frameworks help Banks comply with GDPR by mapping the requirements of the regulation with the practices of the frameworks. In a second phase, interviews will be conducted with professionals in the field, in a specific sector where there is more sensitivity for these topics, the bank industry.

Keywords: GDPR, Data Protection, Information Security, *Frameworks*.

Index

Table Index

Figure Index

List of Abbreviations

DP	Data Protection
DPA	Data Protection Authority
DPR	Data Privacy
DS	Data Subject
EC	European Commission
EU	European Union
FATCA	Foreign Account Tax Compliance Act
GDPR	General Data Protection Regulation
IoT	Internet of Things
IS	Information Security
IT	Information Technology
PD	Personal Data
PI	Personal Information
SCPD	Special Category Personal Data
US	United States

Chapter 1 – Introduction

The rapid development of computers in the last 20 years, with the reduced prices for data storage, allows the processing of large amounts of personal data (PD), with the help of big data and data science, to use or exploit them late. Plus, with the large volume of PD collected, companies are facing serious vulnerabilities, like the misuse, that could result in privacy breaches (Agarwal, 2016).

The roles between governments, data subject (DS) rights, and data protections authorities (DPA) are different across the countries, due to significant levels of enforcement and legal competencies (Custers, Dechesne, Sears, Tani, & van der Hof, 2018). Therefore, The European Union (EU) published their own directive for data protection (DP), since the adoption in 1995, the Data Protection Directive 95/46/EC (Council, 1995) has been the central legislative for personal data privacy (DPR) instrument in the EU (Tikkinen-Piri, Rohunen, & Markkula, 2018). Considering this is not a regulation, all member states must translate it into local laws, which makes a non-uniformization of the laws across EU.

Since its inception, DP has, in turn, been driven by the development of information technology (IT) (Phillips, 2018), and in the last years with the increase use of IT by the citizens, in particularly the residents in EU, the Data Protection Directive 95/46/EC no longer meets the privacy requirements of the present-day digital environment. To solve this problem the European Commission (EC) has been developing, since 2009, the General Data Protection Regulation (GDPR), that has published a proposal for the DP reform in 2012 (Tikkinen-Piri et al., 2018).

In May 2018, the GDPR came into effect to replace the Data Protection Directive 95/46/EC, to meet current challenges related to personal DP and to harmonise DP across the EU (Tikkinen-Piri et al., 2018).

One major difference from the old directive is, that GDPR is a regulation and not a directive. This means that it will apply directly in all member states without them translating it into local laws. One of the main objectives of GDPR is to lead to consistency of DP in EU and this justifies the transition from a Directive to Regulation (Malatras et al., 2017).

As this regulation is currently available only in the textual format, it will require significant human and time effort to adhere to it. The regulation challenge the way that companies process data, where our data is a product companies trade and sell (Krempel & Beyerer, 2018). Therefore, since every industry has their own specifications (for instance, financial services or healthcare), and since GDPR is not regulated by a specific sector, once again it requires significant time effort to understand the specific requirements of each industry.

1.1.Problem and Motivation

The transformation to digital society and digital economy is one of the consequences of ongoing process of digitalisation and globalisation. The creation of digital single market in EU has motivated that digital economy in EU has become increasingly reliant on the control and processing of personal data. This progression creates enormous opportunities for business, but in another way leaves open serious issues like the implementation of new technologies, and the increasing public awareness and concern for the importance of personal DP (Ri et al., 2018), and generate serious privacy, trust and security risks (Teixeira, 2018). To answer these challenges nowadays exists in the market a set of IS frameworks to improve the security and enhancing the following approaches (Srinivas, Kumar, & Kumar, 2019):

- Improve the efficiency and effectiveness of key processes;
- Facilitate the systems integration and interoperability;
- Entitle various products or methods, which need to be compared significantly;
- Provide a means for users to evaluate new products/services;
- Structure the method to deploy new technologies/business models;
- Simplify complex environments.

The lack of trust can reduce the development, use and adoption of new technologies (Reding, 2010), and many new business opportunities may be missed if appropriate DP practices are not implemented (Ayala-rivera & Pasquale, 2018). So the GDPR came to bring and benefit companies by offering data protection practices across the EU member states and others that deal with personal data of EU citizens and by enabling more integrated EU DP policies (Tikkinen-Piri et al., 2018), moreover the adoption of the requirements in addition to ensuring compliance with the GDPR also brings competitive advantage to the companies.

The GDPR aims to meet the current challenges related to PD, consolidate online privacy rights and improvement Europe digital economy, and provide individuals with better capabilities for controlling and managing their PD (Mantelero, 2013), hence striving to reinforce the DS trust in PD collecting companies. Within the new DP framework, individual service users may also benefit from the free movement of data if it results in growing businesses with improved and personalised services (Ayala-rivera & Pasquale, 2018).

Nowadays, companies collect, process and interlink data in an expanded way (Reding, 2010). The appearance and mass usage of Internet of Things (IoT) and cloud computing that are available online to EU citizens, has increased the security risks related to personal information (PI) data breaches. In the past years there have been many security incidents lately and they serve to highlight the challenges that exist related to IS, DP and DPR of EU citizens.

1.2. Research Objectives

DP laws have been growing up since the 1960s, with the development of PD collection and processing technologies, but in the EU this law is not fragmented by specific sector, that means they must be generic for all sectors that deal with PD.

Subsequently the bank industry is one of the most regulated industries in the world, mainly because the giant reserves of rich data and its large scope for ambitious hackers, the DS expect their PD to be secure and protected by the most robust processes and technologies, which means that information security (IS) must be the number one priority throughout this industry to ensure that all transactional processes are efficient, reliable, secure and compliant (Sydekum & Networks, 2018).

Based on this information and since companies need to rearrange their own processes and technologies to be compliant with GDPR, especially a set of critical sectors, this investigation focus on bank industry.

Therefore, this research aims to explore how can current IS frameworks help Banks comply with GDPR.

1.3. Methodology Approach

The methodology used in this research is the Design Science Research (DSR). A literature review was performed to collect the information available in literature/papers.

Moreover, presential interviews with experts in the bank industry will be conducted to demonstrate and evaluate the proposed artefact.

1.4. Structure of the Master Thesis

This master thesis is composed in nine chapters, in the first chapter is the introduction and research objective. The second chapter is a theoretical background about GDPR and IS frameworks. The third chapter is about the related work. The fourth chapter is about the research methodology that is used in this research. The fifth and sixth chapter is the design and development. The seventh chapter is the demonstration and evaluation with the interviews that will be performed, proceeding by the eighth chapter analysis and discussion of results. For the last chapter is the conclusions to present the main findings of the research and the future work.

Chapter 2 – Theoretical Background

The definitions of the main concepts used in this research are summarized in this section. The sub-chapters detailed bellow are GDPR and IS Frameworks.

2.1. GDPR

The GDPR was designed to harmonize DP laws across Europe in order to give greater protection and capabilities to individuals for controlling their PD in the face of new technological developments. Plus, GDPR applies to all the organizations that handle PD about EU residents, regardless of their physical locations (Ayala-rivera & Pasquale, 2018).

GDPR comes with two new elements never seen before in DP. First, DP is mandatory, and fines are huge. Infringements are fined up to 20 million € or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The second part is called territorial scope. The regulation does not only apply to EU companies but to every company selling into the EU or marketing to EU citizens (Krempel & Beyerer, 2018), this means that applies to companies outside the EU, not just because they have a website accessible to a citizen in the EU, but because compliance is required when offering of goods or services to DS.

This regulation has four major focus points: accountability, transparency, protection and reliability. GDPR brings an onus to collect PD for specific purpose only, to uphold the trust of the person who gives their PD, to maintain and protect the information and to erase it when no longer required. PD and the special category personal data (SCPD) should be protected and EU is safeguarding the economic value of digitally kept information of citizens through GDPR. In the wrong hands an amalgamation of multiple data points from the same individual potentially leads to identity frauds (Philip, 2018).

Moreover, although some of the GDPR obligations were already specified in the Data Protection Directive 95/46/EC, these have mainly been perceived as “recommendations”. Therefore, most organizations have only started recently to implement measures to comply with the GDPR (Ayala-rivera & Pasquale, 2018).

So, the major challenge related to a solid implementation of the GDPR is the organizations lack awareness and understanding of the forthcoming changes and requirements that the GDPR enforces through its new rules. These requirements have various practical implications for organisational design of systems, practices and processes, as well as personnel training (awareness) and assignment of new responsibilities in the organisations (accountability). In short, it brings out the need to review the current DPR practices, technological DP measures and IS measures, as well as possibly plan new ones to ensure compliance with the GDPR (Ayala-rivera & Pasquale, 2018). Additionally frequency in communication between IS and privacy teams is considered crucial for effective overall enterprise cybersecurity (Heimes, 2016).

2.2. IS Frameworks

The exploitation of IS in organisations needs a strategic alignment with the objectives to start the implementation, in consequence the transition from the alignment to the practical implementation needs a good framework to integrate/guide these strategic goals and identify the risks that organizations are exposed (Rijsenbrij, 2019), thus frameworks are created to lead to a uniformity that are simple to understand and manage by the organizations and with this fill the gaps, in most of the times derived by the lack of inexperience that exist in human resources and the need of obligations provided by the regulator, enhancing with this the risk of penalties and providing competition with other enterprises (Al-ahmad & Mohammad, 2012).

An additional guidance on IS frameworks is that organizations can develop codes of conduct or certifications of compliance, because the GDPR expressly provides that adherence to approved codes of conduct and certifications might demonstrate compliance (Heimes, 2016).

Chapter 3 – Related Work

This section aims to explore what the scientific community has been studying regarding the application of IS frameworks in the GDPR domain or GDPR implementation.

3.1. Similar Studies

As can been seen in Table 1, seven relevant articles were found relating this research topics. From this universe, only two explore the implications during the implementation of GDPR and four explore the use of IS frameworks.

Table 1 – Related Work

ID	Author	Title	IS frameworks?	Industry
RS.1	*Tankard & Pathways (2016)*	*What the GDPR means for businesses*	*ISO 27001*	*Generic*
RS.2	*Teixeira (2018)*	*The Critical Success Factors of GDPR Implementation: a Systematic Literature Review*	*ISO 27001*	*Generic*
RS.3	*Freitas & Mira (2018)*	*GDPR Compliance in SMEs: There is much to be done*	-	*Industrial SME*
RS.4	*Krystlik (2018)*	*With GDPR, preparation is everything*	-	*Generic*
RS.5	*Wilson (2018)*	*A framework for security technology cohesion in the era of the GDPR*	-	*Generic*
RS.6	*Lopes, Guarda, & Oliveira (2019)*	*How ISO 27001 can help achieve GDPR compliance*	*ISO 27001*	*Generic*
RS.7	*Centro Nacional de Cibersegurança (2019)*	*Quadro Nacional De Referência para a Cibersegurança*	*ISO 27001 & COBIT*	*Generic*

The first research, Tankard & Pathways (2016), did a review of the barriers and consequences from not being in compliance and at the end they mention the importance of using ISO 27001. They insists that the implementation of ISO 27001 can force the appropriate measures and technological help that organizations need, as well, defining responsibilities in the organizations about who can have access to the data and showing for the exterior that they have more credibility.

The second research, Teixeira (2018) performed a systematic literature review in order to identify the critical success factors that contribute for GDPR implementation. The main goal of this review is to find the barriers and enablers so that the organizations can prioritize their GDPR compliance program. The author refers the ISO 27001 as an internationally recognized IS framework and as it may help the organizations to ensure the appropriate level of desired security to safe their PI.

The third research, (Freitas & Mira, 2018) is related to the state of the art of GDPR implementation, in small and medium-sized Portuguese organizations and her level of knowledge in the subject. This exploratory study is performed by means of presential interviews with the senior official of each company. At the end of the study the authors highlighted the low maturity (10%) on GDPR knowledge among the interviewed organizations. Drawing special attention to the fact that organizations need to restructure their processes and technology procedures to adapt for GDPR compliance.

The fourth author, Krystlik (2018), talks about the principal barriers implementing GDPR, such as the Shadow IT, because many organizations create databases that have PD and with this exponential growth without a correct inventory of PD can be very frustrating in compliance achievement. The article mentions other problems like the cloud and how this can have consequences of having PD in other foreign country.

Wilson (2018) calls the attention for the fact that the organizations must know where the data is, the importance of the Data Protection Officer and their responsibilities in defining policies and procedures to be in place. Another important point is the communication between the Data Protection Officer and the IT team.

Lopes, Guarda, & Oliveira (2019), is an article started due to the difficulties that companies must implement GDPR. The authors study how the implementation of ISO 27001 might represent a facilitating factor to organizations, for an easier compliance with the regulation, from a top approach with the guidelines imposed by GDPR, mostly with the objectives of ISO 27001, and how can an independent certification could help proactively manage IS risks. This article is based on information published on websites about IS and governance.

Most recently, at the end of June 2019, was published in Portugal the "Quadro Nacional de Referência para a Cibersegurança" (QNRCS), from the Centro Nacional de

Cibersegurança, which is a generic framework for all types of organizations that aggregates all the best practices used by the principal IS frameworks. This work is not specific for GDPR because her own focus is cybersecurity, i.e. do not cover only DP/DPR. QNRSC has 5 main goals for security: identify; protect; detect; answer and recover.

3.2. Synthesis of the Related Work

Overall, the related articles mention the difficulties about implementing GDPR and the lack of awareness among companies. This happen because GDPR is a recent subject and concrete measures are not mentioned, appealing for implementing the requirements according to the level of risk that they have, for all the industries managing PD.

Plus, four studies argue that IS frameworks (ISO 27001 or COBIT) may help organizations achieving the level of compliance desired by GDPR, since the IS frameworks is not new and offers more concrete guidelines for implementing IS measures, reducing the risk of data breaches. However, none of these studies provide insights on how these IS Frameworks can do it.

As one can see in Table 1, there is no related work investigating how can IS frameworks help in GDPR compliance. Moreover, the few existent researches focus on the preparation without using IS frameworks and are generic to all industries.

To sum up, there is studies pointing IS Frameworks as useful to help companies comply with GDPR but no studies provide practical insights on how that can be done. This research intends to contribute with novel insights on how IS Frameworks can help companies. In this case it will be focused on Bank Industry.

Chapter 4 – Research Methodology

This research applies the DSR in order to design, build and evaluate how can current IS frameworks help Banks comply with GDPR.

Since this research purposes to expand the limits of human capacities and organizations, to create the artefacts invoking the Design Science Research Methodology (DSRM) is the right choice (Hevner, March, Park, & Ram, 2004). Plus, the DSR methodology consist in three more elements, the conceptual principles that help define the DSR, practical rules for DSR impersonation and procedures to perform and conduct the research (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007).

The DSR process applied in this research can be seen in more detail in Figure 1.

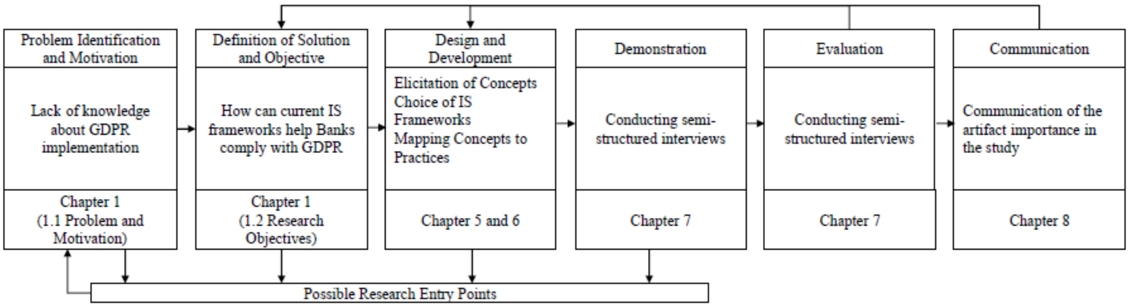

Problem Identification and Motivation
Lack of knowledge about GDPR implementation
Chapter 1 (1.1 Problem and Motivation)
Definition of Solution and Objective
How can current IS frameworks help Banks comply with GDPR
Chapter 1 (1.2 Research Objectives)
Design and Development
Elicitation of Concepts Choice of IS Frameworks Mapping Concepts to Practices
Chapter 5 and 6
Demonstration
Conducting semi-structured interviews
Chapter 7
Evaluation
Conducting semi-structured interviews
Chapter 7
Communication
Communication of the artifact importance in the study
Chapter 8
Possible Research Entry Points

Figure 1 – DRS Process Model

The first two activities of this process have already been mentioned, in the respective chapters. The remaining DSR process is organized as follows.

In the design and development activity, is where all the design of the proposed artefact is done and the practical development of the same. Initially, the artefact is theoretically constructed, in other words, the IS frameworks model that will help in the implementation of GDPR in the bank industry is designed, through an instantiation of the artefact. Then, in the practical part, the development of the proposed artefact is made, based on the inputs of previous activities.

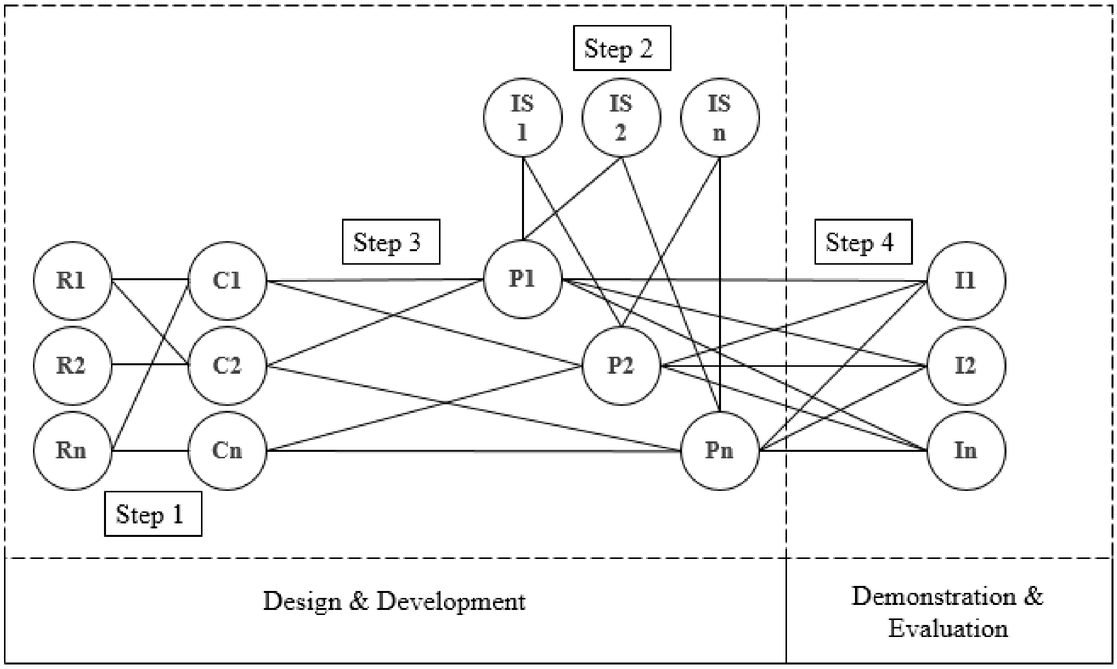
The demonstration and evaluation phase are where the validation of the artefact developed throughout this research will be performed. By conducting semi-structured interviews, a validation of the work developed is done, as well as the demonstration that it can be applied in the bank industry, by collecting the practices proposed in the research and already used by the interviewees. The interviewees are experienced professionals in the areas of DP or IS and all of them work in the bank industry.

Finally, in the communication, is presented a list of the main findings throughout this research and what are the key aspects that differentiate the banking industry from the requirements imposed by the GDPR.

Chapter 5 – Design

The focus of this research starts with the GDPR and the fact that is generic for all industries, IS Frameworks and the Bank industry. After the research work, it was not found in the scientific community, a set of IS frameworks to assist GDPR compliance in the Bank industry, because the GDPR requirements are generic for all industries. In attendance that the banks are changing their information systems, processes and methodologies to become GDPR compliant, there is a need in banks to more specific guidelines for implementing the GDPR.

Figure 2 synthesizes the Design of the proposed artefact. Four steps were performed sequentially. The final step was used to demonstrate and evaluate the proposed artefact.



R – Requirement (Requirements from the GDPR, i.e., the articles); C – Concept (Concepts that can be extracted from the requirements); IS - Information Security Frameworks (IS frameworks that exists in the market); P – Practices (Practices or controls from the IS Frameworks); I – Interview (Presential interviews to obtain qualitative data to the research)

Figure 2 –Diagram of the Design

In the following chapters will be explained the steps, that are related to the Objectives of this research.

5.1. Step 1 – Elicitation of the List of Concepts

The first part of the design consists in reading all the GDPR regulation (11 chapters and 99 articles) and from each of them extracting concepts that are related to the security of data, DP and rights of DS.

It must be noted that articles related to DPA obligations, such as for example investigations carried out to data breaches, penalties that could be applied to organizations, etc, were not considered.

5.2. Step 2 – Choice of IS Frameworks

Several IS frameworks exist, that despite not mandatory some could be certified to attest the compliance of the organizations with IS requirements. These frameworks offer a solid base to start implementing IS in the organizations, offering structures and practices not present in GDPR.

5.3. Step 3 – Mapping Concepts with Framework Practices

After complete Step 1 and Step 2 it was time to map the concepts with each IS framework. For each elicited concept, one or more practices from the frameworks were selected when met the requirement of the concept. The goal was for each concept, that GDPR do not give any specific instruction on how to implement them, find practices that give more precise instructions and can be applied to the bank industry in order to achieve the appropriate level of compliance.

5.4. Step 4 - Conducting Semi-structured Interviews

This step aimed to demonstrate and evaluate the applicability of the artefact with experts in the area, i.e. that have experience in the bank industry and in GDPR. Therefore, the qualitative method interview was chosen to assess if the proposed artefact is suitable to help Banks comply with GDPR.

The goal of interviews is to collect data that cannot be obtained using quantitative methods, interviewing people that gives insight into the subject studied and their opinion (Hove, 2005).

Several types of interviews exist like structured interviews, semi-structured interviews and non-structured interviews. In structured interviews, the interviewer has all the questions and only need the response, they are fairly straightforward, like an “if-then-else” (Seaman, 1999). The non-structured interview has the goal to obtain as much information on the topic as possible without a defined set of questions but can have a large coast and not comparable results (Seaman, 1999). Last but not least, the semi-structured interview is a hybrid between the last two types of interviews, i.e. they start with a specific set of questions, but the interviewer can gather unexpected information to be used in the study, and is good to be used in exploratory studies (Seaman, 1999).

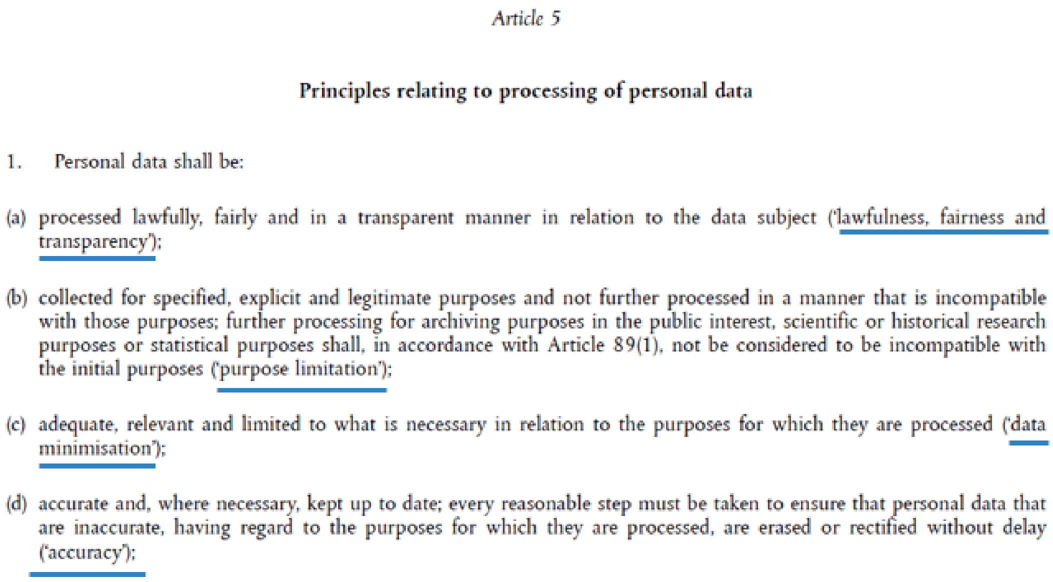
For this research, individual semi-structured will be used since this study has an exploratory strand. To obtain more information and validate the practices that are applied in the bank industry, the questions are open-ended, asking other information when necessary. Another additional point is that the interviews will be conducted individual and in presence.

Chapter 6 – Development

This research aims to explore how can current IS frameworks help banks comply with GDPR. To answer this, the next sub-chapters will provide the necessary knowledge and evidences about the artefact developed.

6.1. Step 1 – Elicitation of the List of Concepts

The first part of the artefact consists in extracting from the GDPR articles/requirements all the concepts that are related to the security of data, DP and rights of DS. For example in the below image (Figure 3), can be seen the following concepts: Lawfulness, Fairness and Transparency, Purpose Limitation, etc, that are present in the Table 3 and in Annex A with the full description of each concept.



Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

Figure 3 – Example of elicited concepts from article 5

It should be noted that both the same concept can be elicited from more than one article and one article could have more than one concept, as can be seen in Annex A.

Table 2 – Chapters of GDPR

Chapters with Concepts	*Principles;*
	Rights of the data subject;
	Controller and processor;
	Transfers of personal data to third countries or international organisations;

Chapters without Concepts	General provisions;
	Independent supervisory authorities;
	Cooperation and consistency;
	Remedies, liability and penalties;
	Provisions relating to specific processing situations;
	Delegated acts and implementing acts;
	Final provisions;

At the end of this step, 37 concepts (Annex A) were extracted from the 11 chapters (Table 2) and 99 articles that compose the GDPR. Some chapters were not considered since are not related to DPA obligations (for example, independent supervisory authorities or penalties that could be applied to the organizations and other subjects) and therefore are not directly related to the mandatory requirements of the organizations.

Table 3 – Example of extracted concepts from GDPR

Concepts
Lawfulness, fairness and transparency
Data Minimisation
Inaccurate Data
Storage Limitation
….

6.2. Step 2 – Choice of IS Frameworks

From the list of IS frameworks existent in the market, the following four frameworks were chosen to ground the remaining steps of the research:

- ISO/IEC 27001:2013 (ISO/IEC, 2013) - Information technology - Security techniques - Information security management systems - Requirements
- ISO 27552 (ISO/IEC DIS 27552, 2019) - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
- NIST SP 800-53 rev.4 (NIST, 2015) - Security and Privacy Controls for Federal Information Systems and Organizations

- COBIT 2019 Framework (Cobit, 2019) - Governance and Management Objectives

The most know/used frameworks are ISO/IEC 27001:2013, that is the most used in the Europe by professionals, and NIST SP 800-53 that is more used in the US since it was created in the agency of the United States Department.

COBIT is the most used by IT professionals in IT Governance and addresses topics related to security of data. In 2019, a new version was released with updated practices regarding security aspects.

For last, ISO 27552 is a new framework, that is an extension of the ISO/IEC 27001:2013 and address the DPR and in especial the GDPR requirements. Since this is a new framework, it is only available right now in a draft.

In this research the practices are the controls from ISO 27001, NIST SP 800-53 and ISO 27552 or the activities from COBIT.

6.3. Step 3 – Mapping Concepts with Framework Practices

In this step, individually, for each of the identified concepts, was performed a research of the practices presented in every IS Framework, in order to check if the practice can fulfil the level of compliance.

The goal is from each of the concept, that do not give any specific instruction to implement them, find practices that give more precise instructions and can be applied to the bank industry to achieve the level of compliance. In case the practice fulfils the requirement of the concept, then it would add to the list (Annex B).

In Annex B can be seen the full list of the practices mapped to the each of the concepts. Some practices were used more than one time because they can be used to comply with more than one concept, and as we will see in the next section, some may not be the indicated for the concept or may not be applied in the bank industry.

Not all the concepts could be mapped with at least one practice from each framework, since there are some subjects that the frameworks do not cover at 100 percent, such as for example the concept "Lawfulness, fairness and transparency", in the Table 4, that is not covered by the ISO/IEC 27001:2013.

Table 4 – Example of a concept with the practices

Article	Paragraph/ Line	Concept	ISO 27552	ISO 27001:2013	COBIT 2019	NIST SP 800-53 v4
5	*1-A*	*Lawfulness, fairness and transparency*	*7.2.2 - Identify lawful basis* *8.2.2 - Organization's purposes*	-	*EDM05.02 - Direct stakeholder engagement, communication and reporting*	*AP-2 - Purpose Specification*

Chapter 7 – Demonstration and Evaluation

After the development of the artefact, it's time to research possible contacts, who works in the bank industry and available for an interview, to do the demonstration and evaluation.

For the choice of interviewees, two methods where used:

- Personal contact list;
- LinkedIn professional contact network.

After the search, 11 possible banks were found, with at least one person to be interviewed. After the invitation was sent, six banks accept to participate in the study, and one of them with two people available for the interview. Table 5 shows the list of banks identified, how many accepted and the number of conducted interviews.

Table 5 – Selected banks overview

Bank	Contact Type	Accepted?	Interviewees
B.1	*Personal Contact*	*Yes*	*2*
B.2	*Personal Contact*	*Yes*	*1*
B.3	*Personal Contact*	*Yes*	*1*
B.4	*Personal Contact*	*Yes*	*1*
B.5	*Personal Contact*	*Yes*	*1*
B.6	*Personal Contact*	*Yes*	*1*
B.7	*Personal Contact*	*No*	-
B.8	*Personal Contact*	*No*	-
B.9	*LinkedIn*	*No*	-
B.10	*LinkedIn*	*No*	-
B.11	*LinkedIn*	*No*	-

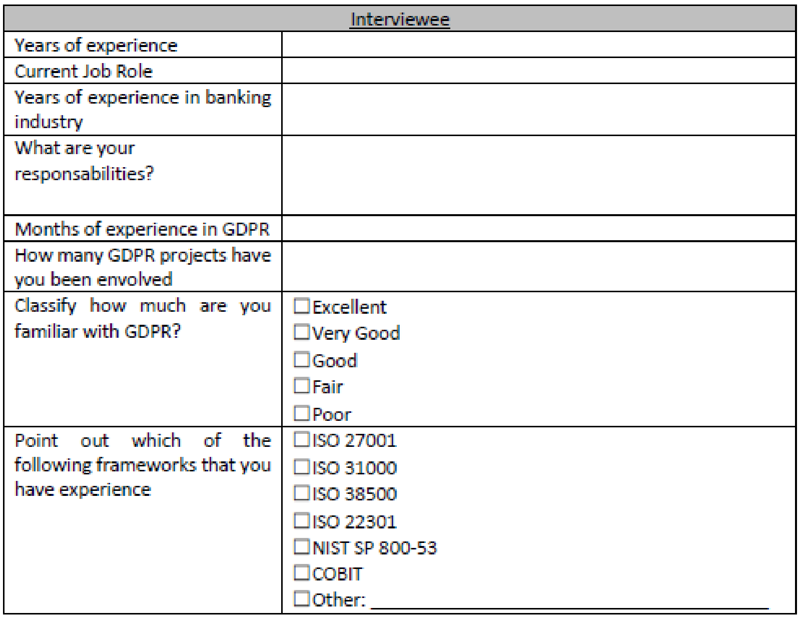
The interviews were conducted in person on the headquarters of six Portuguese banks, with a total of seven interviewees, from different departments, responsibilities and years of experience. All the selected interviewees have both knowledge in GDPR, DP and IS.

The goal of the interviews is to demonstrate and evaluate the developed artefact, to understand the following things:

- Is there any concept missing?
- The practice(s) are applicable to the related concept in the bank industry, and fulfil the concept?
- Is there any gap that does not allow for compliance with these practices?

To conduct this interview, a questionnaire was developed, as can be seen in Annex C, with the following structure. First, the header of the questionnaire is composed by generic questions (Table 6), to certify the experience of the interviewee in the bank industry and GDPR.

Table 6 – Interviewee specific questions



Interviewee	
Years of experience	
Current Job Role	
Years of experience in banking industry	
What are your responsabilities?	
Months of experience in GDPR	
How many GDPR projects have you been envolved	
Classify how much are you familiar with GDPR?	☐Excellent ☐Very Good ☐Good ☐Fair ☐Poor
Point out which of the following frameworks that you have experience	☐ISO 27001 ☐ISO 31000 ☐ISO 38500 ☐ISO 22301 ☐NIST SP 800-53 ☐COBIT ☐Other: ______________________________

Additionally, directed to the bank exists a set of four specific questions related to the number of employees and frameworks that the bank follow/perform.

For each practice mapped to a concept, one question is made, to understand if the practice fulfils de concept, always in the bank industry. In each of these questions the interviewee must point out if the practice in the following concept is:

- Not Applicable (N/A) – If the practice is not applicable to the concept in the bank industry, or, if the practice is not applicable for this concept because it is not in the scope of them;
- Partially Compliant (PC) – In case of the selected practice do not meet all the requirement that the concept needs to meet, in the bank industry;
- Fully Compliant (FC) – If the practices fulfil at 100% the requirements of the concept in the bank industry.

Additionally, is proposed to be answered by the interviewee, if the practice is being implemented at their bank, in order to do the evaluation, with the following options:

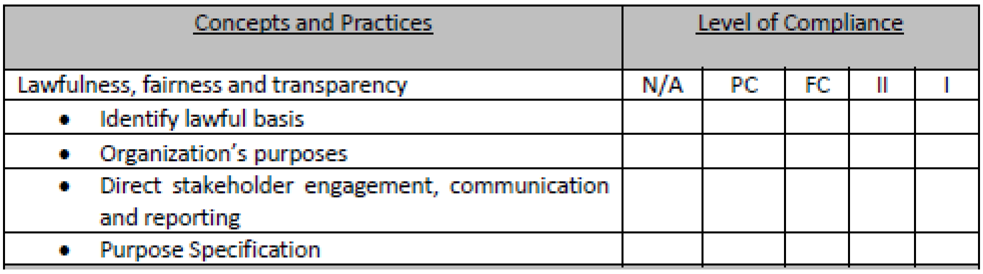
- In Implementation (II) – If the bank is implementing this practice;

- Implemented (I) – In the case of the bank already implemented them.

Plus, the frameworks studied are not exposed to the interviewees until the end of the interview, due to possible influence on their own answers.

Table 7 lists an example of the first concept and their mapped practices with the possible questions to be answered by the interviewees. In addition to these questions and whenever as possible, additional information was gathered about the concepts and practices in the bank industry, as well as feedback about the implementation of the practices.

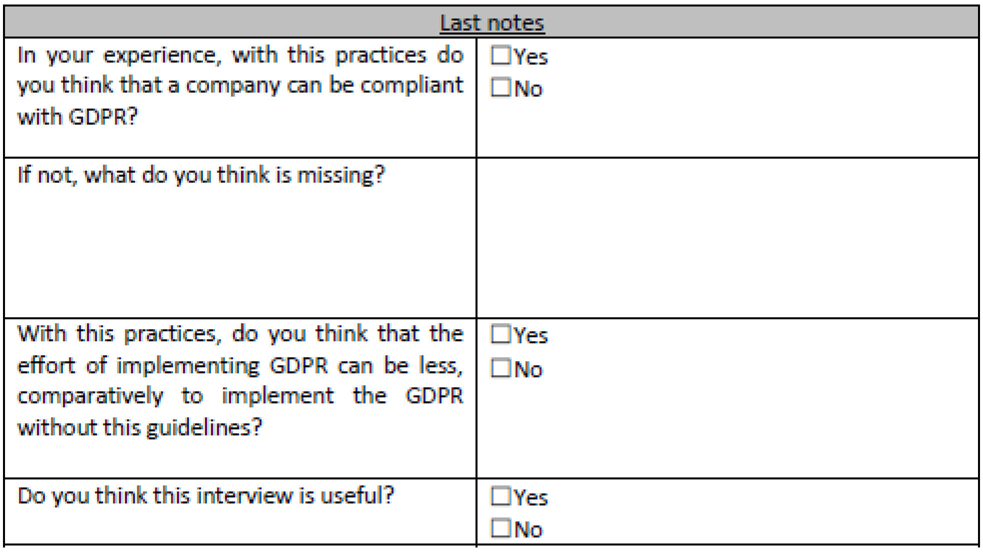
Table 7 – Concepts and practices question



Concepts and Practices	Level of Compliance				
Lawfulness, fairness and transparency	N/A	PC	FC	II	I
• Identify lawful basis					
• Organization's purposes					
• Direct stakeholder engagement, communication and reporting					
• Purpose Specification					

At the end of the interview (Table 8), each interviewee was asked if with this concepts and practices, once again in the bank industry, they could be compliant with GDPR, if the implementation effort would be smaller and if the interview is useful.

Table 8 – Last notes



Last notes	
In your experience, with this practices do you think that a company can be compliant with GDPR?	☐Yes ☐No
If not, what do you think is missing?	
With this practices, do you think that the effort of implementing GDPR can be less, comparatively to implement the GDPR without this guidelines?	☐Yes ☐No
Do you think this interview is useful?	☐Yes ☐No

As mentioned earlier, the interviews were performed in six Portuguese banks, for a total of seven interviewees, from different departments, responsibilities and years of experience. Once again, the selected interviewees participated in at least one GDPR project, and their professional experience is from IS or DP. Their current roles are the following:

- Chief Information Security Officer;
- Data Protection Officer;
- IT Auditor;
- Responsible of Risk and Security of IS/IT;
- Senior Manager of IS/IT.

In Table 9 it is possible to see an overview of interviewees, as well as their knowledge in GDPR and frameworks. Regarding the evaluation made by the interviewees about their knowledge of GDPR, it is normal to have dissonances between the experience (months) and the given evaluation, as it will depend on the feeling of each one and the degree of involvement of them in the projects, during this period of months.

The duration of the interviews in average was 1 hour and 30 minutes. The shortest took 1 hour and the longest took 2 hours and 30 minutes. The total of interviews duration was 12 hours.

Table 9 – Interviewees comparation

Interview	Years of Experience	Role	Years of experience in bank industry	Months experience in GDPR	Number of GDPR projects	How much are familiar with GDPR (*)	Frameworks in which they have experience	Interview duration
I.1	*8*	*IT Auditor*	*8*	*12*	*1*	*Good*	*ISO 27001; ISO 31000; ISO 22301; COBIT; NIST Cybersecurity Framework*	*1:30*
I.2	*13*	*IT Auditor*	*13*	*12*	*1*	*Good*	*ISO 27001; NIST SP 800-53; COBIT; ITIL*	*1:00*
I.3	*15*	*Senior Manager of IS/IT*	*12*	*26*	*2*	*Very Good*	*ISO 27001; ISO 31000; ISO 22301*	*1:30*
I.4	*14*	*DPO*	*12*	*10*	*1*	*Very Good*	*ISO 27001; COBIT*	*1:30*
I.5	*25*	*CISO*	*19*	*30*	*2*	*Good*	*ISO 27001; ISO 31000; ISO 38500; ISO 22301; COBIT; ISO 20000; ISO 9001; ISO 14000*	*2:00*
I.6	*26*	*DPO*	*26*	*30*	*1*	*Very Good*	*ISO 27001; NIST SP 800-53; ISO 27005*	*2:00*
I.7	*33*	*Responsible of Risk and Security of IS/IT*	*30*	*30*	*1*	*Good*	*ISO 27001; ISO 22301; COBIT*	*2:30*

*Scale = Excellent; Very Good; Good; Fair; Poor;

From the banks that participated in this study, half have more than 500 employees, as shown in Figure 4. Plus, all banks are present in Portugal and four of them have international presence.

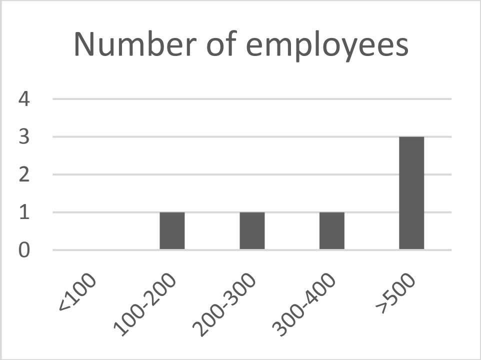


Figure 4 – Number of employees

The interviewees said that all the banks follow/perform a framework or best practice. The most used framework among the interviewed banks is ISO 27001, with the justification that is the IS framework of reference in Europe. The second most used framework is COBIT, related to IT governance and IS, this framework is widely used by IT auditors as a reference for the processes to be audited in the bank industry.

Figure 5 shows the distribution of used frameworks in the banks. This list is not restricted only to IS frameworks.

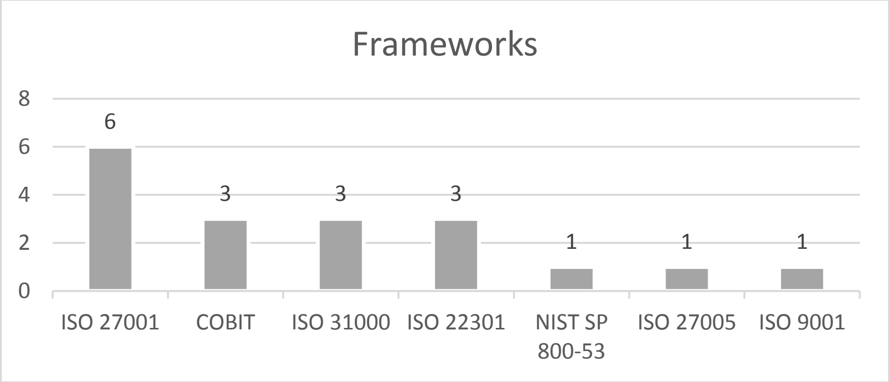


Figure 5 – Frameworks followed/performed in the banks

As can be seen, most of the banks are of a considerable size, with a strong international presence, which requires compliance with more laws than those required in Portugal. Another important point, is that all the banks already follow one IS framework, as is the case of ISO 27001 which is present in all banks, although they don't implement everything. Additionally, there is a strong concern in this industry for compliance with this type of laws, in order to avoid reputational damage.

All the interviewees agreed that all the presented concepts are correct, and no further concepts were proposed as missing. Another additional point that all the interviewees agreed is that all concepts are required to be in place, but for this industry, some of them have some exceptions in their specifications, mainly due to other laws existent in this sector, that overlaps GDPR.

In a high-level evaluation, it can be stated that more than half of the banks interviewed already use most of the practices, and some may still be in implementation.

For the “Security of Personal Data” and “Security of Processing” concept, the opinion is that none of the existing practices is 100% compliant. However, the presented set of practices are the required to be compliant in the bank industry.

At the end of each interview a set of questions was performed to gather interviewees feedback on the research. This final set of questions is important for assessing the scope of this research and its usefulness.

As can be seen in Table 10, all the interviewees considered that they can be compliant with these practices. Regarding the effort required to implement GDPR, all interviewees said that the effort decrease, except for one interviewee, arguing that it will always depend on the approach of each bank, and if there is no IS framework already to be followed, the effort would be the same. For last, all the interviewees pointed this research as useful.

Table 10 – Final set of questions

	Can you be compliant with these practices?	**Would the effort of GDPR implementation decrease by implementing these practices?**	**This research is useful?**
I.1	*Yes*	*Yes*	*Yes*
I.2	*Yes*	*Yes*	*Yes*
I.3	*Yes*	*Yes*	*Yes*
I.4	*Yes*	*No*	*Yes*
I.5	*Yes*	*Yes*	*Yes*
I.6	*Yes*	*Yes*	*Yes*
I.11	*Yes*	*Yes*	*Yes*

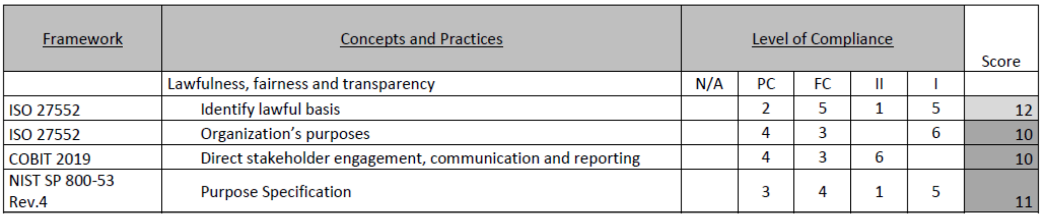
Chapter 8 – Analysis and discussion of results

Due to the existence of some questions in which there is a lot of divergence of answers by the interviewees, in this chapter a detailed analysis of the obtained results will be done.

To better support this analysis, in Annex D can be seen the sum of the answers given by the interviewees in each question. In order to separate practices into three groups (Not Applicable, Partially Compliance and Fully Compliance), a formula was created to obtain a score per practice, with the following assumptions:

- Score of each practice = (Sum of answers with N/A * 0) + (Sum of answer with PC * 1) + (Sum of answers with FC * 2)
- N/A = 0
- PC = 1
- FC = 2

For example, in Figure 6, the practice "Identity lawful basis", have 12 on score, based on this calculation (0*0) + (2*1) + (5*2) = 12



Framework	Concepts and Practices	Level of Compliance					Score
	Lawfulness, fairness and transparency	N/A	PC	FC	II	I	
ISO 27552	Identify lawful basis		2	5	1	5	12
ISO 27552	Organization's purposes		4	3		6	10
COBIT 2019	Direct stakeholder engagement, communication and reporting		4	3	6		10
NIST SP 800-53 Rev.4	Purpose Specification		3	4	1	5	11

Figure 6 – Concept and Practices with score

To differentiate the practices that are fully compliant with the concept, partially compliant or not applicable, a range of values was created, as can be seen in Table 11, based on the score formula.

Table 11 – Score Matrix

Level of Compliance	Score range	Color
N/A – Not Applicable	*0 – 7.99*	▓
PC – Partially Compliance	*8 – 11.99*	▒
FC – Fully Compliance	*12 - 14*	░

After applying the previous formula in all practices, 13 out of 37 concepts have practices that are fully compliant. This means that 35% of the concepts have at least one practice that address the entire concept in the bank industry. Table 12 lists the concepts that have at least one practice that fulfil all the requirement, with the related practice(s).

Regarding the concept “Storage Limitation”, six of the interviewees agreed that is very difficult to implement due to the existence of old systems and many dependencies between them. Plus, this inhibits the banks to delete the information after the retention period, the solution is rebuilding the systems/applications, which are currently developed in technologies already obsolete.

Regarding data portability, the interviewees all agreed that it is urgent to create a form for data portability between banks, like what is already widely used in telecommunications companies. This point despite having the fully compliant practice, is crucial to create a form for the bank industry.

The transfer of data to third parties, the bank industry, must transfer PD to other countries, such as compliance with Foreign Account Tax Compliance Act (FATCA), which requires the sending of PD about the US citizens.

Table 12 – Concepts with practices fully compliant

Concept	**Practice**
Lawfulness, fairness and transparency	*Identify lawful basis*
Storage Limitation	*Support data archiving and retention* *Data Retention and Disposal*
Accountability	*Policies for information security* *Information security roles and responsibilities*
Right of access by the data subject	*Individual Access*
Right to rectification	*Access, correction and/or erasure* *Evaluate and update or retire information*
Notification obligation regarding rectification or erasure of personal data or restriction of processing	*PII controllers' obligations and third parties*
Right to data portability	*Providing copy of PII processed*
Right to object	*Provide mechanism to object to PII processing*
Notification of a personal data breach to the supervisory authority	*Responsibilities and procedures*
Data Protection Impact Assessment	*Privacy impact assessment*
Designation of the data protection officer	*Acquire and maintain adequate and appropriate staffing* *Governance and Privacy Program*
Tasks of the data protection officer	*Establish roles and responsibilities* *Governance and Privacy Program*
General principle for transfers	*Information Sharing with Third Parties*

On the Table 13 there are the concepts that have practices with less or equal seven in their score. The information gathered during the interviews was enough to justify this low score, and most of it is due to the specifications of the industry.

All practices that refer to automated decisions have a low score, because in the bank industry there are no automated decisions, they may have some automated decisions in processes, but their final output is made by humans. For example, it's impossible to automatically decide if a mortgage loan can be decided based only in automated decision at this moment.

The concept "Information to be provided where personal data have not been obtained from the data subject", unlike other industries that collect data and sell them, such as marketing companies, the bank industry when collect data they can only obtain them from Bank of Portugal or other regulators, for effects of money laundering and terrorist financing or other debtors blacklist. In this case the data subject cannot ask for rectification or erasure because there are other laws/regulations that overlap the GDPR. If this information is incorrect, the data subject must prove the home institution, responsible for the list that the data are incorrect, and never directly to the bank.

The practice "Review effectiveness of business process controls" is not necessary because it is redundant, as there are more complete practices outlined for the concept, since it is very abstract.

The practices of the concept "Communication of a personal data breach to the data subject" had a low score solely because they are not in the context of this concept. In reporting the incident to the DS it is not necessary to say what is being done to mitigate the problem, only to the regulator.

Table 13 – Concepts with practices not applicable

Concept	Practice
Information to be provided where personal data are collected from the data subject	*Automated decision making*
Information to be provided where personal data have not been obtained from the data subject	*Provide mechanism to modify or withdraw consent* *Provide mechanism to object to processing* *Providing copy of PII processed* *Automated decision making* *System of Records Notices and Privacy Act Statements*
Right of access by the data subject	*Automated decision making* *Identify basis for international PII transfer* *Direct stakeholder engagement, communication and reporting*
Right to object	*Providing information to PII principals*
Automated individual decision-making, including profiling	*Establish data profiling methodologies, processes and tools* *Data Mining Protection*
Regularly Testing, Assessing and Evaluating	*Review effectiveness of business process controls*
Communication of a personal data breach to the data subject	*Response to information security incidents* *Define classification schemes for incidents and service requests*

As can be seen in Table 14, the average practices score per concept almost always indicates that they are in the partially compliance range, which is in line with what was said by the interviewees, that in most cases the practices complement each other to comply with the concept, in the bank industry.

The overall average of the concepts is 9.7, which is among the "partially compliance" range. There are 2 concepts that have a score below 8, because as explained earlier most of the practices do not apply in bank industry, although the concepts are necessary.

These results reinforce what was previously said by the interviewees, that the practices, with the exception of those removed (Table 13), will complement each other, thus obtaining a list of good practices, from IS frameworks, that help in GDPR implementation.

Table 14 – Practice score level per concept

Concept	Practice score level
Lawfulness, fairness and transparency	*10.75*
Data Minimisation	*10*
Innacurate Data	*9,8*
Storage Limitation	*11*
Security of Personal Data	*9,46*
Accountability	*9,92*
Transparent information, communication and modalities for the exercise of the rights of the data subject	*10,16*
Information to be provided where personal data are collected from the data subject	*9,11*
Information to be provided where personal data have not been obtained from the data subject	*7,22*
Right of access by the data subject	*9*
Right to rectification	*11,33*
Right to erasure ('right to be forgotten')	*8,75*
Right to restriction of processing	*10,4*
Notification obligation regarding rectification or erasure of personal data or restriction of processing	*10,5*
Right to data portability	*10*
Right to object	*9,2*
Automated individual decision-making, including profiling	*7,75*
Data Protection Policies	*10*
Codes of Conduct	*10,2*
Data Protection by Design	*9,12*
Data Protection by Default	*9*
Processor	*9,6*
Records of Processing Activities	*9,69*
Security of processing	*9,7*
Pseudonymisation	*9,14*
Encryption of Personal Data	*9,42*
Confidentiality, Integrity, Availability and Resilience	*10,11*
Restore the Availability	*10,25*
Regularly Testing, Assessing and Evaluating	*8,71*
Approved Certification	*9*
Notification of a personal data breach to the supervisory authority	*10,71*
Communication of a personal data breach to the data subject	*8,85*
Data Protection Impact Assessment	*9,87*
Designation of the data protection officer	*11,5*
Tasks of the data protection officer	*11*
Certification	*8,5*
General principle for transfers	*10,66*

Chapter 9 – Conclusion

This research aimed to explore how can current IS frameworks help Banks comply with GDPR. To answer this question, a research was carried out on mapping the concepts (requirements) with the practices of the IS frameworks. Then, semi-structured interviews were conducted with professionals working in the bank industry.

This research took contributions by exploring an area that was not explored previously, improving the body of knowledge about GDPR implementation with IS frameworks.

At the end, several conclusions could be withdrawn about the specificities of the bank industry, IS frameworks and the GDPR implementation. According to the evidence presented in previous chapters, one may argue that an IS framework is a good starting point to implement GDPR and getting more specific instructions, on how to implement controls to mitigate the IS and DP risk that the organizations are exposed.

In terms of particularities in the bank industry, the main findings are:

- When PD have not been obtained from the DS, the DS cannot deny the consent;
- There are not automated decisions at the end of the process;
- Storage limitation is very difficult to implement, even though is mandatory and applicable in this industry;
- There is no template for data portability between banks;
- Other laws can overlap GDPR, like FATCA, money laundering and terrorist financing, etc;
- With the use of IS frameworks the banks can develop certifications of compliance, for example if they implement the entire controls of ISO 27001, because the GDPR expressly provides that adherence to approved certifications to demonstrate compliance.

In general, the interviewees are satisfied with the proposal due to the ability to improve the GDPR implementation and reduce the level of effort. Plus, with these practices they can have a more solid view of what to do, to comply with GDPR.

As can be seen, there is not a single IS framework that has practices for all concepts. This is due to several factors such as:

- Only ISO 27552 has been developed to comply with GDPR;
- The NIST SP 800-53 is very technical and oriented to IS and DP;
- ISO 27001 was last updated in 2013, when DP was not yet a hot topic;
- COBIT is very focused on governance and management of IT, although it was updated in 2019 and added new controls to IS.

However, the IS frameworks of this research complement each other and in answer to the objective of this research, it is possible for an IS framework assist in the implementation of GDPR, achieving the compliance and thereby decrease the level of effort required.

In conclusion, the research question, “How can current IS frameworks help Banks comply with GDPR” was answered positively and proves that IS frameworks can help Banks comply with GDPR, although not only with a single IS framework. Additionally, for this industry there are some limitations that should be considered.

9.1. Research Limitations

Throughout this research some limitations were identified. As the bank industry touches on critical data and the information shared abroad is greatly reduced, only 6 banks were able to participate in the study.

Another limitation found is that the study based its demonstration and evaluation on the knowledge of the interviewees and was not possible to create group meetings to do a brainstorming, since this point would have been more beneficial for the validation of some concepts and practices.

9.2. Future Work

The future work involves a second round of interviews to validate the results obtained in the previous chapter, ideally using Delphi techniques. Finally, with the final list of practices and concepts should be implemented in a bank with a low level of maturity, thus evaluating the usefulness of using the IS frameworks.

References

2019, C. (2019). *Governance and Management*. *Governance and Management Objectives*. https://doi.org/10.1201/b13869-7

Agarwal, S. (2016). Towards dealing with GDPR uncertainty. Retrieved from http://www.ifip-summerschool.org/wp-content/uploads/2016/08/IFIP-SC-2016_pre_paper_13.pdf

Al-ahmad, W., & Mohammad, B. (2012). CAN A SINGLE SECURITY FRAMEWORK ADDRESS INFORMATION SECURITY RISKS ADEQUATELY ?, *2*(3), 222–230.

Ayala-rivera, V., & Pasquale, L. (2018). “ The Grace Period Has Ended ” : An Approach to Operationalize GDPR Requirements. *2018 IEEE 26th International Requirements Engineering Conference (RE)*, 136–146. https://doi.org/10.1109/RE.2018.00023

Council, O. F. T. H. E. (1995). DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995, (L).

Council, O. F. T. H. E. (2016). (Text with EEA relevance), *2014*(April).

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law and Security Review*, *34*(2), 234–243. https://doi.org/10.1016/j.clsr.2017.09.001

Freitas, C., & Mira, M. (2018). GDPR Compliance in SMEs : There is much to be done, *3*(4), 1–7.

Heimes, R. (2016). Global InfoSec and Breach Standards. *IEEE Security and Privacy*, *14*(5), 68–72. https://doi.org/10.1109/MSP.2016.90

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hove, S. E. (2005). Experiences from Conducting Semi-Structured Interviews in Empirical Software Engineering Research, (Metrics).

ISO/IEC DIS 27552. (2019). DRAFT INTERNATIONAL STANDARD ISO / IEC DIS

27552 Security techniques — Extension to ISO / IEC 27001 and ISO / IEC 27002 for privacy information management — Requirements and guidelines, *2018*.

ISO/IEC, I. O. for S. E. C. (2013). Iso/Iec 27001: 2013. *Information Technology Standard*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Krempel, E., & Beyerer, J. (2018). The EU General Data Protection Regulation and Its Effects on Designing Assistive Environments. *Proceedings of the 11th PErvasive Technologies Related to Assistive Environments Conference*, 327–330. https://doi.org/10.1145/3197768.3201567

Krystlik, J. (2018). With GDPR , preparation is everything. *Computer Fraud & Security Bulletin*, *2017*(6), 5–8. https://doi.org/10.1016/S1361-3723(17)30050-7

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance, (June), 1–6. https://doi.org/10.23919/cisti.2019.8760937

Malatras, A., Sanchez, I., Beslay, L., Coisel, I., Vakalis, I., D'Acquisto, G., … Zorkadis, V. (2017). Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law and Security Review*, *33*(4), 458–469. https://doi.org/10.1016/j.clsr.2017.03.013

NIST. (2015). NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. *Sp-800-53Ar4*, 462. https://doi.org/10.6028/NIST.SP.800-53Ar4

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). <Design Science Research Methodology 2008.pdf>. *Published in Journal of Management Information Systems*, *24*(3), 45–78. https://doi.org/10.2753/MIS0742-1222240302

Philip, R. K. (2018). General Data Protection Regulation (GDPR) and paediatric medical practice in Ireland: a personal reflection. *Irish Journal of Medical Science*, (1), 1–4. https://doi.org/10.1007/s11845-018-1857-3

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human Genetics*, *137*(8), 575–582. https://doi.org/10.1007/s00439-018-1919-7

Portugal, C. N. de C. (2019). REFERÊNCIA PARA A, 0–160.

Ri, P., Dwd, H., Rq, D., Plohwd, G., Frp, J., Ri, S., … Ri, Q. L. (2018). $q ,psdfw ri *hqhudo 'dwd 3urwhfwlrq 5hjxodwlrq rq d 6pduw &lw\ &rqfhsw, 390–394. https://doi.org/10.23919/MIPRO.2018.8400074

Rijsenbrij, D. (2019). PrimaVera Working Paper Series PrimaVera Working Paper 2000-19 Redefining business – IT alignment.

Seaman, C. B. (1999). Qualitative Methods in Empirical Studies of Software Engineering, *25*(4), 557–572.

Srinivas, J., Kumar, A., & Kumar, N. (2019). Government regulations in cyber security : Framework , standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Sydekum, R., & Networks, F. (2018). Can consumers bank on financial services being secure with GDPR ?, 11–13. https://doi.org/10.1016/S1361-3723(18)30054-X

Tankard, C., & Pathways, D. (2016). What the GDPR means for. *Network Security*, *2016*(6), 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

Teixeira, G. (2018). *The Critical Success Factors of GDPR Implementation : a Systematic Literature Review*.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Wilson, S. (2018). A framework for security technology cohesion in the era of the GDPR. *Computer Fraud & Security Bulletin*, *2018*(12), 8–11. https://doi.org/10.1016/S1361-3723(18)30119-2

Annex and Appendices

Annex A – List of extracted concepts and their meaning

Article	Paragraph/Line	Concept	Meaning
5	**1-A**	Lawfulness, fairness and transparency	Processed lawfully, fairly and in a transparent manner in relation to the data subject (Council, 2016)
5	**1-B**	Data Minimisation	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Council, 2016)
5	**1-D**	Inaccurate Data	The GDPR does not give a definition of the term accuracy. However, the Data Protection Act 2018 (DPA 2018) states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact (Council, 2016)
5	**1-E**	Storage Limitation	Kept in a form which permits identifications of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Council, 2016)
5	**1-F**	Security of Personal Data	Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality' (Council, 2016)
5	**2**	Accountability	The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability') (Council, 2016)
12		Transparent information, communication and modalities for the exercise of the rights of the data subject	The controller shall take appropriate measures related to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Council, 2016)

13		Information to be provided where personal data are collected from the data subject	Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available (Council, 2016)

14		Information to be provided where personal data have not been obtained from the data subject	Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) the categories of personal data concerned; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available (Council, 2016)

15		Right of access by the data subject	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Council, 2016)
16		Right to rectification	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement (Council, 2016)

17		Right to erasure (‘right to be forgotten’)	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay (Council, 2016)
18		Right to restriction of processing	The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject (Council, 2016)
19		Notification obligation regarding rectification or erasure of personal data or restriction of processing	The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it (Council, 2016)
20		Right to data portability	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (Council, 2016)

21		Right to object	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions (Council, 2016)
22		Automated individual decision-making, including profiling	The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (Council, 2016)
24	**2**	Data Protection Policies	Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection by the controller (Council, 2016)
24	**2**	Codes of Conduct	Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in article 42 may be used as na element by which to demonstrate compliance with the obligations of the controller (Council, 2016)
25	**1**	Data Protection by Design	Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processig and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects (Council, 2016)

25	**2**	Data Protection by Default	The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extend of their processing, the period of their storage and ther accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons (Council, 2016)
28	**1**	Processor	Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject (Council, 2016)

30	**1**	Records of Processing Activities	1.Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e)where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) (Council, 2016)

30	**2**	Records of Processing Activities	2.Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c)where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) (Council, 2016)
32	**1**	Security of processing	1.Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Council, 2016)
32	**1-A**	Pseudonymisation	(a) the pseudonymisation and encryption of personal data (Council, 2016)
32	**1-A**	Encryption of Personal Data	(a) the pseudonymisation and encryption of personal data (Council, 2016)
32	**1-B**	Confidentiality, Integrity, Availability and Resilience	(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (Council, 2016)
32	**1-C**	Restore the Availability	(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (Council, 2016)

32	**1-D**	Regularly Testing, Assessing and Evaluating	(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (Council, 2016)
32	**3**	Approved Certification	Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article (Council, 2016)
33	**1**	Notification of a personal data breach to the supervisory authority	1.In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay (Council, 2016)
34	**1**	Communication of a personal data breach to the data subject	1.When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay (Council, 2016)
35	**1**	Data Protection Impact Assessment	1.Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks (Council, 2016)

37	**1**	Designation of the data protection officer	1.The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10 (Council, 2016)

39		Tasks of the data protection officer	1.The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter. 2.The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing (Council, 2016)
42	**1**	Certification	1.The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account (Council, 2016)

44		General principle for transfers	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined (Council, 2016)

Annex B – List of GDPR Concepts Mapped to Practices

Article	Paragraph/Line	Concept	ISO 27552	ISO 27001:2013	COBIT 2019	NIST SP 800-53 v4
5	**1-A**	Lawfulness, fairness and transparency	7.2.2 - Identify lawful basis 8.2.2 - Organization’s purposes		EDM05.02 - Direct stakeholder engagement, communication and reporting	AP-2 - Purpose Specification
5	**1-B**	Data Minimisation	A.7.2.1 - Identify and document purpose A.7.4.1 - Limit collection B.8.2.2 - Organization's purposes		APO14.04 - Define a data quality strategy	DM-1 - Minimization of Personally Identifiable Information DM-3 - Minimization of PII Used in Testing, Training, and Research
5	**1-D**	Inaccurate Data	A.7.3.6 - Access, correction and/or erasure A.7.4.3 - Accuracy and quality		APO14.07 - Define the data cleansing approach	DI-1 - Data Quality IP-3 - REDRESS
5	**1-E**	Storage Limitation	A.7.4.3 - Accuracy and quality A.7.4.7 - Retention		APO14.09 - Support data archiving and retention	DM-2 - Data Retention and Disposal

5	**1-F**	Security of Personal Data	6.5.2.1 - Classification of information 6.5.3.1 - Management of removable media 6.5.3.3 - Physical media transfer 6.6.2.1 - User registration and de-registration 6.6.2.2 - User access provisioning 6.6.4.2 - Secure log-on procedures 6.8.2.7 - Secure disposal or re-use of equipment 6.8.2.9 - Clear desk and clear screen policy 6.9.3.1 - Information backup 6.9.4.1 - Event logging 6.9.4.2 - Protection of log information 6.10.2.1 - Information transfer policies and procedures 6.10.2.4 - Confidentiality or non-disclosure agreements 6.11.1.2 - Securing application services on public networks 6.11.3.1 - Protection of test data 6.12.1.2 - Addressing security within supplier agreements 6.13.1.1 - Responsibilities and	A.8.2.1 - Classification of information A.8.3.1 - Management of removable media A.8.3.3 - Physical media transfer A.9.2.1 - User registration and de-registration A.9.2.2 - User access provisioning A.9.4.2 - Secure log-on procedures A.11.2.7 - Secure disposal or re-use of equipment A.11.2.9 - Clear desk and clear screen policy A.12.3.1 - Information backup A.12.4.1 - Event logging A.12.4.2 - Protection of log information A.13.2.1 - Information transfer policies and procedures A.13.2.4 - Confidentiality or non-disclosure agreements A.14.1.2 - Securing application services on	APO13.01 - Establish and maintain an information security management system (ISMS) APO13.02 - Define and manage an information security and privacy risk treatment plan APO13.03 - Monitor and review the information security management system (ISMS) DSS05.01 - Protect against malicious software DSS05.02 - Manage network and connectivity security DSS05.03 - Manage endpoint security DSS05.04 - Manage user identity and logical access DSS05.05 - Manage physical access to I&T assets DSS05.06 - Manage sensitive documents and output devices	AC-1 - Access Control Policy and Procedures AC-5 - Separation of Duties AC-6 - Least Privilege AC-19 - Access Control for Mobile Devices AC-20 - Use of External Information Systems AU-2 - Audit Events CA-7 - Continuous Monitoring CA-8 - Penetration Testing MA-1 - System Maintenance Policy and Procedures MP-1 - Media Protection Policy and Procedures PE-1 - Physical and Environmental Protection Policy and Procedures SA-8 - Security Engineering Principles SA-11 - Developer Security Testing and Evaluation SA-17 - Developer Security Architecture and Design SC-12 - Cryptographic Key Establishment and Management

			procedures 6.15.1.1 - Identification of applicable legislation and contractual A.7.4.8 - Disposal B.8.4.3 - PII transmission controls	public networks A.14.3.1 - Protection of test data A.15.1.2 - Addressing security within supplier agreements A.16.1.1 - Responsibilities and procedures A.18.1.1 - Identification of applicable legislation and contractual		SI-3 - Malicious Code Protection

5	**2**	Accountability	6.15.1.3 - Protection of records A.7.2.6 - Contracts with PII processors A.7.2.8 - Records related to processing PII	A.5.1.1 - Policies for information security A.5.1.2 - Review of the policies for information security A.6.1.1 - Information security roles and responsibilities A.12.1.1 - Documented operating procedures A.18.1.1 - Identification of applicable legislation and contractual requirements A.18.1.3 - Protection of records A.18.2.2 - Compliance with security policies and standards	DSS06.03 - Manage roles, responsibilities, access privileges and levels of authority APO01.05 Establish roles and responsibilities	AU-1 - Audit and Accountability Policy and Procedures
12		Transparent information, communication and modalities for the exercise of the rights of the data subject	A.7.3.1 - Determining and fulfilling obligations to PII principals A.7.3.3 - Providing information to PII principals A.7.3.9 - Handling requests		EDM05.02 - Direct stakeholder engagement, communication and reporting	AP-1 - Authority to Collect AP-2 - Purpose Specification

13		Information to be provided where personal data are collected from the data subject	A.7.3.2 - Determining information for PII principals A.7.3.3 - Providing information to PII principals A.7.3.5 - Provide mechanism to object to processing A.7.3.6 - Access, correction and/or erasure A.7.3.8 - Providing copy of PII processed A.7.3.10 - Automated decision making A.7.4.7 - Retention		EDM05.02 - Direct stakeholder engagement, communication and reporting	AP-2 - Purpose Specification
14		Information to be provided where personal data have not been obtained from the data subject	A.7.3.2 - Determining information for PII principals A.7.3.4 - Provide mechanism to modify or withdraw consent A.7.3.5 - Provide mechanism to object to processing A.7.3.6 - Access, correction and/or erasure A.7.3.8 - Providing copy of PII processed A.7.3.10 - Automated decision making A.7.4.7 - Retention		EDM05.02 - Direct stakeholder engagement, communication and reporting	TR-2 - System of Records Notices and Privacy Act Statements

15		Right of access by the data subject	A.7.3.2 - Determining information for PII principals A.7.3.3 - Providing information to PII principals A.7.3.8 - Providing copy of PII processed A.7.3.9 - Handling requests A.7.3.10 - Automated decision making A.7.5.1 - Identify basis for international PII transfer A.7.5.2 - Countries and organizations to which PII might be transferred B.8.3.1 - Obligations to PII principals		EDM05.02 - Direct stakeholder engagement, communication and reporting	IP-2 - Individual Access
16		Right to rectification	A.7.3.6 - Access, correction and/or erasure		BAI08.04 - Evaluate and update or retire information	IP-3 - REDRESS
17		Right to erasure ('right to be forgotten')	A.7.2.2 - Identify lawful basis A.7.3.6 - Access, correction and/or erasure B.8.3.1 - Obligations to PII principals		BAI08.04 - Evaluate and update or retire information	
18		Right to restriction of processing	A.7.2.2 - Identify lawful basis A.7.3.2 - Determining information for PII principals A.7.3.4 - Provide mechanism to modify or withdraw consent		BAI08.04 - Evaluate and update or retire information	IP-1 - Consent

19		Notification obligation regarding rectification or erasure of personal data or restriction of processing	A.7.3.7 - PII controllers' obligations and third parties		EDM05.02 - Direct stakeholder engagement, communication and reporting	
20		Right to data portability	A.7.3.8 - Providing copy of PII processed		APO01.10 - Define and implement infrastructure, services and applications to support the governance and management system	
21		Right to object	A.7.3.2 - Determining information for PII principals A.7.3.3 - Providing information to PII principals A.7.3.5 - Provide mechanism to object to PII processing		APO01.10 - Define and implement infrastructure, services and applications to support the governance and management system	IP-2 - Individual Access
22		Automated individual decision-making, including profiling	A.7.2.2 - Identify lawful basis A.7.3.10 - Automated decision making		APO14.05 - Establish data profiling methodologies, processes and tools	AC-23 - Data Mining Protection

24	**2**	Data Protection Policies	6.2.1.1 - Policies for information security 6.15.1.3 - Protection of records	A.5.1.1 - Policies for information security A.18.1.3 - Protection of records	APO01.09 - Define and communicate policies and procedures APO13.02 - Define and manage an information security and privacy risk treatment plan	AR-1 - Governance and Privacy Program TR-1 - Privacy Notice
24	**2**	Codes of Conduct	6.2.1.1 - Policies for information security 6.15.1.3 - Protection of records	A.5.1.1 - Policies for information security A.18.1.3 - Protection of records	APO01.09 - Define and communicate policies and procedures	
25	**1**	Data Protection by Design	6.11.2.5 - Secure systems engineering principles	A.14.2.5 - Secure system engineering principles	APO03.01 - Develop the enterprise architecture vision APO03.04 - Define architecture implementation APO11.03 - Manage quality standards, practices and procedures and integrate quality management into key processes and solutions APO13.02 - Define and manage an information security and privacy risk treatment plan	AR-7 - Privacy-Enhanced System Design and Development SA-8 - Security Engineering Principles

25	**2**	Data Protection by Default	A.7.4.2 - Limit processing		APO14.09 - Support data archiving and retention.	DM-1 - Minimization of Personally Identifiable DM-2 - Data Retention and Disposal DM-3 - Minimization of PII Used in Testing, Training, and Research
28	**1**	Processor	6.12.1.2 - Addressing security within supplier agreements 6.15.1.1 - Identification of applicable legislation and contractual requirements	A.6.1.1 - Information security roles and responsibilities A.7.2.1 - Management responsibilities A.15.1.2 - Addressing security within supplier agreements A.18.1.1 - Identification of applicable legislation and contractual requirements	APO09.03 - Define and prepare service agreements APO10.03 - Manage vendor relationships and contracts	AR-3 - Privacy Requirements for Contractors and Service Providers PS-7 - Third-Party Personnel Security

30	**1**	Records of Processing Activities	A.7.2.8 - Records related to processing PII A.7.5.1 - Identify basis for PII transfer between jurisdictions A.7.5.2 - Countries and international organizations to which PII might be transferred A.7.5.3 - Records of transfer of PII A.7.5.4 - Records of PII disclosures to third parties B.8.4.2 - Return, transfer or disposal of PII B.8.5.3 - Records of PII disclosures to third parties		BAI09.01 - Identify and record current assets	SE-1 - Inventory of Personally Identifiable Information
30	**2**	Records of Processing Activities	6.12.1.2 - Addressing security within supplier agreements 6.15.1.1 - Identification of applicable legislation and contractual requirements B.8.2.6 - Records related to processing PII B.8.5.2 - Countries and international organizations to which PII might be transferred	A.15.1.2 - Addressing security within supplier agreements A.18.1.1 - Identification of applicable legislation and contractual requirements	BAI09.01 - Identify and record current assets	SE-1 - Inventory of Personally Identifiable Information

32	**1**	Security of processing	5.4.1.2 - Information security risk assessment 5.4.1.3 - Information security risk treatment 6.5.3.1 - Management of removable media 6.5.3.3 - Physical media transfer 6.7.1.1 - Policy on the use of cryptographic controls 6.9.3.1 - Information backup 6.11.1.2 - Securing application services on public networks 6.12.1.2 - Addressing security within supplier agreements 6.15.1.1 - Identification of applicable legislation and contractual requirements 6.15.2.1 - Independent review of information security 6.15.2.3 - Technical compliance review A.7.4.5 - PII de-identification and deletion at the end of processing	6.1.2 - Information security risk assessment 6.1.3 - Information security risk treatment A.8.3.1 - Management of removable media A.8.3.3 - Physical media transfer A.10.1.1 - Policy on the use of cryptographic controls A.12.3.1 - Information backup A.14.1.2 - Securing application services on public networks A.15.1.2 - Addressing security within supplier agreements A.18.1.1 - Identification of applicable legislation and contractual requirements A.18.2.1 - Independent review of information security A.18.2.3 - Technical compliance review A.7.4.5 - PII de-identification and	APO12.01 - Collect data APO12.02 - Analyze risk APO12.06 - Respond to risk APO13.01 - Establish and maintain an information security management system (ISMS) APO13.02 - Define and manage an information security and privacy risk treatment plan APO13.03 - Monitor and review the information security management system (ISMS)	CA-1 - Security Assessment and Authorization Policies and Procedures

				deletion at the end of processing		

32	**1-A**	Pseudonymisation	6.5.3.1 - Management of removable media 6.5.3.3 - Physical media transfer 6.7.1.1 - Policy on the use of cryptographic controls 6.11.1.2 - Securing application services on public networks A.7.4.5 - PII de-identification and deletion at the end of processing	A.8.3.1 - Management of removable media A.8.3.3 - Physical media transfer A.10.1.1 - Policy on the use of cryptographic controls A.14.1.2 - Securing application services on public networks A.14.1.3 - Protecting application services transactions A.18.1.5 - Regulation of cryptographic controls	DSS06.06 - Secure information assets	SC-12 - Cryptographic Key Establishment and Management SC-13 - Cryptographic Protection
32	**1-A**	Encryption of Personal Data	6.5.3.1 - Management of removable media 6.5.3.3 - Physical media transfer 6.7.1.1 - Policy on the use of cryptographic controls 6.11.1.2 - Securing application services on public networks A.7.4.5 - PII de-identification and deletion at the end of processing	A.8.3.1 - Management of removable media A.8.3.3 - Physical media transfer A.10.1.1 - Policy on the use of cryptographic controls A.14.1.2 - Securing application services on public networks A.14.1.3 - Protecting application services transactions A.18.1.5 - Regulation of cryptographic controls	DSS06.06 - Secure information assets	SC-12 - Cryptographic Key Establishment and Management SC-13 - Cryptographic Protection

32	**1-B**	Confidentiality, Integrity, Availability and Resilience	5.4.1.3 - Information security risk treatment 6.12.1.2 - Addressing security within supplier agreements 6.15.1.1 - Identification of applicable legislation and contractual requirements	6.1.3 - Information security risk treatment A.15.1.2 - Addressing security within supplier agreements A.18.1.2 - Identification of applicable legislation and contractual requirements	DSS06.02 - Control the processing of information DSS06.06 - Secure information assets	SC-6 - Transmission Confidentiality and Integrity
32	**1-C**	Restore the Availability	6.9.3.1 - Information backup	A.6.1.1 - Responsibilities and procedures A.12.3.1 - Information backup A.17.1.1 - Planning information security continuity A.17.2.1 - Availability of information processing facilities	DSS04.03 - Develop and implement a business continuity response DSS04.04 - Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)	CP-2 - Contingency Plan
32	**1-D**	Regularly Testing, Assessing and Evaluating	6.15.2.1 - Independent review of information security	A.18.2.1 - Independent review of information security	MEA02.01 - Monitor internal controls MEA02.02 - Review effectiveness of business process controls MEA02.03 - Perform control self-assessments MEA02.04 - Identify and report control deficiencies	CA-7 - Continuous Monitoring

32	**3**	Approved Certification	5.2.1 - Independent review of information security	A.18.2.1 - Independent review of information security		
33	**1**	Notification of a personal data breach to the supervisory authority	6.13.1.1 - Responsibilities and procedures 6.13.1.5 - Response to information security incidents	A.16.1.1 - Responsibilities and procedures A.16.1.5 - Response to information security incidents	DSS02.01 - Define classification schemes for incidents and service requests DSS03.01 - Identify and classify problems	SE-2 - Privacy Incident Response
34	**1**	Communication of a personal data breach to the data subject	6.13.1.1 - Responsibilities and procedures 6.13.1.5 - Response to information security incidents	A.16.1.1 - Responsibilities and procedures A.16.1.5 - Response to information security incidents	DSS02.01 - Define classification schemes for incidents and service requests DSS03.01 - Identify and classify problems	SE-2 - Privacy Incident Response
35	**1**	Data Protection Impact Assessment	5.2.2 - Understanding the needs and expectations of interested parties A.7.2.5 - Privacy impact assessment B.8.2.1 - Cooperation agreement	4.2 - Understanding the needs and expectations of interested parties 6.1.2 - Information security risk assessment	APO12.01 - Collect data APO12.02 - Analyze risk	AR-2 - Privacy Impact and Risk Assessment
37	**1**	Designation of the data protection officer	6.3.1.1 - Information security roles and responsibilities	A.6.1.1 - Information security roles and responsibilities	APO07.01 - Acquire and maintain adequate and appropriate staffing	AR-1 - Governance and Privacy Program

39		Tasks of the data protection officer	6.3.1.1 - Information security roles and responsibilities 6.4.2.2 - Information security awareness, education and training	A.6.1.1 - Information security roles and responsibilities A.7.2.2 - Information security awareness, education and training	APO01.05 - Establish roles and responsibilities	AR-1 - Governance and Privacy Program
42	**1**	Certification	5.2.1 - Independent review of information security	A.18.2.1 - Independent review of information security		
44		General principle for transfers	A.7.5.1 - Identify basis for PII transfer between jurisdictions B.8.5.1 - Basis for PII transfer between jurisdictions			UL-2 - Information Sharing with Third Parties

Annex C – Interview Questionnaire

Interview

Best Frameworks for Demonstrable GDPR Compliance in Bank Industry

This interview about Frameworks and General Data Protection Regulation (GDPR) is carried out within the scope of a master's thesis of ISCTE.

The results will be sent to the interviewee by email after all the interviews, with specialist in bank industry, was finished.

It is guaranteed that both company and interviewee name and identification will be treated confidentially and shall never be revealed.

Thank you in advance for your availability and most sincere response.

Interviewee	
Years of experience	
Current Job Role	
Years of experience in banking industry	
What are your responsabilities?	
Months of experience in GDPR	
How many GDPR projects have you been envolved	
Classify how much are you familiar with GDPR?	☐Excellent ☐Very Good ☐Good ☐Fair ☐Poor
Point out which of the following frameworks that you have experience	☐ISO 27001 ☐ISO 31000 ☐ISO 38500 ☐ISO 22301 ☐NIST SP 800-53 ☐COBIT ☐Other: _______________________________

Bank

Number of employees:	☐<100
	☐100-200
	☐200-300
	☐300-500
	☐>500
Multinational	☐Yes ☐No
Do the bank follow/perform any framework or best practices?	☐Yes ☐No
If yes, which framework(s)?	☐ISO 27001 ☐ISO 31000 ☐ISO 38500 ☐ISO 22301 ☐NIST SP 800-53 ☐COBIT ☐Other: _______________________________________

For the following concepts extracted from the GDPR, please point out for each practice one of the three options bellow:

- Not Applicable (N/A)
- Partially Compliant (PC)
- Fully Compliant (FC)

Additionally, and if you have implemented or starting the implementation of one, please mark on the correspondent column:

- In Implementation (II)
- Implemented (I)

Concepts and Practices	Level of Compliance				
Lawfulness, fairness and transparency	N/A	PC	FC	II	I
• Identify lawful basis					
• Organization’s purposes					
• Direct stakeholder engagement, communication and reporting					
• Purpose Specification					
Data Minimisation	N/A	PC	FC	II	I
• Identify and document purpose					
• Limit collection					
• Organization's purposes					
• Define a data quality strategy					
• Minimization of Personally Identifiable Information					

• Minimization of PII Used in Testing, Training, and Research					
Innacurate Data	N/A	PC	FC	II	I
• Access, correction and/or erasure					
• Accuracy and quality					
• Define the data cleansing approach					
• Data Quality					
• REDRESS					
Storage Limitation	N/A	PC	FC	II	I
• Accuracy and quality					
• Retention					
• Support data archiving and retention					
• Data Retention and Disposal					
Security of Personal Data	N/A	PC	FC	II	I
• Classification of information					
• Classification of information*					
• Management of removable media					
• Management of removable media*					
• Physical media transfer					
• Physical media transfer*					
• User registration and de-registration					
• User registration and de-registration*					
• User access provisioning					
• User access provisioning*					
• Secure log-on procedures					
• Secure log-on procedures*					
• Secure disposal or re-use of equipment					
• Secure disposal or re-use of equipment*					
• Clear desk and clear screen policy					
• Clear desk and clear screen policy*					
• Information backup					
• Information backup*					
• Event logging					
• Event logging*					
• Protection of log information					
• Protection of log information*					
• Information transfer policies and procedures					
• Information transfer policies and procedures*					
• Confidentiality or non-disclosure agreements					
• Confidentiality or non-disclosure agreements*					

• Securing application services on public networks					
• Securing application services on public networks*					
• Protection of test data					
• Protection of test data*					
• Addressing security within supplier agreements					
• Addressing security within supplier agreements*					
• Responsibilities and procedures					
• Responsibilities and procedures*					
• Identification of applicable legislation and contractual requirements					
• Identification of applicable legislation and contractual requirements*					
• Disposal					
• PII transmission controls					
• Establish and maintain an information security management system (ISMS)					
• Define and manage an information security and privacy risk treatment plan					
• Monitor and review the information security management system (ISMS)					
• Protect against malicious software					
• Manage network and connectivity security					
• Manage endpoint security					
• Manage user identity and logical access					
• Manage physical access to I&T assets					
• Manage sensitive documents and output devices					
• Access Control Policy and Procedures					
• Separation of Duties					
• Least Privilege					
• Access Control for Mobile Devices					
• Use of External Information Systems					
• Audit Events					
• Continuous Monitoring					
• Penetration Testing					
• System Maintenance Policy and Procedures					
• Media Protection Policy and Procedures					
• Physical and Environmental Protection Policy and Procedures					
• Security Engineering Principles					
• Developer Security Testing and Evaluation					

• Developer Security Architecture and Design					
• Cryptographic Key Establishment and Management					
• Malicious Code Protection					
Accountability	N/A	PC	FC	II	I
• Protection of records					
• Protection of records*					
• Contracts with PII processors					
• Records related to processing PII					
• Policies for information security					
• Review of the policies for information security					
• Information security roles and responsibilities					
• Documented operating procedures					
• Identification of applicable legislation and contractual requirements					
• Compliance with security policies and standards					
• Manage roles, responsibilities, access privileges and levels of authority					
• Establish roles and responsibilities					
• Audit and Accountability Policy and Procedures					
Transparent information, communication and modalities for the exercise of the rights of the data subject	N/A	PC	FC	II	I
• Determining and fulfilling obligations to PII principals					
• Providing information to PII principals					
• Handling requests					
• Direct stakeholder engagement, communication and reporting					
• Authority to Collect					
• Purpose Specification					
Information to be provided where personal data are collected from the data subject	N/A	PC	FC	II	I
• Determining information for PII principals					
• Providing information to PII principals					
• Provide mechanism to object to processing					
• Access, correction and/or erasure					
• Providing copy of PII processed					
• Automated decision making					
• Retention					

• Direct stakeholder engagement, communication and reporting					
• Purpose Specification					
Information to be provided where personal data have not been obtained from the data subject	N/A	PC	FC	II	I
• Determining information for PII principals					
• Provide mechanism to modify or withdraw consent					
• Provide mechanism to object to processing					
• Access, correction and/or erasure					
• Providing copy of PII processed					
• Automated decision making					
• Retention					
• Direct stakeholder engagement, communication and reporting					
• System of Records Notices and Privacy Act Statements					
Right of access by the data subject	N/A	PC	FC	II	I
• Determining information for PII principals					
• Providing information to PII principals					
• Providing copy of PII processed					
• Handling requests					
• Automated decision making					
• Identify basis for international PII transfer					
• Countries and organizations to which PII might be transferred					
• Obligations to PII principals					
• Direct stakeholder engagement, communication and reporting					
• Individual Access					
Right to rectification	N/A	PC	FC	II	I
• Access, correction and/or erasure					
• Evaluate and update or retire information					
• REDRESS					
Right to erasure (‘right to be forgotten’)	N/A	PC	FC	II	I
• Identify lawful basis					
• Access, correction and/or erasure					
• Obligations to PII principals					
• Evaluate and update or retire information					
Right to restriction of processing	N/A	PC	FC	II	I

• Identify lawful basis					
• Determining information for PII principals					
• Provide mechanism to modify or withdraw consent					
• Evaluate and update or retire information					
• Consent					
Notification obligation regarding rectification or erasure of personal data or restriction of processing	N/A	PC	FC	II	I
• PII controllers' obligations and third parties					
• Direct stakeholder engagement, communication and reporting					
Right to data portability	N/A	PC	FC	II	I
• Providing copy of PII processed					
• Define and implement infrastructure, services and applications to support the governance and management system					
Right to object	N/A	PC	FC	II	I
• Determining information for PII principals					
• Providing information to PII principals					
• Provide mechanism to object to PII processing					
• Define and implement infrastructure, services and applications to support the governance and management system					
• Individual Access					
Automated individual decision-making, including profiling	N/A	PC	FC	II	I
• Identify lawful basis					
• Automated decision making					
• Establish data profiling methodologies, processes and tools					
• Data Mining Protection					
Data Protection Policies	N/A	PC	FC	II	I
• Policies for information security					
• Policies for information security*					
• Protection of records					
• Protection of records*					
• Define and communicate policies and procedures					
• Define and manage an information security and privacy risk treatment plan					
• Governance and Privacy Program					

• Privacy Notice					
Codes of Conduct	N/A	PC	FC	II	I
• Policies for information security					
• Policies for information security*					
• Protection of records					
• Protection of records*					
• Define and communicate policies and procedures					
Data Protection by Design	N/A	PC	FC	II	I
• Secure system engineering principles					
• Secure systems engineering principles*					
• Develop the enterprise architecture vision					
• Define architecture implementation					
• Manage quality standards, practices and procedures and integrate quality management into key processes and solutions					
• Define and manage an information security and privacy risk treatment plan					
• Privacy-Enhanced System Design and Development					
• Security Engineering Principles					
Data Protection by Default	N/A	PC	FC	II	I
• Limit processing					
• Support data archiving and retention					
• Minimization of Personally Identifiable Information					
• Data Retention and Disposal					
• Minimization of PII Used in Testing, Training, and Research					
Processor	N/A	PC	FC	II	I
• Addressing security within supplier agreements					
• Addressing security within supplier agreements *					
• Identification of applicable legislation and contractual requirements					
• Identification of applicable legislation and contractual requirements*					
• Information security roles and responsibilities					
• Management responsibilities					
• Define and prepare service agreements					

• Manage vendor relationships and contracts					
• Privacy Requirements for Contractors and Service Providers					
• Third-Party Personnel Security					
Records of Processing Activities	N/A	PC	FC	II	I
• Addressing security within supplier agreements					
• Addressing security within supplier agreements*					
• Identification of applicable legislation and contractual requirements					
• Identification of applicable legislation and contractual requirements*					
• Records related to processing PII					
• Identify basis for PII transfer between jurisdictions					
• Countries and international organizations to which PII might be transferred					
• Records of transfer of PII					
• Records of PII disclosures to third parties					
• Return, transfer or disposal of PII					
• Records of PII disclosures to third parties					
• Identify and record current assets					
• Inventory of Personally Identifiable Information					
Security of processing	N/A	PC	FC	II	I
• Information security risk assessment					
• Information security risk assessment*					
• Information security risk treatment					
• Information security risk treatment*					
• Management of removable media					
• Management of removable media*					
• Physical media transfer					
• Physical media transfer*					
• Policy on the use of cryptographic controls					
• Policy on the use of cryptographic controls*					
• Information backup					
• Information backup*					
• Securing application services on public networks					
• Securing application services on public networks*					

• Addressing security within supplier agreements					
• Addressing security within supplier agreements*					
• Identification of applicable legislation and contractual requirements					
• Identification of applicable legislation and contractual requirements*					
• Independent review of information security					
• Independent review of information security*					
• Technical compliance review					
• Technical compliance review*					
• PII de-identification and deletion at the end of processing					
• Collect data					
• Analyze risk					
• Respond to risk					
• Establish and maintain an information security management system (ISMS)					
• Define and manage an information security and privacy risk treatment plan					
• Monitor and review the information security management system (ISMS)					
• Security Assessment and Authorization Policies and Procedures					
Pseudonymisation	N/A	PC	FC	II	I
• Management of removable media					
• Management of removable media*					
• Physical media transfer					
• Physical media transfer*					
• Policy on the use of cryptographic controls					
• Policy on the use of cryptographic controls*					
• Securing application services on public networks					
• Securing application services on public networks*					
• PII de-identification and deletion at the end of processing					
• Protecting application services transactions					
• Regulation of cryptographic controls					
• Secure information assets					
• Cryptographic Key Establishment and Management					
• Cryptographic Protection					

Encryption of Personal Data	N/A	PC	FC	II	I
• Management of removable media					
• Management of removable media*					
• Physical media transfer					
• Physical media transfer*					
• Policy on the use of cryptographic controls					
• Policy on the use of cryptographic controls*					
• Securing application services on public networks					
• Securing application services on public networks*					
• PII de-identification and deletion at the end of processing					
• Protecting application services transactions					
• Regulation of cryptographic controls					
• Secure information assets					
• Cryptographic Key Establishment and Management					
• Cryptographic Protection					
Confidentiality, Integrity, Availability and Resilience	N/A	PC	FC	II	I
• Information security risk treatment					
• Information security risk treatment*					
• Addressing security within supplier agreements					
• Addressing security within supplier agreements*					
• Identification of applicable legislation and contractual requirements					
• Identification of applicable legislation and contractual requirements*					
• Control the processing of information					
• Secure information assets					
• Transmission Confidentiality and Integrity					
Restore the Availability	N/A	PC	FC	II	I
• Information backup					
• Information backup*					
• Responsibilities and procedures					
• Planning information security continuity					
• Availability of information processing facilities					
• Develop and implement a business continuity response					

• Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)					
• Contingency Plan					
Regularly Testing, Assessing and Evaluating	N/A	PC	FC	II	I
• Independent review of information security					
• Independent review of information security*					
• Monitor internal controls					
• Review effectiveness of business process controls					
• Perform control self-assessments					
• Identify and report control deficiencies					
• Continuous Monitoring					
Approved Certification	N/A	PC	FC	II	I
• Independent review of information security					
• Independent review of information security*					
Notification of a personal data breach to the supervisory authority	N/A	PC	FC	II	I
• Responsibilities and procedures					
• Responsibilities and procedures*					
• Response to information security incidents					
• Response to information security incidents*					
• Define classification schemes for incidents and service requests					
• Identify and classify problems					
• Privacy Incident Response					
Communication of a personal data breach to the data subject	N/A	PC	FC	II	I
• Responsibilities and procedures					
• Responsibilities and procedures*					
• Response to information security incidents					
• Response to information security incidents*					
• Define classification schemes for incidents and service requests					
• Identify and classify problems					
• Privacy Incident Response					
Data Protection Impact Assessment	N/A	PC	FC	II	I
• Understanding the needs and expectations of interested parties					
• Understanding the needs and expectations of interested parties*					

• Privacy impact assessment					
• Cooperation agreement					
• Information security risk assessment					
• Collect data					
• Analyze risk					
• Privacy Impact and Risk Assessment					
Designation of the data protection officer	N/A	PC	FC	II	I
• Information security roles and responsibilities					
• Information security roles and responsibilities*					
• Acquire and maintain adequate and appropriate staffing					
• Governance and Privacy Program					
Tasks of the data protection officer	N/A	PC	FC	II	I
• Information security roles and responsibilities					
• Information security roles and responsibilities*					
• Information security awareness, education and training					
• Information security awareness, education and training*					
• Establish roles and responsibilities					
• Governance and Privacy Program					
Certification	N/A	PC	FC	II	I
• Independent review of information security					
• Independent review of information security*					
General principle for transfers	N/A	PC	FC	II	I
• Identify basis for PII transfer between jurisdictions					
• Basis for PII transfer between jurisdictions					
• Information Sharing with Third Parties					

Last notes	
In your experience, with this practices do you think that a company can be compliant with GDPR?	☐Yes ☐No
If not, what do you think is missing?	

With this practices, do you think that the effort of implementing GDPR can be less, comparatively to implement the GDPR without this guidelines?	☐Yes ☐No
Do you think this interview is useful?	☐Yes ☐No

Annex D – Interviews Overview

Framework	Concepts and Practices	Level of Compliance					Score
	Lawfulness, fairness and transparency	N/A	PC	FC	II	I	
ISO 27552	Identify lawful basis		2	5	1	5	12
ISO 27552	Organization’s purposes		4	3		6	10
COBIT 2019	Direct stakeholder engagement, communication and reporting		4	3	6		10
NIST SP 800-53 Rev.4	Purpose Specification		3	4	1	5	11
	Data Minimisation	N/A	PC	FC	II	I	
ISO 27552	Identify and document purpose		3	4	3	3	11
ISO 27552	Limit collection		3	4	5	1	11
ISO 27552	Organization's purposes		5	2	2	3	9
COBIT 2019	Define a data quality strategy		4	3	4	1	10
NIST SP 800-53 Rev.4	Minimization of Personally Identifiable Information		3	4	5		11
NIST SP 800-53 Rev.4	Minimization of PII Used in Testing, Training, and Research		6	1	4		8
	Innacurate Data	N/A	PC	FC	II	I	
ISO 27552	Access, correction and/or erasure		4	3	5	1	10
ISO 27552	Accuracy and quality		4	3	5		10
COBIT 2019	Define the data cleansing approach		4	3	5		10
NIST SP 800-53 Rev.4	Data Quality		5	2	5		9

NIST SP 800-53 Rev.4	REDRESS		4	3	4	2	10
	Storage Limitation	N/A	PC	FC	II	I	
ISO 27552	Accuracy and quality		4	3	5		10
ISO 27552	Retention		4	3	4	2	10
COBIT 2019	Support data archiving and retention		2	5	5	1	12
NIST SP 800-53 Rev.4	Data Retention and Disposal		2	5	5	1	12
	Security of Personal Data	N/A	PC	FC	II	I	
ISO 27001:2013	Classification of information		4	3	5	1	10
ISO 27552	Classification of information*		3	4	6		11
ISO 27001:2013	Management of removable media		5	2	3	2	9
ISO 27552	Management of removable media*		5	2	3	2	9
ISO 27001:2013	Physical media transfer		5	2	2	2	9
ISO 27552	Physical media transfer*		5	2	2	2	9
ISO 27001:2013	User registration and de-registration		4	3		6	10
ISO 27552	User registration and de-registration*		3	4		6	11
ISO 27001:2013	User access provisioning		5	2	1	5	9
ISO 27552	User access provisioning*		5	2	2	4	9
ISO 27001:2013	Secure log-on procedures		5	2	2	4	9
ISO 27552	Secure log-on procedures*		4	3	3	3	10
ISO 27001:2013	Secure disposal or re-use of equipment		5	2	1	4	9
ISO 27552	Secure disposal or re-use of equipment*		4	3	1	4	10
ISO 27001:2013	Clear desk and clear screen policy		5	2	3	1	9
ISO 27552	Clear desk and clear screen policy*		5	2	3	1	9

ISO 27001:2013	Information backup		4	3		5	10
ISO 27552	Information backup*		3	4	1	4	11
ISO 27001:2013	Event logging		6	1	5		8
ISO 27552	Event logging*		5	2	5		9
ISO 27001:2013	Protection of log information		5	2	2	2	9
ISO 27552	Protection of log information*		4	3	2	2	10
ISO 27001:2013	Information transfer policies and procedures		6	1	4	1	8
ISO 27552	Information transfer policies and procedures*		5	2	4	1	9
ISO 27001:2013	Confidentiality or non-disclosure agreements		4	3	3	3	10
ISO 27552	Confidentiality or non-disclosure agreements*		3	4	3	3	11
ISO 27001:2013	Securing application services on public networks		4	3	1	3	10
ISO 27552	Securing application services on public networks*		3	4	1	3	11
ISO 27001:2013	Protection of test data		5	2	3	3	9
ISO 27552	Protection of test data*		4	3	3	3	10
ISO 27001:2013	Addressing security within supplier agreements		4	3	5	1	10
ISO 27552	Addressing security within supplier agreements*		3	4	5	1	11
ISO 27001:2013	Responsibilities and procedures		5	2	3	3	9
ISO 27552	Responsibilities and procedures*		4	3	2	3	10
ISO 27001:2013	Identification of applicable legislation and contractual requirements		5	2	3	3	9
ISO 27552	Identification of applicable legislation and contractual requirements*		4	3	2	4	10
ISO 27552	Disposal		6	1	4	2	8
ISO 27552	PII transmission controls		5	2	3	2	9
COBIT 2019	Establish and maintain an information security management system (ISMS)		5	2	4	1	9

COBIT 2019	Define and manage an information security and privacy risk treatment plan		5	2	4	2	9
COBIT 2019	Monitor and review the information security management system (ISMS)		5	2	4		9
COBIT 2019	Protect against malicious software		5	2	1	4	9
COBIT 2019	Manage network and connectivity security		4	3	1	3	10
COBIT 2019	Manage endpoint security		5	2	1	4	9
COBIT 2019	Manage user identity and logical access		4	3	3	2	10
COBIT 2019	Manage physical access to I&T assets		5	2	3	2	9
COBIT 2019	Manage sensitive documents and output devices		3	4	3	2	11
NIST SP 800-53 Rev.4	Access Control Policy and Procedures		4	3	3	3	10
NIST SP 800-53 Rev.4	Separation of Duties		3	4	4	2	11
NIST SP 800-53 Rev.4	Least Privilege		4	3	3	2	10
NIST SP 800-53 Rev.4	Access Control for Mobile Devices		5	2		5	9
NIST SP 800-53 Rev.4	Use of External Information Systems	1	3	3	2	3	9
NIST SP 800-53 Rev.4	Audit Events		5	2	5		9
NIST SP 800-53 Rev.4	Continuous Monitoring		5	2	4		9
NIST SP 800-53 Rev.4	Penetration Testing		5	2	2	4	9
NIST SP 800-53 Rev.4	System Maintenance Policy and Procedures	1	3	3	1	3	9

NIST SP 800-53 Rev.4	Media Protection Policy and Procedures		4	3	2	3	10
NIST SP 800-53 Rev.4	Physical and Environmental Protection Policy and Procedures		4	3	2	4	10
NIST SP 800-53 Rev.4	Security Engineering Principles		5	2	4	1	9
NIST SP 800-53 Rev.4	Developer Security Testing and Evaluation		5	2	4	1	9
NIST SP 800-53 Rev.4	Developer Security Architecture and Design		6	1	4		8
NIST SP 800-53 Rev.4	Cryptographic Key Establishment and Management		6	1	3	2	8
NIST SP 800-53 Rev.4	Malicious Code Protection		5	2	1	3	9
	Accountability	N/A	PC	FC	II	I	
ISO 27001:2013	Protection of records		4	3		5	10
ISO 27552	Protection of records*		4	3	1	4	10
ISO 27552	Contracts with PII processors		5	2	4		9
ISO 27552	Records related to processing PII		4	3	4	1	10
ISO 27001:2013	Policies for information security		2	5	1	5	12
ISO 27001:2013	Review of the policies for information security		4	3	1	5	10
ISO 27001:2013	Information security roles and responsibilities		2	5	1	5	12
ISO 27001:2013	Documented operating procedures		4	3	3	2	10
ISO 27001:2013	Identification of applicable legislation and contractual requirements		4	3	2	4	10
ISO 27001:2013	Compliance with security policies and standards		4	3	2	4	10
COBIT 2019	Manage roles, responsibilities, access privileges and levels of authority		6	1	3	2	8

COBIT 2019	Establish roles and responsibilities		5	2	4	1	9
NIST SP 800-53 Rev.4	Audit and Accountability Policy and Procedures		5	2	1	3	9
	Transparent information, communication and modalities for the exercise of the rights of the data subject	N/A	PC	FC	II	I	
ISO 27552	Determining and fulfilling obligations to PII principals		4	3	3	3	10
ISO 27552	Providing information to PII principals		4	3	3	3	10
ISO 27552	Handling requests		3	4	2	4	11
COBIT 2019	Direct stakeholder engagement, communication and reporting		4	3	4	2	10
NIST SP 800-53 Rev.4	Authority to Collect		4	3	2	4	10
NIST SP 800-53 Rev.4	Purpose Specification		4	3		5	10
	Information to be provided where personal data are collected from the data subject	N/A	PC	FC	II	I	
ISO 27552	Determining information for PII principals		4	3	1	5	10
ISO 27552	Providing information to PII principals		4	3	1	5	10
ISO 27552	Provide mechanism to object to processing		5	2	2	4	9
ISO 27552	Access, correction and/or erasure		5	2	4	2	9
ISO 27552	Providing copy of PII processed		4	3	3	2	10
ISO 27552	Automated decision making	1	5	1	3	1	7
ISO 27552	Retention		5	2	4	2	9
COBIT 2019	Direct stakeholder engagement, communication and reporting	1	4	2	3	2	8
NIST SP 800-53 Rev.4	Purpose Specification		4	3	2	4	10

	Information to be provided where personal data have not been obtained from the data subject	N/A	PC	FC	II	I	
ISO 27552	Determining information for PII principals	1	4	2	1	4	8
ISO 27552	Provide mechanism to modify or withdraw consent	3	1	3	1	3	7
ISO 27552	Provide mechanism to object to processing	3	2	2	1	3	6
ISO 27552	Access, correction and/or erasure	1	4	2	4	2	8
ISO 27552	Providing copy of PII processed	3	2	2	3	1	6
ISO 27552	Automated decision making	2	4	1	2	2	6
ISO 27552	Retention	1	3	3	1	5	9
COBIT 2019	Direct stakeholder engagement, communication and reporting	1	4	2	2	2	8
NIST SP 800-53 Rev.4	System of Records Notices and Privacy Act Statements	2	3	2		5	7
	Right of access by the data subject	N/A	PC	FC	II	I	
ISO 27552	Determining information for PII principals	1	3	3	1	4	9
ISO 27552	Providing information to PII principals		3	4	1	5	11
ISO 27552	Providing copy of PII processed		3	4	3	3	11
ISO 27552	Handling requests	1	3	3	1	4	9
ISO 27552	Automated decision making	1	5	1	2	1	7
ISO 27552	Identify basis for international PII transfer	1	5	1	3	1	7
ISO 27552	Countries and organizations to which PII might be transferred	1	4	2	2	2	8
ISO 27552	Obligations to PII principals	1	3	3	1	3	9
COBIT 2019	Direct stakeholder engagement, communication and reporting	1	5	1	4	1	7
NIST SP 800-53 Rev.4	Individual Access		2	5	1	4	12
	Right to rectification	N/A	PC	FC	II	I	

ISO 27552	Access, correction and/or erasure		2	5	3	3	12
COBIT 2019	Evaluate and update or retire information		2	5	4	2	12
NIST SP 800-53 Rev.4	REDRESS		4	3	3	3	10
	Right to erasure (‘right to be forgotten’)	N/A	PC	FC	II	I	
ISO 27552	Identify lawful basis	1	3	3	1	3	9
ISO 27552	Access, correction and/or erasure	1	4	2	4		8
ISO 27552	Obligations to PII principals		5	2	3	2	9
COBIT 2019	Evaluate and update or retire information	1	3	3	4		9
	Right to restriction of processing	N/A	PC	FC	II	I	
ISO 27552	Identify lawful basis		4	3	2	4	10
ISO 27552	Determining information for PII principals		4	3	3	3	10
ISO 27552	Provide mechanism to modify or withdraw consent		3	4	3	3	11
COBIT 2019	Evaluate and update or retire information		4	3	4	2	10
NIST SP 800-53 Rev.4	Consent		3	4	1	5	11
	Notification obligation regarding rectification or erasure of personal data or restriction of processing	N/A	PC	FC	II	I	
ISO 27552	PII controllers' obligations and third parties		2	5	3	3	12
COBIT 2019	Direct stakeholder engagement, communication and reporting		5	2	4	2	9
	Right to data portability	N/A	PC	FC	II	I	
ISO 27552	Providing copy of PII processed		2	5	4	2	12

COBIT 2019	Define and implement infrastructure, services and applications to support the governance and management system		6	1	6		8
	Right to object	N/A	PC	FC	II	I	
ISO 27552	Determining information for PII principals	1	4	2	2	3	8
ISO 27552	Providing information to PII principals	1	5	1	3	2	7
ISO 27552	Provide mechanism to object to PII processing		2	5	1	4	12
COBIT 2019	Define and implement infrastructure, services and applications to support the governance and management system		5	2	4	2	9
NIST SP 800-53 Rev.4	Individual Access	1	2	4	1	4	10
	Automated individual decision-making, including profiling	N/A	PC	FC	II	I	
ISO 27552	Identify lawful basis		4	3	1	2	10
ISO 27552	Automated decision making	1	3	3	3		9
COBIT 2019	Establish data profiling methodologies, processes and tools	1	5	1	4		7
NIST SP 800-53 Rev.4	Data Mining Protection	2	5		1		5
	Data Protection Policies	N/A	PC	FC	II	I	
ISO 27001:2013	Policies for information security		4	3	1	5	10
ISO 27552	Policies for information security*		3	4	1	5	11
ISO 27001:2013	Protection of records		4	3	2	4	10
ISO 27552	Protection of records*		3	4	2	3	11
COBIT 2019	Define and communicate policies and procedures		5	2	3	3	9
COBIT 2019	Define and manage an information security and privacy risk treatment plan		4	3	3	3	10

NIST SP 800-53 Rev.4	Governance and Privacy Program		5	2	2	4	9
NIST SP 800-53 Rev.4	Privacy Notice		4	3	1	5	10
	Codes of Conduct	N/A	PC	FC	II	I	
ISO 27001:2013	Policies for information security		4	3	1	4	10
ISO 27552	Policies for information security*		3	4	1	4	11
ISO 27001:2013	Protection of records		4	3	2	3	10
ISO 27552	Protection of records*		3	4	2	3	11
COBIT 2019	Define and communicate policies and procedures		5	2	2	3	9
	Data Protection by Design	N/A	PC	FC	II	I	
ISO 27001:2013	Secure system engineering principles		6	1	4	1	8
ISO 27552	Secure systems engineering principles*		5	2	4	1	9
COBIT 2019	Develop the enterprise architecture vision		6	1	3	1	8
COBIT 2019	Define architecture implementation		5	2	6		9
COBIT 2019	Manage quality standards, practices and procedures and integrate quality management into key processes and solutions		4	3	5		10
COBIT 2019	Define and manage an information security and privacy risk treatment plan		3	4	4	1	11
NIST SP 800-53 Rev.4	Privacy-Enhanced System Design and Development		4	3	4		10
NIST SP 800-53 Rev.4	Security Engineering Principles		6	1	5	1	8
	Data Protection by Default	N/A	PC	FC	II	I	
ISO 27552	Limit processing		5	2	3	2	9

COBIT 2019	Support data archiving and retention		5	2	2	3	9
NIST SP 800-53 Rev.4	Minimization of Personally Identifiable Information		5	2	5		9
NIST SP 800-53 Rev.4	Data Retention and Disposal		5	2	5		9
NIST SP 800-53 Rev.4	Minimization of PII Used in Testing, Training, and Research		5	2	3	2	9
	Processor	N/A	PC	FC	II	I	
ISO 27001:2013	Addressing security within supplier agreements		6	1	5	1	8
ISO 27552	Addressing security within supplier agreements *		5	2	5	1	9
ISO 27001:2013	Identification of applicable legislation and contractual requirements		4	3	2	3	10
ISO 27552	Identification of applicable legislation and contractual requirements*		4	3	3	3	10
ISO 27001:2013	Information security roles and responsibilities		4	3	3	2	10
ISO 27001:2013	Management responsibilities		5	2	3	2	9
COBIT 2019	Define and prepare service agreements		5	2	4	2	9
COBIT 2019	Manage vendor relationships and contracts		4	3	4	2	10
NIST SP 800-53 Rev.4	Privacy Requirements for Contractors and Service Providers		3	4	3	3	11
NIST SP 800-53 Rev.4	Third-Party Personnel Security		4	3	4	1	10
	Records of Processing Activities	N/A	PC	FC	II	I	
ISO 27001:2013	Addressing security within supplier agreements	1	4	2	5		8
ISO 27552	Addressing security within supplier agreements*	1	4	2	5		8

ISO 27001:2013	Identification of applicable legislation and contractual requirements		4	3	3	3	10
ISO 27552	Identification of applicable legislation and contractual requirements*		4	3	3	3	10
ISO 27552	Records related to processing PII		3	4	5		11
ISO 27552	Identify basis for PII transfer between jurisdictions		4	3	2	3	10
ISO 27552	Countries and international organizations to which PII might be transferred		4	3	3	2	10
ISO 27552	Records of transfer of PII		4	3	3	2	10
ISO 27552	Records of PII disclosures to third parties		4	3	3	1	10
ISO 27552	Return, transfer or disposal of PII	1	4	2	3	1	8
ISO 27552	Records of PII disclosures to third parties		4	3	3	1	10
COBIT 2019	Identify and record current assets		4	3	3	2	10
NIST SP 800-53 Rev.4	Inventory of Personally Identifiable Information		3	4	3	2	11
	Security of processing	N/A	PC	FC	II	I	
ISO 27001:2013	Information security risk assessment		4	3	3	3	10
ISO 27552	Information security risk assessment*		3	4	3	3	11
ISO 27001:2013	Information security risk treatment		4	3	3	3	10
ISO 27552	Information security risk treatment*		3	4	3	3	11
ISO 27001:2013	Management of removable media		6	1	3	2	8
ISO 27552	Management of removable media*		5	2	2	2	9
ISO 27001:2013	Physical media transfer		6	1	1	3	8
ISO 27552	Physical media transfer*		5	2		3	9
ISO 27001:2013	Policy on the use of cryptographic controls		5	2	2	3	9
ISO 27552	Policy on the use of cryptographic controls*		5	2	2	3	9

ISO 27001:2013	Information backup		4	3		5	10
ISO 27552	Information backup*		3	4	1	4	11
ISO 27001:2013	Securing application services on public networks		4	3		4	10
ISO 27552	Securing application services on public networks*		3	4		4	11
ISO 27001:2013	Addressing security within supplier agreements		6	1	4	2	8
ISO 27552	Addressing security within supplier agreements*		5	2	4	2	9
ISO 27001:2013	Identification of applicable legislation and contractual requirements		4	3	1	5	10
ISO 27552	Identification of applicable legislation and contractual requirements*		4	3	1	5	10
ISO 27001:2013	Independent review of information security		3	4	2	3	11
ISO 27552	Independent review of information security*		3	4	2	3	11
ISO 27001:2013	Technical compliance review		5	2	2	2	9
ISO 27552	Technical compliance review*		5	2	2	2	9
ISO 27552	PII de-identification and deletion at the end of processing		5	2	4		9
COBIT 2019	Collect data		3	4	1	4	11
COBIT 2019	Analyze risk		4	3	4	1	10
COBIT 2019	Respond to risk		5	2	4	1	9
COBIT 2019	Establish and maintain an information security management system (ISMS)		5	2	3	2	9
COBIT 2019	Define and manage an information security and privacy risk treatment plan		4	3	4	1	10
COBIT 2019	Monitor and review the information security management system (ISMS)		5	2	3	1	9
NIST SP 800-53 Rev.4	Security Assessment and Authorization Policies and Procedures		3	4	2	3	11

	Pseudonymisation	N/A	PC	FC	II	I	
ISO 27001:2013	Management of removable media		6	1	6		8
ISO 27552	Management of removable media*		5	2	6		9
ISO 27001:2013	Physical media transfer		6	1	4	1	8
ISO 27552	Physical media transfer*		5	2	4	1	9
ISO 27001:2013	Policy on the use of cryptographic controls		5	2	2	2	9
ISO 27552	Policy on the use of cryptographic controls*		5	2	2	2	9
ISO 27001:2013	Securing application services on public networks		4	3	1	3	10
ISO 27552	Securing application services on public networks*		3	4	1	3	11
ISO 27552	PII de-identification and deletion at the end of processing	1	4	2	5		8
ISO 27552	Protecting application services transactions	1	2	4	3	2	10
ISO 27552	Regulation of cryptographic controls		4	3	2	3	10
COBIT 2019	Secure information assets		4	3	4	2	10
NIST SP 800-53 Rev.4	Cryptographic Key Establishment and Management		6	1	3	1	8
NIST SP 800-53 Rev.4	Cryptographic Protection		5	2	3	2	9
	Encryption of Personal Data	N/A	PC	FC	II	I	
ISO 27001:2013	Management of removable media		6	1	4	1	8
ISO 27552	Management of removable media*		5	2	4	1	9
ISO 27001:2013	Physical media transfer		5	2	3	2	9
ISO 27552	Physical media transfer*		4	3	3	2	10
ISO 27001:2013	Policy on the use of cryptographic controls		5	2	2	2	9
ISO 27552	Policy on the use of cryptographic controls*		5	2	2	2	9
ISO 27001:2013	Securing application services on public networks		5	2	1	3	9
ISO 27552	Securing application services on public networks*		4	3	1	3	10

ISO 27552	PII de-identification and deletion at the end of processing		5	2	5		9
ISO 27001:2013	Protecting application services transactions		3	4	3	2	11
ISO 27001:2013	Regulation of cryptographic controls		5	2	2	2	9
COBIT 2019	Secure information assets		4	3	4	1	10
NIST SP 800-53 Rev.4	Cryptographic Key Establishment and Management		4	3	2	2	10
NIST SP 800-53 Rev.4	Cryptographic Protection		4	3	2	2	10
	Confidentiality, Integrity, Availability and Resilience	N/A	PC	FC	II	I	
ISO 27001:2013	Information security risk treatment		4	3	3	3	10
ISO 27552	Information security risk treatment*		3	4	3	3	11
ISO 27001:2013	Addressing security within supplier agreements		5	2	5	1	9
ISO 27552	Addressing security within supplier agreements*		4	3	5	1	10
ISO 27001:2013	Identification of applicable legislation and contractual requirements		4	3	2	4	10
ISO 27552	Identification of applicable legislation and contractual requirements*		4	3	2	4	10
COBIT 2019	Control the processing of information		4	3	3	2	10
COBIT 2019	Secure information assets		4	3	4	1	10
NIST SP 800-53 Rev.4	Transmission Confidentiality and Integrity		3	4	2	3	11
	Restore the Availability	N/A	PC	FC	II	I	
ISO 27001:2013	Information backup		3	4		6	11
ISO 27552	Information backup*		3	4		5	11
ISO 27001:2013	Responsibilities and procedures		4	3	2	3	10
ISO 27001:2013	Planning information security continuity		3	4	2	4	11

ISO 27001:2013	Availability of information processing facilities		5	2	2	3	9
COBIT 2019	Develop and implement a business continuity response		4	3	2	3	10
COBIT 2019	Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)		3	4	2	4	11
NIST SP 800-53 Rev.4	Contingency Plan		5	2	1	4	9
	Regularly Testing, Assessing and Evaluating	N/A	PC	FC	II	I	
ISO 27001:2013	Independent review of information security	1	4	2	2	3	8
ISO 27552	Independent review of information security*	1	3	3	2	2	9
COBIT 2019	Monitor internal controls		4	3	3	2	10
COBIT 2019	Review effectiveness of business process controls	1	5	1	2	2	7
COBIT 2019	Perform control self-assessments		6	1	2	2	8
COBIT 2019	Identify and report control deficiencies		3	4	1	3	11
NIST SP 800-53 Rev.4	Continuous Monitoring		6	1	3	1	8
	Approved Certification	N/A	PC	FC	II	I	
ISO 27001:2013	Independent review of information security		5	2	2	3	9
ISO 27552	Independent review of information security*		5	2	2	3	9
	Notification of a personal data breach to the supervisory authority	N/A	PC	FC	II	I	
ISO 27001:2013	Responsibilities and procedures		2	5	1	5	12
ISO 27552	Responsibilities and procedures*		2	5	1	5	12
ISO 27001:2013	Response to information security incidents		4	3	4	2	10
ISO 27552	Response to information security incidents*		3	4	4	2	11
COBIT 2019	Define classification schemes for incidents and service requests		4	3	2	3	10

COBIT 2019	Identify and classify problems		4	3	4	2	10
NIST SP 800-53 Rev.4	Privacy Incident Response		4	3	3	3	10
	Communication of a personal data breach to the data subject	N/A	PC	FC	II	I	
ISO 27001:2013	Responsibilities and procedures		4	3	3	3	10
ISO 27552	Responsibilities and procedures*		3	4	2	4	11
ISO 27001:2013	Response to information security incidents	1	5	1	3	2	7
ISO 27552	Response to information security incidents*	1	4	2	3	2	8
COBIT 2019	Define classification schemes for incidents and service requests	2	4	1	3	1	6
COBIT 2019	Identify and classify problems		5	2	3	3	9
NIST SP 800-53 Rev.4	Privacy Incident Response		3	4	3	3	11
	Data Protection Impact Assessment	N/A	PC	FC	II	I	
ISO 27001:2013	Understanding the needs and expectations of interested parties		5	2	3	3	9
ISO 27552	Understanding the needs and expectations of interested parties*		4	3	3	3	10
ISO 27552	Privacy impact assessment		2	5	3	3	12
ISO 27552	Cooperation agreement	1	3	3	3		9
ISO 27001:2013	Information security risk assessment		5	2	5		9
COBIT 2019	Collect data		4	3	5	1	10
COBIT 2019	Analyze risk		5	2	5		9
NIST SP 800-53 Rev.4	Privacy Impact and Risk Assessment		3	4	6		11
	Designation of the data protection officer	N/A	PC	FC	II	I	
ISO 27001:2013	Information security roles and responsibilities		3	4	1	5	11

ISO 27552	Information security roles and responsibilities*		3	4		6	11
COBIT 2019	Acquire and maintain adequate and appropriate staffing		2	5	4	2	12
NIST SP 800-53 Rev.4	Governance and Privacy Program		2	5	1	4	12
	Tasks of the data protection officer	N/A	PC	FC	II	I	
ISO 27001:2013	Information security roles and responsibilities		4	3	1	5	10
ISO 27552	Information security roles and responsibilities*		3	4	1	5	11
ISO 27001:2013	Information security awareness, education and training		4	3	4	2	10
ISO 27552	Information security awareness, education and training*		3	4	4	2	11
COBIT 2019	Establish roles and responsibilities		2	5	1	4	12
NIST SP 800-53 Rev.4	Governance and Privacy Program		2	5	1	3	12
	Certification	N/A	PC	FC	II	I	
ISO 27001:2013	Independent review of information security		5	2	1	3	9
ISO 27552	Independent review of information security*	1	4	2	1	3	8
	General principle for transfers	N/A	PC	FC	II	I	
ISO 27552	Identify basis for PII transfer between jurisdictions		4	3	3	3	10
ISO 27552	Basis for PII transfer between jurisdictions		4	3	3	3	10
NIST SP 800-53 Rev.4	Information Sharing with Third Parties		2	5	2	3	12