CLOUD COMPUTING AND GDPR: LEGAL AND TECHNICAL IMPLICATIONS
OF THE NEW REGULATION ON SAAS IN THE PORTUGUESE CONTEXT

Catarina Amaral da Costa Brás da Cunha

Uminho | 2019

Universidade do Minho
Escola de Direito

Catarina Amaral da Costa Brás da Cunha

CLOUD COMPUTING AND GDPR: LEGAL AND TECHNICAL IMPLICATIONS OF THE NEW REGULATION ON SAAS IN THE PORTUGUESE CONTEXT

outubro de 2019

Universidade do Minho
Escola de Direito

Catarina Amaral da Costa Brás da Cunha

CLOUD COMPUTING AND GDPR: LEGAL AND TECHNICAL IMPLICATIONS OF THE NEW REGULATION ON SAAS IN THE PORTUGUESE CONTEXT

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação de
Professor Doutor Francisco Andrade
Professor Doutor José Bacelar Almeida

outubro de 2019

AGRADECIMENTOS

Não raras vezes, agradecer algo é uma tarefa inglória, já que implica qualificar e quantificar a taxa de esforço ou de apoio que alguém nos deu em dado momento. Para mim, essa tarefa afigura-se como fácil, pois as pessoas que serão referidas indubitavelmente contribuíram para que esta dissertação fosse concluída com sucesso, tanto quanto me é possível aferir.

Desde logo, é com amor que agradeço à minha família, sem qualquer tipo de ordem preferencial (Mãe, Pai, Renata e babies). Por mais insana que possa parecer a jornada a que muitos chamam vida, eu não seria feliz sem eles. Reformulo: eu não seria eu sem eles. No máximo, seria uma sombra de mim.

Ao meu tio Eduardo, pelas palavras sábias que me transmite. Mesmo abordando o assunto mais trivial, tem uma capacidade de reflexão, conhecimento e espírito crítico que em muito admiro.

À Ângela, por ser uma irmã mais velha emprestada que está sempre disponível para me ajudar e me fazer rir com as suas histórias.

Às minhas companheiras de conhecimento, Ana e Joana. Há reuniões na vida que têm uma continuidade que inicialmente parecia ser efémera. Começamos como colegas, continuamos como amigas, na verdadeira aceção da palavra.

À Cristiana, por ao final de mais de 20 anos ainda termos momentos de aprendizagem juntas, tal como no início dos tempos.

À minha equipa, em especial ao meu chefe Jorge Ferreira, que muito teve que me fazer rir quando eu desesperava com a sobrecarga de trabalho e que sempre me apoiou quando bem foi necessário.

À Dr.ª Raquel, por me auxiliar a manter a sanidade mental ou mesmo a recuperá-la quando já me parecia perdida.

Ao meu mentor, Amadeu Recasens i Brunet, por saber como potenciar as minhas escolhas no meu caminho académico e profissional, nunca me dando a solução, mas sim as ferramentas.

A todos, muito obrigada.

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration.

I further declare that I have fully acknowledged the Code of Ethical Conduct of the University of Minho.

ABSTRACT

GDPR came into force, in order to reduce legal fragmentation, provide greater legal certainty, improve the protection of individuals, and contribute to the free flow of personal data within the Union but some uncertainties have arrived with it. The neutrality towards technology and the further data protection law developments, such as the Portuguese one, may create some grey areas that need further reflection.

Law needs to take into consideration some sources that it traditionally didn't, and it must acknowledge its dependence on cooperation with private experts to address inherent problems that come with the massive development in technology. Private standards are becoming increasingly important for the law and adopting them requires new procedural rules.

Data protection developments seem to be not as fast as the technological ones and cloud computing is just one example. Cloud computing can be considered a new paradigm that is rapidly changing the landscape of information technology and consequently, various business models have evolved to integrate this technology into software applications, programming platforms, data storage, computing infrastructures and hardware as a service. Once again., private experts were quicker than the legislator and addressed first the privacy issues on the cloud computing context.

This study aims to compare the already developed standards and the GDPR, in order to understand if compliance with the standards could be translated into compliance with the GDPR as well. If so, the Portuguese context will also be taken into consideration.

This study is focused on SaaS structures, more precisely from the processor's perspective, which, in this particular case, is the SaaS provider/developer.

KEYWORDS: GDPR; COMPLIANCE; SAAS; CLOUD COMPUTING; PORTUGAL

INDEX

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

2FA - Double Factor Authentication

API - Application Programming Interface

B2B – Business-to-Business

CFREU - Charter of Fundamental Rights of the European Union

CNPD – Comissão Nacional de Proteção de Dados

CPR - Constitution of the Portuguese Republic

CRUD - Create, Read, Update, Delete

CSA – Cloud Security Alliance

CSC - Cloud Service Customer

CSP – Cloud Service Provider

DB – Database

DNS - Domain Name System

DPIA – Data Protection Impact Assessment

DPO – Data Protection Officer

ECHR - European Court of Human Rights

ECJ – European Court of Justice

EEA – European Economic Area

ENISA - European Union Agency for Cybersecurity

EU – European Union

FE – Front-End

GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

I/O – Input/Output

IaaS – Infrastructure as a Service

ICT – Information and Communication Technology

IEC – International Electrotechnical Commission

IPQ – Instituto Português da Qualidade

ISMS - Information Security Management System

ISO – International Organization for Standardization

JTC – Joint Technical Committee

NIS Directive - Network and Information Security Directive

NSA - National Security Agency

OS – Operating System

OWASP - Open Web Application Security Project

PaaS – Platform as a Service

PET - Privacy Enhancing Technology

PIA – Privacy Impact Assessment

PII – Personally Identifiable Information

PIMS - Privacy Information Management System

SaaS – Software as a Service

SLA – Service Level Agreement

TEU – Treaty on European Union

TFEU - Treaty on the Functioning of the European Union

TLS - Transport Layer Security

ToE - Target of Evaluation

UDHR - Universal Declaration of Human Rights

URL - Uniform Resource Locator

VPN - Virtual Private Network

WG – Working Group

WP29 - Article 29 Data Protection Working Party

WWII - Second World War

CITATION STYLE

The chosen citation style for this dissertation was the APA style (6th edition).

However, some adjustments were made, since the European legislation has a different structure from the American one.

Therefore, when there are direct quotes related with legislation, instead of the page number, the Article and/or the Recital are provided. When there are direct quotes concerning the standards, the chapters are indicated.

To provide an easier reading, Articles/Recitals/Chapters may be included on the footnotes, when there is no direct quote.

The format of the Bibliography follows the conventional APA style, without any alterations.

1. Objectives and Research Questions

The GDPR, as a formal and European binding solution to data protection and privacy concerns, brought with it new challenges both on a legal level and on a technical level, especially if we consider ICT systems. While analysing the GDPR and its implementation under the Portuguese context, it is important to take into consideration a multilevel governance approach. Thus, it will be considered the global regulatory dimension as well as mutual interactions between global, European and national regulatory processes, as recommended by the literature (Wouters, Wessel, & Follesdal, 2008). Therefore, besides the European legal framework and its impact, it will also be analysed the specific consequences on the Portuguese context under this new regulation [1], considering the guidelines and policies developed within this country. The national and European legal order is part of, and subject to, a multilevel normative process. Thus, the creation, interpretation and application of national and European norms must take account of the multilevel structure of the system (Wouters et al., 2008).

With this dissertation, it will be assessed which are the implications of the GDPR in cloud services, namely on SaaS structures, both on a legal and technical perspective.

More than a legal approach, it is expected to assess the technical implications that both European and Portuguese approaches bring to the processes related to SaaS structures.

Therefore, a qualitative approach will be chosen, not in the traditional non-doctrinal research sense (Dobinson & John, 2017), but taking into account its premises, while considering the technical impact that the new regulation will carry with it.

Considering that the GDPR is technologically neutral, it will be assessed if a public SaaS structure would be compliant with GDPR if it follows ISO/IEC standards. It will be assessed if a SaaS structure would be compliant with GDPR (and if so, afterwards with the Portuguese approach) if designed following the ISO/IEC 29100 family of standards[2], namely ISO/IEC 29100:2011[3], ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019, considering the data protection/privacy requirements needed for planning, designing and building ICT system architectures.

[1] A regulation is a document adopted by an authority providing binding legislative rules. (ISO, n.d.-h).

[2] A standard is a document that provides rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order and harmonization in a given context, being based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits, being established by consensus and approved by a recognized body (ISO, n.d.-h).

[3] Amended by the 2018 version.

It is important to clarify that this study will consider the point of view of the actor that designs/develops the SaaS structure and afterwards the point of view of the actor that makes available the SaaS structure to the public. Other perspectives will be left for further studies.

Thus, this dissertation has got several main research questions.

As for the design/implementation of data protection requirements on ICT systems, namely on SaaS structures:

1. Does the combination of ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019 standards have the same function, considering the design and implementation of data protection requirements to ICT systems, as interpreted by the functional method, as the GDPR regarding data protection?
2. If the first question has got a positive answer, then would a combination of the ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019 standards be an accurate technical approach regarding public SaaS solutions to be compliant with the GDPR?
3. If the second question also has got a positive answer, would a combination of the ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019 standards be an accurate technical approach regarding public SaaS solutions to be compliant with the Portuguese data protection law, that regulates the implementation on the national context of GDPR?

2. Legal and Political Context

2.1. Globalization, Multilevel Governance and Legal Pluralism

Globalization and global governance have become central themes in the study of international and national law (Wessel & Wouters, 2007, 2008). More legislating actors appear, operating in different legal fields and on different levels (Günther, 2008). Also, in technology, among others areas, private actors create their own law, without any involvement of a public legislator (Günther, 2008).

With the development of the international legal order, the creation of legal norms outside the national legal systems has grown. This has a particular effect on the European Union: more than affecting EU Member States, European Law is increasingly affecting their citizens and businesses (Wessel & Wouters, 2008). In this sense, it is possible that the effect of integration and the impact of the European Law will destroy or replace existing national legal orders (Karhu, 2004). While national governments are participants in EU policy making, control was given to supranational institutions and, consequently, the locus of political control has changed (Hooghe, Marks, & Marks, 2003). Also, the boundaries between European and national law became blurred and precarious, while national legal systems are increasingly influenced of international regulation (Bache, 2005; Wessel & Wouters, 2008; Wouters et al., 2008).

At this point is important, to elaborate a distinction between multilevel governance and legal pluralism, because these two concepts will be key elements of the chosen methodology. The first concept is focused on different legal levels and related policies, as well as mainly on a vertical structure (considering supra national, national, regional and local structures), with increased attention on the horizontal dimension (since non-state actors are becoming important in policy-making) (Bache, 2005; Trnski, 2005). The second concept is devoted to the analysis of different legal structures, considering the inherent culture and formality (Tamanaha, 2008).

One example of the infranational legal norms already being superimposed by international and even supranational norms is the European Union law that deeply transforms the national law of the member states (Günther, 2008). With the multi-level governance, European integration has diminished the prerogatives of the state. The state no longer monopolizes European level policymaking, or the aggregation of domestic interests. Instead, the decision-making competencies are shared by actors at different levels rather than monopolized by the States (Hooghe & Marks, 2003; Trnski, 2005).

There is a top down impact of the EU on its member states, with European decisions' impacting member states' politics and policies, with processes of a construction, diffusion and institutionalization of formal and informal rules, procedures, policy paradigms, shared beliefs and norms which are first defined and consolidated in the EU policy process and the incorporated in the national discourse, political structures and public policies. In contrast, there is also process whereby national systems (institutions, policies, governments) shape EU (Bache, 2005; Trnski, 2005). Each level of actors holds important resources, such as information, political power, expertise and prestige, and they all are negotiating, impacting the other level (Trnski, 2005).

The European Commission characterizes the EU as one "based on multi-level governance in which each actor contributes in line with his or her capabilities or knowledge to the success of the overall exercise. In a multi-level system, the real challenge is establishing clear rules for how competence is shared – not separated; only that non-exclusive vision can secure the best interests of all the Member States and all the Union's citizens"(European Commission, 2001, pp. 34–35).

An early explication referred to multilevel governance as "a system of continuous negotiation among nested governments at several territorial tiers"(Marks, 1993, p. 392) and described how supranational, national, regional, and local governments are tangled in territorially overlapping policy networks (Bache, 2005). Multilevel refers to "the increased vertical interactions and interdependence between governments operating at different territorial levels" (Bache, 2008, p. 24), while governance signalled the "growing horizontal interactions between governments and nongovernmental actors" (Bache, 2008, p. 24).

In the EU, domestic implementation of EU policies is problematic because Member States often have incentives to avoid compliance (such as a divergence in political interests, that could lead to parties being outvoted or such as free-riding) while, at the same time, monitoring and enforcing compliance with EU law is costly, difficult, and inevitably strategic (Toshkov, 2016).

In Portugal, there is a weak multilevel governance, despite incremental shifts toward greater subnational and nonstate participation and the creation of new regional structures. The government retained a firm grip over much of the important decision making, with statist politics, a high level of institutional centralization coupled with limited control over decentralised expenditure (Bache, 2008, 2009; Chrabąszcz & Zawicki, 2016).

Different from the multilevel governance is the concept of legal pluralism, as previously referred.

In Moore's words, "the law" may be understood "a short term for a very complex aggregation of principles, norms, ideas, rules, practices, and the activities of agencies of legislation, administration, adjudication and enforcement, backed by political power and legitimacy" (Moore, 1973, p. 719). However, as also stated by the author, though the formal legal institutions the monopoly on the legitimate use of force, they cannot be said to have a monopoly of any kind on the other various forms of effective coercion or effective inducement (Moore, 1973). Many other normative communities articulate norms without formal state power behind them (Berman, 2007). Between the political body and the individual, there are other organized social fields to which the individual is part of, and each of these social fields has got its own customs and rules and the means of coercing or inducing compliance (Moore, 1973).

In the words of Griffiths, "legal pluralism is a concomitant of social pluralism: the legal organization of society is congruent with its social organization. Legal pluralism refers to the normative heterogeneity attendant upon the fact that social action always takes place in a context of multiple, overlapping "semi-autonomous social fields", which, it may be added, is in practice a dynamic condition" (Griffiths, 1986, p. 38).

Various social actors create valid norms and there is a plurality of collective normative systems in a society: legal norms (in the narrow sense) interact with other normative systems in a society (Moore, 1973). In this sense, law is not only internally pluralistic, but it is also externally dependent on other kinds of normative systems (Günther, 2008).

Therefore, legal theory must deal with many different normative systems (Günther, 2008), since our world has multiple normative communities (Berman, 2007). The global legal system is a network of jurisdictional assertions by state, international, and non-state normative communities (Berman, 2007).

A complex mix of public, private, state- and non-state-based norms, principles and rules, (created and maintained by a diverse set of actors, including experts), shapes law. Therefore, governance rules are evolving on a framework constituted by local and transnational actors and norms connected through networks and standards (Zumbansen, 2012), as state law becomes a component in a complex network of national, transnational and international private and public norms (Ladeur, 2004).

The plurality of legal sources and its impact on decision making has to be considered (Ladeur, 2004). Non-state legal (or quasi-legal) norms add to the hybridity. Given increased migration and global communication, people have different affiliations and act based on it, while multiple communities are added to the original territorial ones. Such non-state legal systems often influence (or are incorporated into) state or international rules (Berman, 2007).

Globalisation creates and changes complex legal configurations (von Benda-Beckmann, 2002) and as the global expansion of the economic system is supported by scientific inventions and considering the new developments in ICT, various attempts to promote international legal regulations were made (Günther, 2008). For instance, it is possible to observe tendencies towards self-regulation among scientists (Günther, 2008). In fact, scholars observed that there is a whole range of non-state law-making even in modem nation-states, including corporate bylaws, social customs, private regulatory bodies, and a wide variety of groups, associations, and non-state institutions that can influence it (Berman, 2007).

The law must acknowledge its dependence on cooperation with private actors, since they generate specialised types of knowledge. Private standards are becoming increasingly important for the law and adopting them requires new procedural rules since otherwise it might undermine the homogeneity of the legal system (Ladeur, 2004).

2.2. Privacy as a Fundamental Right

If privacy has largely been a matter of law and policy, security has largely been a matter of technology and policy (IAPP-OneTrust, 2018), even if it was protected as a fundamental right as the other one, considering the UDHR (United Nations, 1948), CFREU (Charter of Fundamental Rights of the European Union, 2012), and considering the Portuguese context, the CPR (Constitution of the Portuguese Republic, 2005).

The Hague Peace Conference of 1899 provided the basic mechanisms of protecting human beings through international agreement between states. For the first time, human rights were regarded as distinct from state rights. Although the purpose of the Conference failed, with the beginning of the first world war, it was the first effort to develop universal standards of justice, which eventually were materialized at the end of the WWII (Normand & Zaidi, 2008). As a consequence of WWII there was a tremendous international pressure to include an international bill of rights in the Charter of the United Nations (Morsink, 1999; Normand & Zaidi, 2008). The UDHR was then adopted in 1948, being regarded as a Human Rights standard (ONU, 2017), determining the ideals related to the principles and rights (Hannum, 1995; Nickel, 1987), going beyond that what was initially predicted. It is a paradigm, on a direct and indirect manner, at a constitutional, legal and political level on what regards human rights protection (Hannum, 1995).

As it was expected, on a post war context, individuals' security was one of the main concerns to be considered, which was reflected in the Article 3 of the UDHR: "Everyone has the right to life, liberty and security of person." (United Nations, 1948, p. 2). Also, the right to privacy emerged in the international law (Hustinx, 2014), being referred on the Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." (United Nations, 1948, p. 4). It is interesting to consider that if the Article 3 the UDHR seems to consider the right to security as an absolute right, the Article 12 makes a remission to the law, even though its terms are not precise regarding the nature of the law itself.

In 1950, the Governments members of the Council of Europe, considering the UDHR and reaffirming their belief in those freedoms, made an agreement, which was materialized on the Convention for the Protection of Human Rights and Fundamental Freedoms, also known as European Convention on Human Rights (European Convention on Human Rights, 1950; van Dijk & Hoof, 1998).

This Convention was designed by the Council of Europe, on a harmonizing attempt between countries during the post WWII period (Harris, O'Boyle, Bates, & Buckley, 2014). This document was ratified by 47 countries (Council of Europe, 2018). Portugal only done such in 1979 (Ministério dos Negócios Estrangeiros, 1979). On its Article 5, it is referred that "Everyone has the right to liberty and security of person." and on the Article 8 it is stated that "Everyone has the right to respect for his private and family life, his home and his correspondence.", giving on its number 2 the following exceptions

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (Conselho da Europa, 1950).

In 2000, the CFREU was created (Vries, 2017). Although human rights did not figure in the original Treaties, they steadily gained in importance from the late 1960s. The Charter set up the main Fundamental Rights, being the first Bill of Rights developed specifically to the EU, comprising a broad range of civil, political and social rights (Zetterquist, 2011). The Charter states on its Article 6 that "Everyone has the right to liberty and security of person." and on its Article 7 that "Everyone has the right to respect for his or her private and family life, home and communications.". Moreover, on Article 8 it defends the "Protection of personal data", indicating that

> Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these

> rules shall be subject to control by an independent authority (Charter of Fundamental Rights of the European Union, 2012).

Clearly the EU was already concerned regarding how personal data could be processed and under which circumstances. The “Freedom of expression and information” was also protected on the Charter on its Article 11 “Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The freedom and pluralism of the media shall be respected.” (Charter of Fundamental Rights of the European Union, 2012).

Finally, the Charter defines on the Article 52 the “Scope of guaranteed rights”, indicating that

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Rights recognised by this Charter which are based on the Community Treaties or the Treaty on EU shall be exercised under the conditions and within the limits defined by those Treaties.

Even though the Charter contains rights that shall be the same as those laid down on the Convention for the Protection of Human Rights and Fundamental Freedoms, it also considers the possibility of the Union law to provide a more extensive protection (Charter of Fundamental Rights of the European Union, 2012). This is a clear indicator that the European Union is devoted to a more protective approach than the Convention if needed.

The Charter is legally binding, being a Constitutional Treaty elaborated by representatives of national parliaments and governments, aiming to promote public awareness (Zetterquist, 2011).

3. GDPR

3.1. Origins

Since years 80, with the increase of information systems capacity, the Internet development and the amount of processed personally identifiable information, privacy and data protection [4] have become a major issue for individuals and organisations, as well as for regulatory authorities (ISO/IEC JTC 1/SC 27/WG 5 & Information, 2017).

The privacy concept has been under considerable change due to the fact of the creation of new social interactions and groups, as well as of a different life experience provided by numerous new technologies (Zhao, 2014). The internationalisation of personal data is due to a more universal life structure based on information digitisation intertwined with connected networks (Zhao, 2014).

The concept of “data protection” was developed in order to provide legal protection to individuals against the misuse of ICT for processing information relating to them. This was based on the conviction that the extensive use of ICT for this purpose could have broader effects for the rights and interests of individuals (Hustinx, 2014). As predicted, the universalisation of information privacy has made long-term impacts on individuals’ lives and laws (Zhao, 2014).

It is possible to consider that privacy and data protection are two sides of the same coin: privacy is related with the right to respect for private life; data protection is related with the right to the protection of someone's personal data. Both are related expressions of a universal idea with strong ethical dimensions: the dignity, autonomy and unique value of every human being (Hustinx, 2014).

In 1968, the Parliamentary Assembly of the Council of Europe asked the Committee of Ministers to examine whether the European Human Rights Convention and the domestic law of the Member States offered adequate protection to the right of personal privacy considering the impact of modern science and technology. A study showed that the national legislations gave insufficient protection to individual privacy and other rights and interests of individuals with regard to automated data banks. Based on these findings, the Committee of Ministers adopted in 1973 and 1974 two resolutions on data protection. The first, Resolution (73)22, established principles of data protection for the private sector and the second,

[4] In the original reference, the term data privacy is used. However, since privacy is a human right related to the intimacy of a natural person and data protection to the protection of personal data related to that natural person, the original term was replaced. Further distinction between the two concepts will be further provided.

Resolution (74)29, did the same for the public sector (Council of Europe, 1981b). Following these Resolutions, the data protection as a fundamental right protected by CPR has its origins in 1976, being subject to alterations in 1982, 1989 and 1997 (Marques & Martins, 2000).

The positive experiences with these initiatives encouraged the Council of Europe to prepare the first binding instrument on the subject. Then, in 1981, there was the adoption of the Data Protection Convention, also known as Convention 108 (Council of Europe, 1981a; Hustinx, 2014; Lynskey, 2015). It is important to state out that it was open for signature to countries outside Europe (Rudgard, 2018).

The Convention 108 was the first legally binding international instrument in data protection (Rudgard, 2018) and had as main purpose to achieve greater unity on this matter between its members. Also, it considered that would be desirable to extend the safeguards for everyone's rights and fundamental freedoms, in particular the right to the respect for privacy. This was considered in the context of an increasing flow across frontiers of personal data undergoing automatic processing (Council of Europe, 1981a).

The real objective of the Convention was to protect individuals against unjustified collection, recording, use and dissemination of their personal details. The Convention's main objective was that any processing of personal data would always observe certain legal conditions (Hustinx, 2014).

Although the provisions of the Convention were not intended to be directly applicable or included in judicial supervision of the ECHR, the ECHR has ruled in several cases that the protection of personal data is of "fundamental importance" for a person's enjoyment of the right to respect for private life under Article 8 ECHR (Hustinx, 2014). Once again, it is possible to conclude how data protection and the privacy rights are related.

Moreover, the Court ruled there are positive obligations for the Member States and that they may be held liable for a breach of privacy committed by a private party:

> The Court reiterates that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (European Court of Human Rights, 2004a, p. 12)

as well as

> The Court reiterates that although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves (European Court of Human Rights, 2004b, p. 23).

Nevertheless, both judgments fail to clarify the criteria for evaluating a legitimate expectation of respect for privacy (Rudolf, 2006).

Although the Council of Europe succeeded in putting data protection on the agenda and setting out the main elements of a legal framework, it failed in terms of ensuring enough consistency across its Member States. Thus, at the end of 1990, the European Commission submitted a proposal for a Directive in order to harmonize the national laws on data protection in the private and most parts of the public sector (Commission of the European Communities, 1990; Hustinx, 2014).

The increasingly frequent processing of personal data in economic and social activities and the new data-exchange requirements enhanced the need in the European Community of measures to ensure the protection of individuals in relation to the processing of personal data. Also, it improved the need of information security processing, considering the development of open telecommunications networks (Commission of the European Communities, 1990).

Following a diversity of national approaches (Commission of the European Communities, 1990), the Directive 95/46/EC (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995) was designed and implemented, aiming to accelerate the harmonization of provisions concerning the protection of data and privacy (Commission of the European Communities, 1990). In addition, the Directive required Member States neither to restrict, nor to prohibit the free flow of personal data between Member States for reasons connected with such protection. This was intended to achieve a balanced development of the internal market, while bringing an equivalent high level of protection in all Member States (Hustinx, 2014; Reding, 2012).

The Directive 95/46/EC set a milestone in the history of the protection of personal data in the European Union (Reding, 2012; Rudgard, 2018). Since the protection of personal data is considered to be one of the basic values in Europe, EU legal rules on data protection do not discriminate between EU citizens and foreigners: the fundamental right to personal data protection is guaranteed to every person in Europe, both citizens and non-citizens (Reding, 2011).

Also, the Directive 95/46/EC pointed out that the approximation of laws in different countries mustn't result in any lessening of the protection they afford but must ensure a high level of protection in the Community (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995).

The Directive aimed to give substance to and amplify the rights contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals, with regard to Automatic Processing of Personal Data, as the principles of protection must apply to any information concerning an identified or identifiable person (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995).

Since the Directive adopted generally formulated concepts and open standards, it permitted Member States to be flexible on the transposition (Hustinx, 2014; Lynskey, 2015; Reding, 2012). The result was a fragmented legal environment and unequal protection for data subjects (Lynskey, 2015; Reding, 2012). Due to the Directive's failure to create uniformity, a regulation was needed to create legal certainty within the internal market and to ensure the data protection by and within the EU (Schwarz, 2014)

The entry into force of the Lisbon Treaty in December 2009 had an enormous impact on the development of EU data protection law (Casagran, 2016; European Commission, 2012a; Hustinx, 2014; Kuner, 2012; Lynskey, 2015). As a binding instrument, not only for the EU institutions and bodies, but also for the Member States acting within the scope of EU, the right to the protection of personal data reinforced, as it was specifically mentioned in Article 16 (Lynskey, 2015; Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community, 2007, p. 51). The Lisbon Treaty closed the loopholes regarding data protection in the EU, ending the risk of adoption of 27 different bilateral agreements (Casagran, 2016).

After several Directive reports regarding its implementation (European Commission, 2012a; Hustinx, 2014) and the consultation on the legal framework for the fundamental right to protection of personal data launched by the European Commission in July 2009 (Article 29 Data Protection Working Party, 2009; Reding, 2011), coinciding with the Lisbon Treaty, it was clear that a comprehensive approach on personal data protection in the European Union was required. Thus, a communication was done (European Commission, 2010).

The rapid technological developments, globalisation, the capabilities of modern technologies, the increased universalization of data flows and the increased access to personal data by law enforcement authorities brought new needs considering the protection of personal data (European Commission, 2010, 2012a; Reding, 2011). It became clear that the EU needed a comprehensive and coherent approach in its policy for the fundamental right to personal data protection, for the EU and beyond (European Commission, 2012a; Kuner, 2012; Reding, 2011). Therefore, it was stated that the Commission would assess the need to adapt other legal instruments to the new general data protection framework (European Commission, 2010; Kuner, 2012).

It was needed to reinforce individuals' rights by ensuring that they have a high level of protection and maintain control over their data, particularly in the online environment, where data protection cloud be not assured, since policies are often unclear, non-transparent, and not always in full compliance with existing rules. Individuals needed to be well-informed in a clear and transparent way by data controllers about how and by whom their data are processed and what are and how to exercise their rights. for free and without excessive constraints (Reding, 2011).

Meanwhile, in May 2013, Edward Snowden stole approximately 1.7 million documents of secret data from the NSA and delivered them to news agencies in order to expose many secret programs conducted against its own citizens, foreign leaders and various targets abroad. These files detailed domestic spying programs held by the NSA that collect data from average American citizens through various online sources (Verble, 2014).

The NSA collected the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers, under a top-secret court order issued in April 2013. The order required Verizon to daily give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries, including the numbers of both parties, location data, call duration, unique identifiers, and the time and duration of all calls (Lyon, 2014; The Guardian, 2013a).

In June 2013, Snowden revealed that NSA was focused on getting intelligence by any means possible, targeting communications of individuals and being able to wiretap any person (The Guardian, 2013b). As encryption tools were gradually blanketing the Web, the NSA invested billions of dollars to preserve its ability to eavesdrop, deploying custom-built, superfast computers to break codes and collaborating with technological partners to build entry points into their products (Perlroth, Larson, & Shane, 2013).

The secret US-NSA program, PRISM, devoted to large-scale mass surveillance of the telecommunication and electronic messages of governments, companies, and citizens, including the United States' allies (Bauman et al., 2014), had a major impact on individuals' privacy. The NSA programs were designed to harvest data from Internet cables and/or to intercept data during their travel. Also, NSA and several European services had a program devoted to the acquisition of consumers' personal data, forcing private companies (such as Google, Microsoft, Apple, or Skype) to collect and deliver data to the intelligence services without the knowledge of users. Finally, there was also a practice which involved the collection of phone calls, text messages, Skype communications and the diverse audio and video signals that passthrough computers, smart phones, satellite communications, and traditional landlines (Bauman et al., 2014; Lyon, 2014).

Snowden's revelations regarding mass surveillance had political repercussions through 2013 and into 2014 and raised profound legal questions. Two interconnected human rights issues arise with regard to mass surveillance: the first is the right of every person to respect for his or her private and family life; the second is the duty of States to protect personal data (Bauman et al., 2014).

In the Google Spain case, the ECHR enhanced the protection of personal data of citizens of the EU, considering that search engines are data controllers, processing personal data according to certain manners and purposes (ECJ, 2014b). This decision was made at a critical moment of EU's data protection law reform, which comprised a series of efforts to enhance personal data protection in the post-Snowden era (Zhao, 2014).

As for the Digital Rights Ireland case, the CJEU determined that the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid, since the Directive 2006/24 didn't provide sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data (ECJ, 2014a).

Finally, in the Schrems case, the EJC referred that the Decision 2000/520 (Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce) was invalid, since the Directive 95/46 prohibited transfers of personal data to a third country not ensuring an adequate level of protection (EJC, 2015).

The growing tendency of providing “free” services in exchange for monitoring created opportunities for large scale spying by many actors, some of them unknown. Therefore, the review of the EU legal framework for data protection took place in a context where the need for more effective protection and the challenges to deliver that protection in practice increased enormously, considering that information technology is playing a prominent role in all fields of life (Hustinx, 2014). Taking this context into account, the Data Protection Directive was then object of a wide review to make it more effective (Hustinx, 2014). Thus, the GDPR proposal was based on Article 16 of the Treaty on the Functioning of the European Union (TFEU). This Article, introduced by the Lisbon Treaty, is the new legal basis for the adoption of comprehensive data protection rules (Reding, 2012).GDPR:

3.2. Portrayal of the New Regulation

Like technology, the way personal data are used and shared in society is permanently changing. This poses a challenge to legislators, since there is a need to establish a legislative framework that will stand the test of time (Reding, 2011).

After assessing the impacts of different policy options, the European Commission proposed that the new framework would consist of a Regulation, replacing Directive 95/46/EC (European Commission, 2012a). This decision took into consideration that the standards implemented on

the Directive 95/46/EC should be kept but the existing deficiencies from the Directive were corrected. The direct applicability of a Regulation in accordance with Article 288 TFEU would reduce legal fragmentation[5], since it would put an end to the cumulative and simultaneous application of different national data protection laws. That would provide greater legal certainty, improve the protection of individuals, and contribute to the free flow of personal data within the Union. (European Commission, 2012a; Poullet, 2018; Reding, 2012). Paper-based and bureaucratic requirements wouldn’t be needed and compliance, harmonization of the law, and individual empowerment would be easier to achieve (European Commission, 2012a; Kuner, 2012).

In fact, several benefits that would come with the new Regulation where referred by the European Commission on a Communication made to the European Parliament and the Council, such as: 1) a

[5] Even if there is some heterogeneity, as a result of Member States being allowed to maintain or introduce national provisions to further specify the application of the rules of the GDPR concerning the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Moreover, Member States have several sector-specific laws in areas that need more specific provisions and, therefore, GDPR also provides a margin of manoeuvre for Member States to specify its rules (GDPR, 2016, Recital 12).

harmonised legal framework leading to a uniform application of rules to the benefit of the EU digital single market, that would be enforced with the one-stop-shop mechanism; 2) a level-playing field for all companies operating in the EU market, since the Regulation requires companies based outside the EU to apply the same rules as companies based in the EU if they are offering goods and services related to the personal data or are monitoring the behaviour of individuals in the Union; 3) the principles of data protection by design and by default creating incentives for innovative solutions to address data protection issues from the start; 4) stronger individuals' rights, with the introduction of new transparency requirements, as well as strengthened rights of information, access and erasure ("right to be forgotten"); 5) silence or inactivity will no longer be considered as valid consent as a clear affirmative action to express the consent is required; 6) protection of children on the online domain; 7) more control over personal data for individuals, that is materialized on a new right to data portability, avoiding the "lock-in" of personal data, and encourage competition between companies; 8) it's easier for citizens to switch between different service providers, which will encourage the development of new services in the context of the digital single market strategy; 9) stronger protection against data breaches, since the Regulation introduces an obligation to notify the supervisory authority at the latest within 72 hours when the data breach is likely to pose a risk to the individual's rights and freedoms – moreover, in certain circumstances, it obliges to inform the person whose data is concerned by the breach; 10) data protection authorities have the power to impose fines on controllers and processors; 11) more flexibility for controllers and processors processing personal data due to unambiguous provisions on responsibility (the accountability principle); 12) more clarity on the obligations of processors and the responsibility of controllers when selecting a processor; 13) a modern governance system to ensure that the rules are enforced more consistently and strongly; 14) the protection of the personal data guaranteed by the Regulation travels with the data outside the EU ensuring a high level of protection (European Commission, 2018).

3.2.1. Subject-matter and objectives

GDPR lays down rules relating to the protection of natural persons about the processing of personal data and rules relating to the free movement of personal data, considering that the processing of personal data should be designed to serve mankind [6](GDPR, 2016).

[6] See Article 1 and Recital 4 of GDPR.

GDPR also protects fundamental rights and freedoms of natural persons and their right to the protection of personal data, as the protection of natural persons in relation to the processing of personal data is a fundamental right [7] (GDPR, 2016).

In this context, it is important to keep in mind the Recital 8, which indicates that where GDPR "provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law" (GDPR, 2016, Recital 8). This is aligned with provisions indicated by CNPD, as it will be further referred[8]. In accordance, the national legislation is meaningful to properly apply the GDPR under some circumstances (Pinheiro, Coelho, Duarte, Gonçalves, & Gonçalves, 2018), as previously referred, especially considering several sector-specific national laws in areas that need more specific provisions and where the GDPR provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ("sensitive data") (GDPR, 2016, Recital 10).

Nevertheless, the right to the protection of personal data is not an absolute right and, therefore, it must be considered in relation to its function in society and be balanced against other fundamental rights, taking into consideration the principle of proportionality. GDPR respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties [9] (GDPR, 2016). Therefore, the "free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data" (GDPR, 2016, Article 1(3)), since GDPR is intended to contribute to the "accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons" (GDPR, 2016, Recital 2).

GDPR also allows for Member States to specify its rules, including for the processing of special categories of personal data and the definition in Member State law of the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal

[7] See Article 1 of GDPR.

[8] See subchapter 3.4.2.

[9] See Recital 1 and Recital 4 of GDPR.

data is lawful[10] (GDPR, 2016). As stated before, this can be understood as an element that may point out some heterogeneity on the application of the GDPR [11].

3.2.2. Material scope

As defined on the Article 2(1), the GDPR applies to "the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system", which means that manual processing is included, if the personal data are contained or are intended to be contained in a filing system[12] (GDPR, 2016). Therefore, and in order to prevent a legal gap and a serious risk of circumvention, the protection of natural persons should be technologically neutral and independent of the used techniques[13] (GDPR, 2016).

However, on the Article 2(2), exceptions to the provisions indicated before are defined:

> This Regulation [GDPR] does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c) by a natural person in the course of a purely personal or household activity[14]; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. (GDPR, 2016).

Moreover, specific guidance is provided for the processing of personal data by the Union institutions, bodies, offices and agencies on Article 2(3) (GDPR, 2016).

[10] See Recital 10 of GDPR.

[11] For further detail, please see the opinion of Alexandre Sousa Pinheiro (Pinheiro et al., 2018).

[12] See Recital 15 of GDPR.

[13] See Recital 15 of GDPR.

[14] For this matter, the Lindqvist case must be analyzed (EJC, 2003)

3.2.3. Territorial scope

With increased territorial scope, the Regulation is applied to all companies processing the personal data of data subjects who are in the Union, regardless of the company's location[15], which is an innovation (EUGDPR.org, n.d.; GDPR, 2016).

GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, even if the processing takes place outside the Union[16,17] (GDPR, 2016). Establishment implies the "effective and real exercise of activity through stable arrangements and the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect" (GDPR, 2016, Recital 22). Once it is concluded that a controller or processor is established in the EU, an *in concreto* analysis should be done to determine whether the processing is carried out in the context of the activities of this establishment, and, therefore, to determine if Article 3(1) applies. In this sense, the EDPB considers that, for the purpose of Article 3(1), the meaning of "processing in the context of the activities of an establishment of a controller or processor" is to be understood considering the relevant case law. Moreover, it is the presence, through an establishment, of a data controller or processor in the EU and the fact that a processing takes place in the context of the activities of that specific establishment that makes the GDPR applicable in that specific scenario (European Data Protection Board, 2018b).

GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: "offering goods or services to EU citizens or the monitoring of behaviour that takes place within the EU" (GDPR, 2016, Article 3(2)) or where Member State law applies by virtue of public international law[18] (GDPR, 2016).

It is important to keep in mind that the application of the targeting criteria is not limited by the citizenship, residence or other type of legal status of the data subject (European Data Protection Board, 2018b), as the Recital 14 clearly states: "The protection afforded by this Regulation [GDPR] should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data." (GDPR, 2016, Recital 14). The requirement that the data subject is located in the Union must be evaluated at the moment of offering of goods or services or the moment when the behaviour is being monitored (European Data Protection Board, 2018b). Moreover, it should be noted that the processing

[15] See Article 3(1) of GDPR.

[16] See Article 3(1) and Recital 22 of GDPR.

[17] The EJC provided guidance on this matter on the Google Spain case (ECJ, 2014b).

[18] See Article 3(3) of GDPR.

of personal data of EU citizens or residents that takes place in a third country does not trigger the application of the GDPR, except when the processing is related to a specific offer directed at individuals in the EU or to a monitoring of their behaviour in the Union (European Data Protection Board, 2018b).

To determine whether a controller or processor is offering goods or services[19] to data subjects who are in the Union, it should be determined if it is apparent that the controller or processor has an intention (materialized by a behaviour) to offer services to data subjects in one or more Member States in the Union. Factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, should be considered to do that evaluation [20] (European Data Protection Board, 2018b). These processing activities related to offering goods or services to such data subjects don't need to be connected to a payment[21] (GDPR, 2016).

In respect to the monitoring of behaviour that takes place within the EU, it should be determined if natural persons are tracked on the internet, including potential subsequent use of personal data processing techniques which consist of profiling a natural person[22] (GDPR, 2016). While Recital 24 of GDPR exclusively relates to the monitoring of a behaviour through the tracking of a person on the internet, the EDPB considers that tracking through other types of network or technology involving personal data processing should also be taken into account in determining whether a processing activity amounts to a behavioural monitoring, since the use of the word "monitoring" implies that the controller has a specific purpose for the collection and subsequent reuse of the relevant data about an individual's behaviour within the EU (European Data Protection Board, 2018b).

3.2.4. Definitions

The GDPR provided more definitions than the previous Directive 95/46/CE: if previously we had 8 definitions, the Regulation now has got 26. This may be understood as a need of enforcing protection and the security of processing, an introduction of clarification of certain types of data and the need to create other definitions considering the scope of the GDPR and the autoregulation model (Pinheiro et al., 2018).

[19] The offering of services also includes the offering of information society services (European Data Protection Board, 2018b).

[20] See Recital 23 of GDPR.

[21] See Recital 23 of GDPR.

[22] See Recital 24 of GDPR.

The following concepts are defined on GDPR and some of them will be subject to further comparison with the ones provides by ISO 29100:

1) personal data:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR, 2016, Article 4(1)).

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols[23] (GDPR, 2016). It is important to clarify that GDPR does not apply to the personal data of deceased persons and Member States may provide for rules regarding the processing of personal data of deceased persons[24] (GDPR, 2016);

2) processing:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (GDPR, 2016, Article 4(2));

3) restriction of processing – "the marking of stored personal data with the aim of limiting their processing in the future" (GDPR, 2016, Article 4(3));
4) profiling:

any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (GDPR, 2016, Article 4(4)).

[23] See Recital 30 of GDPR.

[24] See Recital 27 of GDPR.

Natural persons may be associated with online identifiers that when combined with unique identifiers and other information, may be used to create profiles of the natural persons and identify them[25] (GDPR, 2016). Profiling is constituted by three elements: 1) it has to be an automated form of processing; 2) it has to be carried out on personal data; and 3) the objective of the profiling must be to evaluate personal aspects about a natural person (Article 29 Data Protection Working Party, 2018a);

5) pseudonymisation:

processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (GDPR, 2016, Article 4(5)).

Moreover, personal data

which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments (GDPR, 2016, Recital 26);

6) filing system – "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis" (GDPR, 2016, Article 4(6));

7) controller:

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (GDPR, 2016, Article 4(7));

8) processor – "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (GDPR, 2016, Article 4(8));

9) recipient:

[25] See Recital 30 of GDPR.

a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing (GDPR, 2016, Article 4(9));

10) third party – "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data" (GDPR, 2016, Article 4(10));
11) consent of the data subject – "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (GDPR, 2016, Article 4(11));
12) personal data breach – "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (GDPR, 2016, Article 4(12));
13) genetic data:

personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question (GDPR, 2016, Article 4(13)).

Also,

genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained. (GDPR, 2016, Recital 34);

14) biometric data:

personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (GDPR, 2016, Article 4(14));

15) data concerning health – "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status" (GDPR, 2016, Article 4(15)). Therefore, personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (1) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test. (GDPR, 2016, Recital 35);

16) main establishment:

a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation (GDPR, 2016, Article 4(16)).

The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities are not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking (GDPR, 2016, Recital 36);

17) representative – "natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation" (GDPR, 2016, Article 4(17));
18) enterprise – "a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity" (GDPR, 2016, Article 4(18));
19) group of undertakings – "a controlling undertaking and its controlled undertakings" (GDPR, 2016, Article 4(19)). A group of undertakings

should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings. (GDPR, 2016, Recital 37);

20) binding corporate rules:

personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. (GDPR, 2016, Article 4(20));

21) supervisory authority – "an independent public authority which is established by a Member State pursuant to Article 51" (GDPR, 2016, Article 4(21));

22) supervisory authority concerned:

a supervisory authority which is concerned by the processing of personal data because: a) the controller or processor is established on the territory of the Member State of that supervisory authority; b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or c) a complaint has been lodged with that supervisory authority (GDPR, 2016, Article 4(22));

23) cross-border processing:

a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State. (GDPR, 2016, Article 4(23));

24) relevant and reasoned objection:

an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation [GDPR], which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union (GDPR, 2016, Article 4(24));

25) information society service – "a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1)" (GDPR, 2016, Article 4(25)). According to the EDPB, these services are defined: 1) as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services; 2) as any service which is not paid for directly by the persons who receive them, but are funded by other means, such advertising (European Data Protection Board, 2019b).

26) international organisation – "an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries." (GDPR, 2016, Article 4(26)).

3.2.5. Principles

In GDPR's Chapter II are defined the principles related to processing of personal data, lawfulness of processing, conditions for consent, conditions applicable to child's consent in relation to information society services, processing of special categories of personal data, processing of personal data relating to criminal convictions and offences and processing which does not require identification (GDPR, 2016). The principles of data protection should apply to any information concerning a data subject (GDPR, 2016). Overall, the characteristics of information and communication must be based on: 1) concision; 2) transparency; intelligibility; and easy access (Pinheiro et al., 2018).

There are 7 main principles related to the processing of personal data that must be followed (GDPR, 2016).

The first one is the principle of lawfulness, fairness and transparency[26], which states that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (GDPR, 2016, Article 5(1)(a)). Any processing of personal data should be lawful and fair and in order to the processing to be lawful, personal data should be processed on a legitimate basis, laid down by law, either in GDPR or in other Union or Member State law[27] (GDPR, 2016).

On the other hand, transparency is an overarching obligation under the GDPR applying to three main domains: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights (Article 29 Data Protection Working Party, 2018d). Moreover, a central consideration of the principle of transparency is that the data subject should be able to determine in advance what is the scope and the consequences of the processing (Article 29 Data Protection Working Party, 2018d; GDPR, 2016). It should be transparent to natural persons that personal data concerning them are processed and to what extent the personal data are or will be processed and data subjects should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing[28] (GDPR, 2016). Also, the principle of transparency requires that "any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and

[26] See also the Article 12 of GDPR.

[27] See Recitals 39 and 40 of GDPR.

[28] See Recital 39 of GDPR.

plain language be used" (GDPR, 2016, Recital 39). Transparency, in this sense, is related with comprehensibility criteria (Pinheiro et al., 2018).

The principle of purpose limitation states that personal data shall be "collected for specified, explicit and legitimate[29] 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" (GDPR, 2016, Article 5(1)(b)). Accordingly, the specific purposes for which personal data are processed should be explicit, legitimate and determined, ideally before the processing, but at least the time of the collection of the personal data[30] (GDPR, 2016). In order to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation, the purpose of processing must be sufficiently defined. As for the purpose to be explicit, it must be sufficiently unambiguous and clearly expressed: it must determine what kind of processing is and is not included within it, and to allow that compliance with the law can be assessed and data protection safeguards applied. In this sense, purpose specification sets limits on the purposes for which controllers may use the personal data collected, as well as it helps to establish the necessary data protection safeguards (Article 29 Data Protection Working Party, 2013).

On the other hand, in order to the principle of data minimization to be followed, personal data "should be adequate, relevant and limited to what is necessary for the purposes for which they are processed" (GDPR, 2016, Article 5(1)(c)).

The principle of accuracy[31] indicates that personal data shall be 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 (GDPR, 2016, Article 5(1)(d); Recital 39).

The principle of storage limitation indicates that personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms

[29] See Article 6 of GDPR.

[30] See Recital 39 of GDPR.

[31] See also Articles 16 and 17 of the GDPR.

of the data subject" (GDPR, 2016, Article 5(1)(e)). This requires ensuring that the period for which the personal data are stored is limited to a strict minimum and in order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review[32] (GDPR, 2016).

The principle of integrity and confidentiality[33] states that personal data shall be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures[34] (GDPR, 2016).

Finally, we have the principle of accountability, which indicates that the controller shall be responsible for, and be able to demonstrate compliance with all of the above described principles[35] (GDPR, 2016).

3.2.6. Lawfulness of processing

GDPR clearly indicates that processing shall be lawful only if and to the extent that at least one of the following applies:

> a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of

[32] See Recital 39 of GDPR.

[33] See also the Article 32 of GDPR.

[34] See Article 5(1)(f) and Recital 39 of GDPR.

[35] See Article 5(2) of GDPR.

> the data subject which require protection of personal data, in particular where the data subject is a child (GDPR, 2016, Article 6(1)).

However, there are a few restrictions and other conditions to be considered: 1) point f) shall not apply to processing carried out by public authorities in the performance of their tasks; 2) Member States may maintain or introduce more specific provisions to adapt the application of the rules of the GDPR with regard to processing for compliance with points c) and e) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations; 3) the basis for the processing referred to in point c) and e) shall be laid down by Union law or Member State law to which the controller is subject; and the purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point e) shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR, 2016, Article 6).

Regarding consent, further details will be provided on the next chapter.

As for the contract as a lawful basis, the provision covers situations where processing is necessary for the performance of the contract to which the data subject is a party. The provision must be interpreted strictly and, therefore, it does not cover situations where the processing is unilaterally imposed on the data subject by the controller. Also, this lawful basis covers processing that takes place prior to entering into a contract, provided that steps are taken at the request of the data subject, rather than at the initiative of the controller or any third party (Article 29 Data Protection Working Party, 2014).

Considering the situations where processing is necessary for compliance with a legal obligation to which the controller is subject, the obligation must be imposed by law and the law must fulfil all relevant conditions to make the obligation valid and binding, and must also comply with data protection law (Article 29 Data Protection Working Party, 2014). This does not necessarily require a legislative act adopted by a parliament, but such a legal basis or legislative measures should be clear and precise and its application should be foreseeable to persons subject to it[36] (GDPR, 2016). Moreover, the controller must not have a choice whether or not to fulfil the legal obligation and the legal obligation itself must be sufficiently clear as to the processing of personal data it requires (Article 29 Data Protection Working Party, 2014).

GDPR does not require a specific law for each individual processing, as law could be a basis for several processing operations based on a legal obligation to which the controller is subject, determining the

[36] See Recital 41 of GDPR.

purpose of processing. Moreover, that law could specify the general conditions of GDPR governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing[37] (GDPR, 2016).

Vital interest appears to limit the application of this ground to questions of life and death, or at the very least, threats that pose a risk of injury or other damage to the health of the data subject (Article 29 Data Protection Working Party, 2014). Therefore, processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis[38] (GDPR, 2016).

Where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, the processing should have a basis in Union or Member State law. Once again, GDPR does not require a specific law for each individual processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so[39] (GDPR, 2016). This lawful basis covers two situations and is relevant both to the public and the private sector: 1) it covers situations where the controller itself has an official authority or a public interest task and the processing is needed for exercising that authority or performing that task; 2) it covers situations where the controller is not an official authority, but is requested by a third party having such authority to disclose data or where the controller proactively discloses data to a third party having such an official authority (Article 29 Data Protection Working Party, 2014).

Processing may also be necessary for the purposes of the legitimate interests pursued by the controller or by a third party. This lawful basis does not apply when such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child[40] (GDPR, 2016). This lawful basis requires a balancing test:

[37] See Recital 45 of GDPR.

[38] See Recital 46 of GDPR.

[39] See Recital 45 of GDPR.

[40] See Recital 47 of GDPR.

the legitimate interests of the controller[41] (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject (Article 29 Data Protection Working Party, 2014).

3.2.7. Consent

Under GDPR, the conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, since the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent (EUGDPR.org, n.d.; GDPR, 2016).

As previously referred, according to Article 4(11), consent of the data subject means “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (GDPR, 2016).

The element “free” implies a real choice and control for data subjects: if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment[42] (Article 29 Data Protection Working Party, 2018b; GDPR, 2016). The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR[43]: consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent or there is an inability to exercise free will (Article 29 Data Protection Working Party, 2018b; GDPR, 2016).

Moreover, as stated on Article 7(4), “When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract” (GDPR, 2016). To assess whether such a situation of bundling occurs, it is important to

[41] An interest is the broader stake that a controller may have in the processing, or the benefit that the controller derives - or that society might derive - from the processing. Also, in order to be legit, it must: be lawful; be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject; and represent a real and present interest (Article 29 Data Protection Working Party, 2014)

[42] See Recital 42 of GDPR.

[43] See Recital 43 of GDPR.

determine what the scope of the contract is and what data would be necessary for the performance of that contract (Article 29 Data Protection Working Party, 2018b).

Also, consent is presumed not to be freely given if it does not allow separate consent to be given to different purposes[44] (GDPR, 2016). A service may involve multiple processing operations for more than one purpose: in such cases, the data subjects should be free to choose which purpose they accept or not (Article 29 Data Protection Working Party, 2018b).

Moreover, it shall be as easy to withdraw as to give consent and the data subject shall have the right to withdraw his or her consent at any time[45] (GDPR, 2016).

Consent should be given "by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement" (GDPR, 2016 Recital 32). A declaration of consent preformulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms[46] (EUGDPR.org, n.d.; GDPR, 2016). Moreover, silence, pre-ticked boxes or inactivity do not constitute consent[47] (GDPR, 2016). Therefore, the controller must apply: 1) purpose specification; 2) granularity in consent requests; and 3) clear separation of information related to obtaining consent for data processing activities from information about other matters (Article 29 Data Protection Working Party, 2018b).

For consent to be informed, at least the following information is required: 1) the controller's identity; 2) the purpose of each of the processing operations for which consent is sought; 3) what (type of) data will be collected and used; 4) the existence of the right to withdraw consent; 5) information about the use of the data for automated decision-making in accordance with Article 22(2)(c) where relevant; and 6) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46 of GDPR (Article 29 Data Protection Working Party, 2018b; GDPR, 2016).

Also, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data, where processing is based on consent[48] (GDPR, 2016).

[44] See Recital 43 of GDPR.

[45] See Article 7(3) of GDPR.

[46] See Recital 42 of GDPR.

[47] See Recital 32 of GDPR.

[48] See Article 7(1) and Recital 42 of GDPR.

Special conditions are applicable to child's consent in relation to information society services, as described in GDPR's Article 8. Children "merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data" (GDPR, 2016, Recital 38).

In relation to the offer of information society services directly to a child[49], the processing of the personal data of a child shall be lawful, considering consent, where the child is at least 16 years old. Where the child is below the age of 16 years, it should be considered if the related Member State provide by law for a lower age for those purposes (provided that such lower age is not below 13 years) or if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Moreover, the controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology[50] (GDPR, 2016).

3.2.8. Special categories of personal data and personal data relating to criminal convictions and offences

The GDPR offers particular protection considering certain types of data[51]. In this sense, processing "of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited" (GDPR, 2016, Article 9). However, exceptions to this rule are considered and clearly defined on GDPR's Article 9(2), (3) and (4). It is not under the scope of the present dissertation to explore this prohibition and related exceptions. Also, the "processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority" (GDPR, 2016, Article 10).

[49] If an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence, then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply. (Article 29 Data Protection Working Party, 2018b)

[50] See Article 8 of GDPR.

[51] It is not under the scope of the present dissertation to explore Articles 9 and 10 of GDPR.

3.2.9. Data Subject's Rights

The GDPR sets out the rights data subjects have regarding their personal data (ITGP Privacy Team, 2017). Once again, it is important to be aware that the right to the protection of personal data is not an absolute right, and it must be considered in relation to its function in society and be balanced against other fundamental rights, always considering the principle of proportionality[52] (GDPR, 2016).

Nevertheless, it is also stated on the GDPR that an effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects[53] (GDPR, 2016).

As previously referred, GDPR also enhances the necessity of transparency. On its Article 12, with the epigraph "Transparent information, communication and modalities for the exercise of the rights of the data subject", it is stated on the number 1 that "the controller shall take appropriate measures to provide any information (...) relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child" (GDPR, 2016 Article 12(1)). This statement extends the sentiment of the Directive, which only required that such information was in an intelligible form (ITGP Privacy Team, 2017).

Moreover, the data subject has the right to information and access to personal data. This right shall increase fairness and transparency of data processing activities performed on their personal data since it gives the possibility to the data subject to demand more in-depth information on processing (Voigt & Bussche, 2017).

The right to information requires that the data controller proactively informs the data subject about the identity and the contact details of the controller, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing. Is is important to remark that the information provided to the data subject may be different in some elements when the personal data have been obtained from the data subject or when it haven't[54] (GDPR, 2016; Voigt & Bussche, 2017).

The right to access is organized in two steps. First, the data subject has the right to obtain confirmation from the controller as to whether or not its personal data is being processed. If such processing takes place, then the data subject shall have access to its personal data processed and the purposes of processing, the categories of personal data concerned, the recipients to whom the data has been or will be disclosed, the storage period or the criteria to determine that period, the existence of the data subject's

[52] See Recital 4 of GDPR.

[53] See Recital 11 of GDPR.

[54] See Articles 13 and 14 of GDPR.

rights to deletion, rectification, restriction of processing or the right to object, the right to lodge a complaint with the Supervisory Authority, etc. Furthermore, the data subject is also given the right to have a copy of the personal data undergoing processing, free of charge[55] (GDPR, 2016; Voigt & Bussche, 2017). This represents is a dramatic shift to data transparency and empowerment of data subjects (Kuner, 2012).

According to the 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. Also, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement[56] (GDPR, 2016).

The right to erasure is closely related with the right to be forgotten. The Article 17 of GDPR goes beyond the scope of the right to be forgotten referred in the Google Spain decision, as it imposes information obligations on the controller towards other parties that have received the personal data concerned (Voigt & Bussche, 2017). The data subject has the right to the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase personal data without undue delay where one of the following grounds applies: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based; the data subject objects to the processing pursuant to profiling or direct marketing purposes; the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; the personal data have been collected based on a child's consent in relation to the offer of information security services[57] (GDPR, 2016). Exceptions to the right of erasure are defined on the Article 17(3) of the GDPR.

In order to strengthen the right to be forgotten in the online environment, the right to erasure should also be extended so the controller who has made the personal data public is obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data[58] (GDPR, 2016).

The GDPR also refers the right to restriction of processing[59], when one of the following circumstances applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the

[55] See Article 15 and Recital 63 of GDPR.

[56] See Article 16 of GDPR.

[57] See Article 17 and Recital 65 of GDPR.

[58] See Recital 66 of GDPR.

[59] Restriction of processing means "the marking of stored personal data with the aim of limiting their processing in the future" (GDPR, 2016, Article 4(3))

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 including profiling pending the verification whether the legitimate grounds of the controller override those of the data subject (GDPR, 2016, Article 18).

Moreover, the controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed (GDPR, 2016, Article 19).

The Article 20 of GDPR refers the right to data portability, which states that the data subject shall have the right to receive the personal data concerning him or her, whenever: personal data that the data subject has provided to a controller are processed based on the data subject's consent or based on their necessity for the performance of a contract between the data subject and the controller; and the processing is carried out by automated means[60] (GDPR, 2016; Voigt & Bussche, 2017). The data subject has the right to transmit that data to another controller or to have the personal data transmitted directly from one controller to another (GDPR, 2016; Kuner, 2012). This new right empowers data subjects regarding their own personal data, as it facilitates their ability to control and transmit personal data easily from one IT environment to another: it represents an opportunity to rebalance the relationship between data subjects and data controllers. While exercising his or her right to data portability he or she does so without prejudice to any other right (Article 29 Data Protection Working Party, 2017d).

The data subject has the right to object to specific types of data processing, including direct marketing, processing based on legitimate interests or in the wider public interest and processing for research or statistical purposes[61]. Nevertheless, only the right to object to direct marketing is absolute (GDPR, 2016; ITGP Privacy Team, 2017) and organizations have the obligation to inform data subjects of their right to object (GDPR, 2016; ITGP Privacy Team, 2017).

The data subject has the right to appropriate decision making (ITGP Privacy Team, 2017). Therefore, he/she shall "have the right not to be subject to a decision based solely on automated processing[62],

[60] See Article 20 of GDPR.

[61] See Article 21 of GDPR.

[62] Automated decision-making is the ability to make decisions by technological means without human involvement. (Article 29 Data Protection Working Party, 2018a)

including profiling[63], which produces legal effects concerning him or her or similarly significantly affects him or her" (GDPR, 2016 Article 22). Individuals must be able to trigger intervention, express their point of view, obtain an explanation for a decision and contest the resulting decision (ITGP Privacy Team, 2017). Finally, the data subject has several rights, considering remedies, liability and penalties.

The data subject has the right to lodge a complaint with a Supervisor Authority against the controller/processor if the data subject considers that the processing of personal data relating to him or her infringes the GDPR[64] (GDPR, 2016). Moreover, without "prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them" (GDPR, 2016 Article 78).

3.2.10. Restrictions

There are some conditions where the data subject rights might be restricted, as well as the communication of a personal data breach to the data subject might be limited (GDPR, 2016). These restrictions might be imposed by law to which the data controller or processor is subject and intend to respect the essence of the fundamental rights and freedoms, being a necessary and proportionate measure in a democratic society to safeguard:

> (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

[63] Profiling means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" (GDPR, 2016, Article 4(4))

[64] See Article 77 of GDPR.

> (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims (GDPR, 2016, Article 23(1)).

3.2.11. The Controller

As defined on Article 4(7), controller

> means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (GDPR, 2016).

This definition contains three main blocks:

1) "the natural or legal person, public authority, agency or any other body;
2) which alone or jointly with others
1) determines the purposes and means of the processing of personal data" (Article 29 Data Protection Working Party, 2010, p. 7),

or, as considered by other authors: the non-personalist element; the determination of the purposes and the means of the processing; the possibility of that determination is individual or jointly with other entities (Pinheiro et al., 2018).

The term "determines" has to be analysed considering the factual circumstances regarding the choice made by an entity to process personal data for its own purposes. The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Moreover, control can derive from:

1) explicit legal competence, when the controller or the specific criteria for his nomination are designated by national or Community law or rather than directly appointing the controller or setting out the criteria for his appointment, the law establishes a task or imposes a duty on someone to collect and process certain data;
2) implicit competence, when the capacity to determine is not explicitly laid down by law, nor the direct consequence of explicit legal provisions, but still stems from common legal provisions or established legal practice pertaining to different areas. In this particular case, the capacity to

determine processing activities can be considered as naturally attached to the functional role of a (private) organization; or

3) from factual influence, when the responsibility as controller is attributed on the basis of an assessment of the factual circumstances. In many cases, this will involve an assessment of the contractual relations between the different parties involved or, in case of doubt, other elements than the terms of a contract may be useful to find the controller, such as the degree of actual control exercised by a party, the image given to data subjects and reasonable expectations of data subjects on the basis of this visibility (Article 29 Data Protection Working Party, 2010; Pinheiro et al., 2018).

Considering "purposes and means", it is also important to point out that the determination of the purpose of processing is reserved to the controller, but the determination of the means of processing can be delegated by the controller, as far as technical or organisational questions are concerned (Article 29 Data Protection Working Party, 2010; Pinheiro et al., 2018). "Purpose" of the processing means the objective of the processing activities, which also means that the controller has the power to control, determine and/or decide on which terms the processing activities must be carried out. On the other hand, the "means" has two main elements: 1) components that have to be defined by the controller, such has the amount of data, processing duration, among others; 2) technical, technological and organizational resources (Pinheiro et al., 2018).

Finally, "natural or legal person, public authority, agency or other body" refers to the personal side, who can be a controller (Article 29 Data Protection Working Party, 2010), and therefore considered ultimately responsible for the obligations referred on the Regulation.

The "controller" concept is not limited to the determination of the purposes of the processing of personal data: it involves all the dynamics inherent to the processing activities (Pinheiro et al., 2018)

The controller has several responsibilities (GDPR, 2016; Pinheiro et al., 2018).

First of all, it shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Those measures shall be reviewed and updated where necessary and where proportionate in relation to processing activities, the measures shall include the implementation of appropriate data protection policies[65] (GDPR, 2016).

[65] See Article 24, Recital 74 and Recital 78 of GDPR.

Second, the responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established and, in this sense, the controller must implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with the GDPR, including the effectiveness of the measures[66] (GDPR, 2016; Pinheiro et al., 2018).

Third, 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 processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects – data protection by design[67] (GDPR, 2016).

Also, 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 - data protection by default. 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. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility[68] (GDPR, 2016).

It is important to keep in mind that when developing, designing, selecting and using applications, services and products that process personal data, producers of the products, services and applications should be encouraged to take into account the right to data protection under all stages, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations[69] (GDPR, 2016).

As part of the principle of accountability, each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility, which shall contain all of the following information:

[66] See Recital 74 of GDPR.

[67] See Article 25 and Recital 78 of GDPR.

[68] See Article 25 and Recital 78 of GDPR.

[69] See Recital 78 of GDPR.

> (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) [of the GDPR], 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) [of the GDPR] (GDPR, 2016, Article 30(1)).

This record shall be in writing, including in electronic form and the controller or the processor shall make the record available to the supervisory authority on request[70] (GDPR, 2016).

However, it is important to refer that the obligation of maintaining this record shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) of the GDPR or personal data relating to criminal convictions and offences referred to in Article 10 of GDPR[71] (GDPR, 2016). Therefore, although endowed with less than 250 employees, data controllers who find themselves in the position of either one of the above described conditions are obliged to maintain the record of processing activities. However, such organisations need only maintain records of processing activities for the types of processing mentioned by Article 30(5) (Article 29 Data Protection Working Party, 2018e).

[70] See Article 30 of GDPR.

[71] See Article 30 of GDPR.

3.2.12. Joint Controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers, which means that they shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject[72] (GDPR, 2016). However, in the context of joint control the participation of the parties to the joint determination may take different forms and does not need to be equally shared (Article 29 Data Protection Working Party, 2010).

3.2.13. The Processor

According with the Article 4(8) of GDPR, processor "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (GDPR, 2016). Two basic conditions for qualifying as processor are: 1) being a separate legal entity with respect to the controller; and 2) processing personal data on his behalf. This processing activity may be limited to a very specific task or context or may be more general and extended (Article 29 Data Protection Working Party, 2010).

The object of the contract/legal obligation that determines the existence of a processor consists on the regulation of the processing of personal data by the processor on the behalf of the controller, which means that procedures and practices designed to ensure personal data protection are required to be determined (Pinheiro et al., 2018).

A clear allocation of the responsibilities under the GDPR, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller by a processor, is required to protect the rights and freedoms of data subjects as well as to determine the responsibility and liability of controllers and processors[73] (GDPR, 2016).

The controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement appropriate technical and organisational measures

[72] See Article 26 of GDPR.

[73] See Recital 79 of GDPR.

which will meet the requirements of the GDPR and ensure the protection of the rights of the data subject, including for the security of processing[74] (GDPR, 2016; Pinheiro et al., 2018).

The processing of personal data by a processor

> should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission (GDPR, 2016 Recital 81).

The contract or the other legal shall be in writing, including in electronic form, and shall stipulate that the processor:

> (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality[75]; (c) takes all measures required pursuant to Article 32 of the GDPR; (d) respects the conditions referred to in paragraphs 2 and 4 of the Article 28 of the GDPR for engaging another processor; (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as

[74] See Article 28 and Recital 81 of GDPR.

[75] This includes obligations of facere and non facere (Pinheiro et al., 2018)

> this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR; (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the processor; (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (GDPR, 2016, Article 28).

Also, the processor shall inform the controller if an instruction infringes the GDPR or other Union or Member State data protection provisions[76] (GDPR, 2016).

Finally, 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) [of GDPR], the documentation of suitable safeguards; (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) [of GDPR] (GDPR, 2016, Article 30).

[76] See Article 28 of GDPR.

This record shall be in writing, including in electronic form, and the controller shall make the record available to the supervisory authority on request[77] (GDPR, 2016).

However, it is important to refer that the obligation of maintaining this record shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) of the GDPR or personal data relating to criminal convictions and offences referred to in Article 10 of GDPR[78] (GDPR, 2016). Therefore, although endowed with less than 250 employees, processors who are under one of the above described conditions are obliged to maintain the record of processing activities. However, such organisations need only maintain records of processing activities for the types of processing mentioned by Article 30(5) (Article 29 Data Protection Working Party, 2018e).

If the controller subject to GDPR chooses to use a processor outside the Union and not subject to GDPR, the processor will become indirectly subject to some obligations imposed by the controller subject to the GDPR, by virtue of contractual arrangements under Article 28. Moreover, provisions of Chapter V of the GDPR may apply (European Data Protection Board, 2018b).

3.2.14. Data Protection Officer

The GDPR recognises the DPO as a key player in the new data governance system and lays down conditions for his or her appointment, position and tasks (Article 29 Data Protection Working Party, 2017c).

The controller and the processor shall designate a DPO in any case where:

(a) the processing is carried out by a public authority or body [79], except for courts acting in their judicial capacity; (b) the core activities [80] of the controller or the processor consist of processing

[77] See Article 30 of GDPR.

[78] See Article 30 of GDPR.

[79] The GDPR does not define what constitutes a "public authority or body" and the WP29 considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law (Article 29 Data Protection Working Party, 2017c).

[80] "Core activities" are the key operations necessary to achieve the controller's or processor's goals (Article 29 Data Protection Working Party, 2017c).

> operations which, by virtue of their nature, their scope and/or their purposes, require regular[81] and systematic[82] 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 (GDPR, 2016, Article 37(1)).

In addition to facilitating compliance through the implementation of accountability tools, DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation) (Article 29 Data Protection Working Party, 2017c). It is important to point out that when an organisation designates a DPO on a voluntary basis, the same requirements will apply to his or her designation, position and tasks as if the designation had been mandatory (Article 29 Data Protection Working Party, 2017c).

The same DPO may be designated for several organizations, in accordance with Article 37(2), (3), (4) of GDPR.

The DPO shall be designated "on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks described on the Article 39 of GDPR" (GDPR, 2016, Article 37(5)). Moreover, the DPO "may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract" (GDPR, 2016, Article 37(6)) and "shall be bound by secrecy or confidentiality concerning the performance of his or her tasks..." (GDPR, 2016, Article 38). Nevertheless, the DPO may fulfil other tasks and duties, but the controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests[83] (GDPR, 2016).

Also, the controller or the processor "shall publish the contact details of the data protection officer and communicate them to the supervisory authority" (GDPR, 2016, Article 37(7)).

The controller and the processor shall ensure that the DPO is properly involved, and in a timely manner, in all issues which relate to the protection of personal data and, in order to do so, the controller and processor shall support the DPO in performing its tasks by providing resources necessary to carry out

[81] The WP29 interprets 'regular' as meaning one or more of the following: 1) ongoing or occurring at particular intervals for a particular period; 2) recurring or repeated at fixed times; 3) constantly or periodically taking place. (Article 29 Data Protection Working Party, 2017c)

[82] The WP29 interprets 'systematic' as meaning one or more of the following: 1) occurring according to a system; 2) pre-arranged, organised or methodical; 3) taking place as part of a general plan for data collection; 4) carried out as part of a strategy (Article 29 Data Protection Working Party, 2017c)

[83] See Article 38 of GDPR.

those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge[84] (GDPR, 2016). However, the DPO shall maintain its independence, and the controller and processor must ensure that the DPO does not receive any instructions regarding the exercise of its tasks and he or she cannot be dismissed or penalised by the controller or the processor for performing his tasks [85] (GDPR, 2016). Besides, the DPO shall "directly report to the highest management level of the controller or the processor" (GDPR, 2016, Article 38).

On the other hand, data subjects may contact the DPO with regard to all issues related to processing of their personal data and in order to the exercise of their rights under the GDPR[86] (GDPR, 2016).

So, the DPO 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 [GDPR] and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation [GDPR], 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" (GDPR, 2016, Article 39(1)).

Furthermore, the DPO has to consider the risk associated with processing operations, regarding the nature, scope, context and purposes of processing[87] (GDPR, 2016).

DPOs are not personally responsible in case of non-compliance with the GDPR: it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in

[84] See Article 38 of GDPR.

[85] See Article 38 of GDPR.

[86] See Article 38 of GDPR.

[87] See Article 39 of GDPR.

accordance with its provisions. Therefore, data protection compliance is a responsibility of the controller or the processor (Article 29 Data Protection Working Party, 2017c).

3.2.15. Security of processing

In order to maintain security and to prevent processing in infringement of the GDPR, and 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 inherent in the processing[88] (GDPR, 2016). ENISA already provided some guidance on this particular matter (ENISA, 2017a, 2018c). Moreover, it is also useful to consider the ISO 27001 (Pinheiro et al., 2018)

In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage [89] (GDPR, 2016).

The measures shall include, inter alia as appropriate:

> a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 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; d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (GDPR, 2016, Article 32).

The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. Also, the controller may choose between several specific pseudonymisation techniques (ENISA, 2018a). However, the use pseudonymisation is not intended to exclude any other measures of data protection[90] (GDPR, 2016). When

[88] See Article 32 and Recital 83 of GDPR.

[89] See Article 32 and Recital 83 of GDPR.

[90] See Recital 28 of GDPR.

processing personal data, measures of pseudonymisation should be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that GDPR is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately[91] (GDPR, 2016). "The controller processing the personal data should indicate the authorised persons within the same controller" (GDPR, 2016, Recital 29).

Moreover, the controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law[92] (GDPR, 2016).

3.2.16. Personal data breach

According to Article 4(12) of GDPR, personal data breach means a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (GDPR, 2016).

Therefore, a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of personal data. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in GDPR (Article 29 Data Protection Working Party, 2018c).

Breaches can be categorised according to the following information security principles: 1) "confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data; 2) "integrity breach" - where there is an unauthorised or accidental alteration of personal data; 3) "availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data. Depending on the circumstances, a breach can affect one or more of the security principles concerning personal data at the same time (Article 29 Data Protection Working Party, 2018c).

Depending on the circumstances of the breach, it may or may not require notification to the supervisory authority and communication to affected individuals. To assess that need, the controller will need to evaluate the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the lack of availability of personal data (Article 29 Data Protection Working Party, 2018c).

[91] See Recital 29 of GDPR.

[92] See Articles 29 and 32 of GDPR.

A personal data breach "may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons" (GDPR, 2016, Recital 85). Therefore, in setting the *modus operandi* applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures. Moreover, such rules and procedures should consider the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach[93] (GDPR, 2016).

Whilst it is the responsibility of controllers and processors to adopt suitable measures to be able to prevent, react and address a breach, there are some measures that should be taken in all cases: 1) information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk; 2) risk to individuals as a result of a breach should then be assessed, with relevant sections of the organisation being informed; 3) notification to the supervisory authority, and communication of the breach to the affected individuals should be made, when applicable; 4) the controller should act to contain and recover the breach; 5) document the breach as it develops (Article 29 Data Protection Working Party, 2018c).

It should be determined whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject[94] (GDPR, 2016). The nature and gravity of the personal data breach and its consequences and adverse effects for the data subject should be considered when the notification is made without undue delay[95] (GDPR, 2016).

As soon as the controller is aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where possible, not later than 72 hours after having become aware[96] of it, unless the controller is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, in

[93] See Recital 88 of GDPR.

[94] See Recital 87 of GDPR.

[95] See Recital 87 of GDPR.

[96] A "controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised" (Article 29 Data Protection Working Party, 2018c, pp. 10–11)

Also, after first being informed of a potential breach, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". (Article 29 Data Protection Working Party, 2018c) accordance with the accountability principle[97] (GDPR, 2016). Where such notification cannot be made within 72 hours, the reasons for the delay should accompany the notification and further information may be provided in phases without undue delay [98] (GDPR, 2016).

On its turn, the processor after becoming aware of a personal data breach shall notify the controller without undue delay[99] (GDPR, 2016). It should be noted that the processor is not responsible to evaluate the likelihood of risk arising from a breach before notifying the controller; it is the responsibility of the controller to do this assessment on becoming aware of the breach. Therefore, the controller should be considered as "aware" once the processor has informed it of the breach, which allows it to address the breach and to determine whether or not it is required to notify the supervisory authority and the affected individuals (Article 29 Data Protection Working Party, 2018c).

The notification of the personal data breach to the supervisory shall at least:

> (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects (GDPR, 2016, Article 33(3)).

Furthermore, the controller has to document all personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken, which shall enable the supervisory authority to verify compliance with GDPR[100] (GDPR, 2016).

In certain cases, besides notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals (Article 29 Data Protection Working Party, 2018c): "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" (GDPR, 2016, Article 34(1)). This communication shall describe in clear and plain language the

[97] See Recital 85 and Article 33 of GDPR.

[98] See Recital 85 and Article 33 of GDPR.

[99] See Article 33 of GDPR.

[100] See Article 33 of GDPR.

nature of the personal data breach and contain at least:1) the name and contact details of the data protection officer or other contact point where more information can be obtained; 2) the likely consequences of the personal data breach; 3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects[101] (GDPR, 2016).

Also, such communications to data subjects should be made as soon as possible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities[102] (GDPR, 2016).

However, GDPR provides a few exceptions where the controller does not need to communicate a breach to the affected individuals:

> (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; [or] (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (GDPR, 2016, Article 34(3)).

3.2.17. Data Protection Impact Assessment

A DPIA describes the processing of personal data, assess its necessity and proportionality and helps to manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data. In fact, a DPIA is designed to assess the risks and determine the measures to address them (Article 29 Data Protection Working Party, 2017b).

> 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

[101] See Article 34 of GDPR.

[102] See Recital 86 of GDPR.

> 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 (GDPR, 2016, Article 35(1)).

The controller should be responsible for the carrying-out of a DPIA to evaluate the origin, nature, particularity and severity of that risk, where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, in order to enhance compliance with the GDPR. The outcome of the assessment should be considered when determining the appropriate measures to be applied in order to demonstrate that the processing of personal data complies with the GDPR[103] (GDPR, 2016). When needed, the controller shall review if processing is performed in accordance with the DPIA, at least when there is a change of the risk represented by processing operations[104] (GDPR, 2016).

Where a DPIA indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures a consultation of the supervisory authority should take place prior to the processing[105] (GDPR, 2016).

A DPIA shall contain at least:

> (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation [GDPR] taking into account the rights and legitimate interests of data subjects and other persons concerned" (GDPR, 2016, Article 35(7)).

[103] See Recital 84 of GDPR.

[104] See Article 35 of GDPR.

[105] See Article 36 and Recital 84 of GDPR.

Furthermore, compliance with approved codes of conduct by the relevant controllers or processors shall be considered in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a DPIA[106] (GDPR, 2016).

When carrying out a DPIA, the controller shall seek the advice of the DPO, where designated and it also shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations, where appropriate[107] (GDPR, 2016).

DPIAs shall in particular be required in the case of:

> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1) [of GDPR], or of personal data relating to criminal convictions and offences referred to in Article 10 [of GDPR]; or (c) a systematic monitoring of a publicly accessible area on a large scale (GDPR, 2016, Article 35(3)).

Moreover, the supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a DPIA and it may establish another for those where no data protection impact assessment is required [108] (GDPR, 2016).

But on which other circumstances a processing operation is "likely to result in a high risk"? In order to answer to this question, the Article 29 Data Protection Working Party considers 9 criteria that the controller must be aware of: 1) evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" (GDPR, 2016, Recitals 71 and 91); 2) automated-decision making with legal or similar significant effect - processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly

[106] See Article 35 of GDPR.

[107] See Article 35 of GDPR.

[108] See Article 35 of GDPR.

significantly affects the natural person" (GDPR, 2016, Article 35(3)(a)); 3) systematic monitoring [109] - processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area" (GDPR, 2016, Article 35(3)(c)); 4) sensitive data or data of a highly personal nature[110], which includes special categories of personal data as defined in Article 9 of GDPR, as well as personal data as defined in Article 10 of GDPR, and beyond these provisions, since other categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals, being considered as sensitive because they are linked to household and private activities (such as electronic communications), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation involves serious impacts in the data subject's daily life; 5) data processed on a large scale [111]; 6) matching or combining datasets; 7) data concerning vulnerable data subjects [112] - the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights; 8) innovative use or applying new technological or organisational solutions, because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms; 9) when the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (GDPR, 2016, Article 22 and Recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract (Article 29 Data Protection Working Party, 2017b). In general, the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which

[109] "This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s)." (Article 29 Data Protection Working Party, 2017b, Chapter 9)

[110] In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes (Article 29 Data Protection Working Party, 2017b, Chapter 10)

[111] Even though the GDPR does not define what constitutes large-scale, the recital 91 provides some guidance. Nevertheless, the WP29 recommends that the following factor be considered when determining whether the processing is carried out on a large scale: a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b. the volume of data and/or the range of different data items being processed; c. the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity (Article 29 Data Protection Working Party, 2017b, Chapter 10)

[112] "Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees , more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified." (Article 29 Data Protection Working Party, 2017b, Chapter 10)

the controller intends to adopt. Contrarywise, a processing operation may correspond to the above-mentioned cases and still be considered by the controller not to be "likely to result in a high risk". In such cases the controller should justify and document the reasons for not carrying out a DPIA (in accordance with the accountability principle) and include/record the recommendations/guidance of the DPO (Article 29 Data Protection Working Party, 2017b).

A DPIA can also be useful for assessing the data protection impact of a technology product, where this is likely to be used by different data controllers to carry out different processing operations, being the controller informed of this necessity by the product provider (Article 29 Data Protection Working Party, 2017a).

DPIAs are important tools for accountability, as they help controllers to comply with requirements of the GDPR and to demonstrate that appropriate measures have been taken to ensure compliance with the GDPR (Article 29 Data Protection Working Party, 2017a).

3.2.18. Codes of Conduct and Certifications

Approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a DPO can be used as guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment and the identification of best practices to mitigate the risk[113] (GDPR, 2016).

The Article 40 of GDPR, with the epigraph "Codes of conduct", promotes the drawing up of codes of conduct to contribute to the proper application of the GDPR, since these instruments should take into account the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises (GDPR, 2016).

Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of GDPR, such as with regard to:

> (a) fair and transparent processing; (b) the legitimate interests pursued by controllers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to data subjects; (f) the exercise of the rights of data

[113] See Recital 77, Recital 81, Article 28 and Article 32 of GDPR.

> subjects; (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; (h) the measures and procedures referred to in Articles 24 and 25 [of GDPR] and the measures to ensure security of processing referred to in Article 32 [of GDPR]; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; (j) the transfer of personal data to third countries or international organisations; or (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79 [of GDPR] (GDPR, 2016, Article 40(2)).

Certification has as purpose to demonstrate compliance with GDPR of processing operations by controllers and processors. In fact, to enhance transparency and compliance with GDPR, the establishment of certification mechanisms and data protection seals and marks is encouraged, allowing data subjects to quickly assess the level of data protection of products and services. Nevertheless, a certification does not reduce the responsibility of the controller or the processor for compliance with GDPR[114] (GDPR, 2016). On one hand, a certificate is a statement of conformity; on the other hand, a seal or mark can be used to signify the successful completion of the certification procedure, indicating that the object of certification has been independently assessed in a certification procedure and is compliant with the specified requirements, stated in normative documents such as regulations, standards or technical specifications (European Data Protection Board, 2019a).

GDPR requires the approval of certification criteria of a certification mechanism by: 1) the competent supervisory authority; or 2) in the case of a European Data Protection Seal, certification criteria is approved by the EDPB[115] (GDPR, 2016). When drafting certification criteria the following compliance aspects shall be considered, where applicable:

> the lawfulness of processing pursuant to Article 6; the principles of data processing pursuant to Article 5; the data subjects’ rights pursuant to Articles 12-23; the obligation to notify data breaches

[114] See Article 42 and Recital 100 of GDPR.

[115] See Articles 42(5), 43(2)(b) and 70(1)(o) of GDPR.

> pursuant to Article 33; the obligation of data protection by design and by default, pursuant to Article 25; whether a data protection impact assessment, pursuant to Article 35(7)(d) has been conducted, if applicable; and the technical and organisational measures put in place pursuant to Article 32 (European Data Protection Board, 2019a, p. 15).

Furthermore, certification criteria should:

> be uniform and verifiable; auditable in order to facilitate the evaluation of processing operations under the GDPR, by specifying in particular, the objectives and the implementing guidance for achieving those objectives; be relevant with respect to the targeted audience (e.g. B2B and business to customer (B2C); take into account and where appropriate be inter-operable with other standards (such as ISO standards, national level standards); and be flexible and scalable for application to different types and sizes of organisations including micro, small and medium sized enterprises in accordance with Article 42(1) and the risk-based approach in accordance with Recital 77 (European Data Protection Board, 2019a, p. 20).

The certification procedure, as part of the certification mechanism, includes the requirements of how, by whom, to what extent and the granularity of the assessment which shall take place in individual certification projects concerning a specific object or ToE (European Data Protection Board, 2019a).

When assessing a processing operation, the following components must be considered, where applicable: personal data; technical systems, used to process the personal data; and processes and procedures related to the processing operation(s) (European Data Protection Board, 2019a).

Each component used in processing operations must be subject to assessment and at least four different significant factors can be of influence: 1) the organisation and legal structure of the controller or processor; 2) the department, environment and people involved in the processing operation(s); 3) the technical description of the elements to be assessed; and finally 4) the IT infrastructure supporting the processing operation including operating systems, virtual systems, databases, authentication and authorization systems, routers and firewalls, storage systems, communication infrastructure or Internet access and associated technical measures (European Data Protection Board, 2019a).

Finally, the certification shall be voluntary and available through a transparent process (GDPR, 2016).

Considering cloud services, the main code of conduct published is the voluntary EU Data Protection Code of Conduct for Cloud Service Providers, or in its short version EU Cloud Code of Conduct, that has as a purpose to demonstrate guarantees regarding appropriate technical and organisational measures and make it easier and more transparent for customers to analyse whether cloud services are appropriate for their use case (EU Cloud CoC, 2019). This Code consists of a set of requirements for CSPs and, therefore, is only applicable to B2B cloud services, where the CSP is acting as a processor (EU Cloud CoC, 2019).

3.2.19. Transfers of personal data to third countries or international organisations

There are specific conditions that must be complied with, in order to transfer personal data to third countries or international organizations[116]. Those can be made on the basis of an adequacy decision or subject to appropriate safeguards[117] (GDPR, 2016). The EDPB also provided guidelines for these derogations (European Data Protection Board, 2018a).

3.2.20. Binding corporate rules

There should be approved and applied binding corporate rules[118] for a group of undertakings, or a group of enterprises engaged in a joint economic activity, for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data[119] (GDPR, 2016).
The necessary conditions to approve binding corporate rules are described on Article 47 (GDPR, 2016).

3.2.21. Supervisor Authority

Each Member State shall have one or more independent public authorities (supervisor authority), which are responsible for monitoring the application of GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union. Each supervisory authority shall act with complete independence in performing its tasks and

[116] This particular element of GDPR will be out of the scope of the present study.

[117] See Articles 44, 45 and 46 of GDPR.

[118] This particular element of GDPR will be out of the scope of the present study.

[119] See Recital 110 of GDPR.

exercising its powers in accordance with GDPR and it shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with GDPR on the territory of its own Member State[120] (GDPR, 2016).

Each supervisory authority shall contribute to the consistent application of GDPR throughout the Union and in order to do so, the supervisory authorities shall cooperate with each other and the Commission[121] (GDPR, 2016).

Each supervisory authority shall on its territory to comply with its tasks as described on Article 57(1) of GDPR. Moreover, each supervisor authority also has got investigative powers, corrective powers and authorisation and advisory powers, as described on Article 58.

3.2.22. Penalties

Infringements of GDPR provisions can be subject to administrative fines up to 20 Million EUR or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher[122] (GDPR, 2016).

It is important to note that these rules apply to both controllers and processors, meaning “clouds” will not be exempt from GDPR enforcement (EUGDPR.org, n.d.).

3.3. **Critical aspects**

Regulators need to start looking for new boundary-marking concepts, i.e., concepts that manage to capture the core of privacy intrusions in the 21st century: concepts that reflect what can be intrusive to people’s private life in a world of massive technology. Moreover, it is important to think of privacy in nonspatial and non-physical terms, without reducing privacy to mere informational privacy, since private life is more than the protection of personal data, even in a century in which virtually everything is captured in data (Koops, 2014).

Even if GDPR strengthens EU’s data protection to meet the new privacy challenges brought by the development of digital technologies (Li, Yu, & He, 2019), compliance with the GDPR will be determined in part by rapidly advancing security technology capabilities and evolving and adoption of best practices (Wilson, 2018).

[120] See Articles 51, 52 and 55 of GDPR.

[121] See Article 81 of GDPR.

[122] See Article 83(5) of GDPR.

Emerging technologies such as cloud computing are effective means of boosting performance and productivity, promoting the economy and becoming one of the strongest competitive factors among countries. However, stricter regulations on data handing and processing are likely to inhibit this development and they will inevitably increase the cost to develop new technologies (Wilson, 2018). GDPR compliance will be hard to achieve, and for cloud services this will be especially problematic and challenging (Duncan & Zhao, 2018).

Nevertheless, for the first time, the European lawmaker has officially endorsed and organized a full certification and accreditation process under the GDPR, which contributes to building a regulation continuum with the advent of ICT (Lachaud, 2018).

3.4. GDPR and the Data Protection Portuguese Law

3.4.1. Portuguese legal context

Privacy is culture-dependent and may be interpreted differently in various jurisdictions (Zhao, 2014).

In Portugal, the CPR was one of the first Constitutions in the world, and the first European Constitution, to consider personal data protection, enhancing fundamental rights in relation with the use of new technologies (Castro, 2005, 2016; Vasconcelos, 2012). Nevertheless, as stated before, it was subject to several alterations, considering data protection and the related Article 35 (Castro, 2016; Marques & Martins, 2000).

The Article 26 indicates that

> Everyone is accorded the rights to personal identity, to the development of personality, to civil capacity, to citizenship, to a good name and reputation, to their image, to speak out, to protect the privacy of their personal and family life, and to legal protection against any form of discrimination. The law shall lay down effective guarantees against the improper procurement and misuse of information concerning persons and families and its procurement or use contrary to human dignity (Constitution of the Portuguese Republic, 2005),

being privacy and personal life protected.

The Article 34 "Inviolability of home and correspondence" states that

> Domiciles and the secrecy of correspondence and other means of private communication are inviolable (...). The public authorities are prohibited from interfering in any way with correspondence, telecommunications or other means of communication, save in the cases in which the law so provides in matters related to criminal procedure (Constitution of the Portuguese Republic, 2005),

and the right to prohibit the processing of data relating to privacy informatically, reflected on the Article 35

> Every citizen has the right of access to all computerised data that concern him, which he may require to be corrected and updated, and the right to be informed of the purpose for which they are intended, as laid down by law. The law shall define the concept of personal data, together with the terms and conditions applicable to its automatized treatment and its linkage, transmission and use, and shall guarantee its protection, particularly by means of an independent administrative entity. Information technology may not be used to treat data concerning philosophical or political convictions, party or trade union affiliations, religious faith, private life or ethnic origins, save with the express consent of the data subject, or with an authorisation provided for by law and with guarantees of non-discrimination, or to processing statistical data that are not individually identifiable. Third-party access to personal data is prohibited, save in exceptional cases provided for by law. The allocation of a single national number to any citizen is prohibited. Everyone is guaranteed free access to public-use information technology networks. The law shall define the regime governing cross-border data flows, and the appropriate means for protecting both personal data and other data whose safeguarding is justified in the national interest. Personal data contained in manual files enjoy the same protection as that provided for in the previous paragraphs, as laid down by law. (Constitution of the Portuguese Republic, 2005).

Therefore, Article 35 of the CPR provides for several rights, namely: the right of access to computerized data concerning the data subject; right of rectification; the right to know the purpose for which they are intended to be used for.

This constitutional provision that protects the rights against the use of information technology has as its focus personal data and, consequently, it has implications in the rights and guarantees for the data subjects. On the other hand, it creates obligations and conditions for those who collect them, process them, transmit them, transfer them, conserve them, always considering the quality and security of information [c]

According to Gomes Canotilho & Vital Moreira the "personal data" statement expresses the close connection between these rights and their computer processing and the more data is related to the dignity, personality and self-determination of people, the more restrictions are imposed on their use and collection (Moreira & Canotilho, 2007).

Regarding security, the CPR on Article 27 points out that "Everyone has the right to freedom and security." (Constitution of the Portuguese Republic, 2005).

On its Article 18, the CPR states that

> The constitutional precepts with regard to rights, freedoms and guarantees are directly applicable and are binding on public and private entities. The law may only restrict rights, freedoms and guarantees in cases expressly provided for in the Constitution, and such restrictions must be limited to those needed to safeguard other constitutionally protected rights and interests. Laws that restrict rights, freedoms and guarantees must have a general and abstract nature and may not have a retroactive effect or reduce the extent or scope of the essential content of the constitutional precepts. (Constitution of the Portuguese Republic, 2005).

In accordance with the Directive 95/46/EC, there was a transposition into to the Portuguese context by the Law 67/98[123], concerning the protection of individuals with regard to the processing of personal data and free movement of such data (Assembleia da República, 1998). Its aim was to ensure that "the processing of personal data must be carried out in a transparent manner and in strict respect for the protection of privacy, as well as fundamental rights, freedoms and guarantees" (Assembleia da República, 1998, Article 2).

[123] Not in force anymore, since it was replaced by the Law 58/2019, ensuring the national implementation of GDPR.

In addition to judicial protection, there is an independent administrative entity - the Portuguese Data Protection Authority, CNPD, devoted to the control and enforcement of legal and regulatory provisions relating to personal data, in strict compliance with the rights and the freedoms and guarantees (Assembleia da República, 1998).

The Article 192 of the Portuguese Criminal Law (CP, under the Decree-Law 48/95 – Decreto-Lei n.º 48/95, de 15 de março, in the original), on the Deprivation of Private Life section, establishes that

> 1- Who, without consent and with intent to devastate the private life of persons, namely the intimacy of family or sexual life: a) Intercept, record, use, transmit or disseminate conversation, telephone communication, e-mail or detailed billing; b) Capture, photograph, film, record or disseminate the image of people or objects or intimate spaces; c) Observe or listen to the hidden persons who are in a private place; or (d) to disclose facts relating to the private life or serious illness of another person; shall be punished with imprisonment for up to one year or with a fine of up to 240 days.
>
> 2- The fact foreseen in letter d) of the previous number is not punishable when it is practiced like means suitable to realize a legitimate and relevant public interest. (Decreto-Lei n.◦ 48/95, de 15 de março, 1995).

In this legal precept, the protected legal good is without any doubt the privacy/ protection of the individual's private life. Legal repression thus encompasses the word, image and reservation of the intimacy of private and family life, recognized by the Article 26 of the CPR (Constitution of the Portuguese Republic, 2005). Moreover, the Article 193 on the heading "Intrusion via Computer", states that

> The one, who create, maintain or use automated file of individually identifiable data and relating to political, religious or philosophical, the party or trade union membership, private life, or ethnic origin, shall be punished with imprisonment for up to two years or with a fine of up to 240 days.The attempt is punishable (Decreto-Lei n.◦ 48/95, de 15 de março, 1995).

This precept is, notoriously, the fruit of technological evolution, giving birth to a new type of crime: computer crime. The type of illicit of this precept, refers to the creation, maintenance or use by any person, of "automated file of individually identifiable data". It is therefore understood that it shall be prohibited to create, maintain or use an automated data file that is individually identifiable, and which refers to political, religious or philosophical beliefs, party or trade union affiliation, privacy or ethnic origin. As mentioned above, Article 35 of the CPR, in accordance with Article 193 of CP, states that information technology cannot be used to process data concerning philosophical or political beliefs, party or trade union membership, faith religious, private and ethnic origin, except through the express consent of the holder.

As previously referred, GDPR states that "Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation"(GDPR, 2016, Recital 10). Therefore, it is also important to analyse what changes Portugal will face regarding privacy and data protection Law.

3.4.2. Law 58/2019

Following this orientation, on the Portuguese context was approved the law that ensures the national implementation of GDPR - Law 58/2019 (Assembleia da República, 2019). Only the main elements of the referred law will be analysed, considering the purpose of the present dissertation.

Considering its scope, the Law 58/2019 applies to the processing of personal data that takes place on national territory, regardless of the public or private nature of the controller or processor, even if that processing has got as lawful basis a legal obligation or is being done considering the public interest, being applied all the exclusions predicted under the Article 2 of GDPR. Moreover, this law is also applicable when personal data processing is done outside of the national territory when:

a) it is done under the activity of an establishment located on national territory; or b) it affects data subjects who are located on national territory or even when the processing activities are subordinated to the Article 3(2) of GDPR; or c) it affects data that is inscribed on consular posts which belongs to Portuguese data subjects who are residents abroad (Assembleia da República, 2019, Article 2).

As an exclusion clause, this law does not apply to data files constituted and kept under the responsibility of the Portuguese Intelligence System (Assembleia da República, 2019).

The CNPD is the supervisor authority designated[124] (Assembleia da República, 2019), being its nature and independence described on Article 4 and its composition and functioning on Article 5 (Assembleia da República, 2019).

CNPD's tasks and competences are indicated on Article 6, which doesn't go much further than the dispositions of GDPR, with the exception of the cooperation with the Portuguese Institute of

[124] See Article 3 of the Law 58/2019.

Accreditation[125], which is the entity responsible for the accreditation of data protection certification bodies, considering the requirements defined by CNPD and the GDPR's dispositions on this regard[126] (Assembleia da República, 2019).

Considering DPIAs, there is nothing new, keeping in line with the GDPR's provisions[127]. However, it is important to point out that in accordance with a prior consultation to the EDPB[128] (European Data Protection Board, 2018c; GDPR, 2016), the CNPD provided a list of processing operations which are subject to a DPIA (CNPD, 2018).

About the DPO, besides the general disposition which does not go beyond the GDPR[129], there are also defined tasks that must be followed:

> a) ensure that audits, whether periodic or unscheduled, are done; b) make users aware of the importance of early detection of security incidents and the need to inform the security officer immediately; c) ensure relations with data subjects in matters covered by the GDPR and national data protection law (Assembleia da República, 2019, Article 11).

Once again, the legislator didn't go far from the GDPR's provisions.

Nevertheless, Article 12 indicates the requirements concerning DPOs on public authorities and the legislator defined what should be considered a public authority: a) the State; b) the autonomous regions; c) local authorities and supranational entities as defined by law; d) the independent administrative entities and the Portuguese Bank; e) public institutes; f) public higher education institutions, whatever their nature; g) enterprises of the State business sector and of the regional and local business sectors; h) public associations (Assembleia da República, 2019).

Considering private organizations, the controller and the processor must designate a DPO whenever the main processing activity implies:

> a) operations which, due to their nature, scope and or purpose, require a regular and systematic control of data subjects on a large scale; or b) large-scale processing operations of special

[125] See Article 6 of the Law 58/2019.

[126] See Article 14 of the Law 58/2019.

[127] See Article 7 of the Law 58/2019.

[128] See Article 57(1)(k) of GDPR.

[129] See Article 9 of the Law 58/2019.

categories of data as defined on Article 9 or Article 10 of GDPR (Assembleia da República, 2019, Article 13).

Once again, nothing new.

About certification, as previously stated, the competent authority for the accreditation of data protection certification bodies is the IPAC, I.P. The certification, as well as the emissions of seals and marks, is done by certification bodies properly accredited by IPAC, as has got as main purpose to certify that the implemented procedures are compliant with the GDPR and the Portuguese data protection law[130] (Assembleia da República, 2019).

As defined on Article 15, it is the competence of CNPD "to promote the elaboration of codes of conduct which regulate determined activities, considering the specific needs of micro, small and medium enterprises. The processing of personal data by public authorities is object of proper codes of conduct" (Assembleia da República, 2019, Article 15).

The Portuguese law has dedicated a chapter to special dispositions. On that chapter are defined the consent of children, the protection of personal data of deceased people[131], portability and interoperability of data, video surveillance, duty of secrecy, retention period of personal data, data transference, personal data processing by public authorities to different purposes.

Regarding the consent of children, the Portuguese Law indicates that the personal data of children may only be processed having as lawful basis the consent as defined on of Article 6(1)(a) of GDPR when the same children already are 13 years old. If the child has an inferior age, the processing is only licit if it has been given by the legal representatives of the child[132] (Assembleia da República, 2019).

The personal data of deceased people are protected under the GDPR and the Portuguese law terms when they are integrated on the special categories of personal as defined on Article 9 of GDPR or they are related to the intimacy of private life, image or data related with communications, never forgetting the dispositions of the Article 9(2). The data subject rights defined on GDPR related to personal data of deceased people, in particular, the right of access, the right of rectification and right to erasure, are exercised by the person that the deceased has designated for the effect or on its absence by the heirs of

[130] See Article 14 of the Law 58/2019.

[131] This is particular interesting, since the GDPR does not apply to the personal data of deceased people and gives margin of manoeuvre to the Member States to provide for rules regarding this subject (See Recital 27 of GDPR).

[132] See Article 16 of the Law 58/2019.

the deceased person. Moreover, the data subjects may determine that the previously referred rights cannot be exercised after their death[133] (Assembleia da República, 2019).

Regarding portability and data interoperability, the legislator didn't go much further than the Article 20 of GDPR, only stating that the data portability has to take place, whenever possible, on an open format. Besides, when considering the scope of action of public authority, the National Regulation on Digital Interoperability must be followed[134] (Assembleia da República, 2019).

Concerning video surveillance, there is a direct remission to a specific law, Law 34/2013 (Lei n.º 34/2013, de 16 de maio, in the original), requiring that its Article 31 must be followed in case of purposes of protection of people and goods. Also, the Article 19 imposes some limitations. Cameras cannot be focused on:

> a) public roads, neighbouring properties, or other non-exclusive domain locations of the person in charge, except to the extent strictly necessary to cover access to the property; b) the ATM code entry zone or other payment terminal ATM; c) the interior of areas reserved for customers or users where privacy must be respected, namely toilets, waiting areas and dressing rooms; d) the interior of areas reserved for workers, such as dining areas, changing rooms, gymnasiums, toilets and areas exclusively intended to rest (Assembleia da República, 2019, Article 19(2)).

In educational establishments, video surveillance cameras may only focus on the outer perimeters and access areas, as well as over spaces whose goods and equipment require special protection, such as laboratories or computer rooms. Besides, on the cases where video surveillance is allowed, it is forbidden the sound capture, except within the period that the surveilled installations are closed or if a previous authorization from CNPD is provided[135] (Assembleia da República, 2019).

The legislator chose to make a general remission concerning data retention periods: those will be the ones defined by law or on its absence the ones that are necessary to achieve the purpose of the processing activities. In cases where there is a data retention period imposed by law, the right to erasure provided for in Article 17 of the RGPD may only be exercised after that period[136] (Assembleia da República, 2019).

[133] See Article 17 of the Law 58/2019.

[134] See Article 18 of the Law 58/2019.

[135] See Article 19 of the Law 58/2019.

[136] See Article 21 of the Law 58/2019.

For purposes of public interest archive, scientific or historical research purposes or statistical purposes and when by nature and purpose of the processing activities, it is not possible to determining in advance the moment when it is no longer necessary, it is lawful the conservation of personal data, provided that adequate technical and organizational measures are adopted to guarantee the rights of the data subject, including information on the retention of the data subject. Also, when personal data are required by the controller, or processor, to demonstrate compliance with contractual or other obligations, they may be retained until the expiry of the corresponding rights [137] (Assembleia da República, 2019).

Data on contributory statements for retirement purposes may be retained without a time limit and, therefore, it is not defined a retention period. This was determined in order to assist the holder in re-establishing the contributory careers, provided that appropriate technical and organizational measures are adopted to in order to ensure the rights of the data subject [138] (Assembleia da República, 2019).

However, when the purpose that motivated the initial or subsequent processing of personal data ceases, the controller must destroy or anonymize it [139] (Assembleia da República, 2019). The legislator didn't opt for also considering the pseudonymization option.

Finally, Chapter VI of the Portuguese law provides further information about specific situations of personal data processing, the Chapter VII about administrative and jurisdictional supervision and Chapter VIII about final and transitory dispositions[140] (Assembleia da República, 2019).

As a preliminary analysis, it may be considered that the Portuguese legislator adopted a conservative position: in general, it did not provide further guidance concerning the GDPR application and it did not consider some aspects that remain to be solved (i.e. the use of special categories of data by insurance companies, the processing of data concerning to vulnerable data subjects, particularly given the proliferation of public and private partnerships on education, health and social security sector, where responsibilities are not clearly defined and constantly changing).

Considering DPIAs, there is nothing new, keeping in line with the GDPR's provisions.

About the DPO, besides the general disposition, the legislator didn't go far from the GDPR's provisions. Nevertheless, Article 12 indicates the requirements concerning DPOs on public authorities and the legislator defined what should be considered a public authority (Assembleia da República, 2019).

[137] See Article 21 of the Law 58/2019.

[138] See Article 21 of the Law 58/2019.

[139] See Article 21 of the Law 58/2019.

[140] These 3 Chapters will be considered out of scope for the present dissertation.

Considering private organizations, the controller and the processor must designate a DPO whenever the main processing activity implies: a) operations which require a regular and systematic control of data subjects on a large scale; or b) large-scale processing operations of special categories of data as defined on Article 9 or Article 10 of GDPR (Assembleia da República, 2019).

Regarding the consent of children, the Portuguese law indicates that the personal data of children may only be processed having as lawful basis the consent as defined on Article 6(1)(a) of GDPR when the same children already are 13 years old. If the child has an inferior age, the processing is only licit if it has been given by the legal representatives of the child (Assembleia da República, 2019).

The personal data of deceased people are protected under the GDPR and the Portuguese law terms when they are integrated on the special categories of personal as defined on Article 9 of GDPR or they are related to the intimacy of private life, image or data related with communications. The data subject rights defined on GDPR related to personal data of deceased people, in particular, the right of access, the right of rectification and right to erasure, are exercised by the person that the deceased has designated for the effect or on its absence by the heirs of the deceased person. Moreover, the data subjects may determine that the previously referred rights cannot be exercised after their death (Assembleia da República, 2019).

Regarding portability and data interoperability, the legislator didn't go much further than the Article 20 of GDPR, only stating that the data portability has to take place, whenever possible, on an open format. Besides, when considering the scope of action of public authority, the National Regulation on Digital Interoperability must be followed (Assembleia da República, 2019).

Concerning video surveillance, there is a direct remission to a specific law, Law 34/2013, requiring that its Article 31 must be followed in case of purposes of protection of people and goods. Also, the Article 19 imposes some limitations (Assembleia da República, 2019).

The legislator chose to make a general remission concerning data retention periods: those will be the ones defined by law or on its absence the ones that are necessary to achieve the purpose of the processing activities. In cases where there is a data retention period imposed by law, the right to erasure provided for in Article 17 of the RGPD may only be exercised after that period. When the purpose that motivated the initial or subsequent processing of personal data ceases, the controller must destroy or anonymize it. The legislator didn't opt for also considering the pseudonymization option. An exception is made considering data on contributory statements, not defining a retention period, provided that appropriate technical and organizational measures are adopted to in order to ensure the rights of the data (Assembleia da República, 2019).

Nevertheless, the CNPD already opposed to the Article 2(1) and (2), considering that such definition compromises the application of procedural and of distribution of competences between Supervisor Authorities of the Member States (CNPD, 2019).

It is of particular importance to analyse the opposition made to the territorial application.

The definition of the territorial scope of application of the Portuguese data protection law compromises the application of procedural rules and the distribution of jurisdiction of competence between Member States' national Supervisory Authorities where cross-border treatment is applicable. Indeed, having the controller or processor more than one establishment in the Union, Article 56(1) of the RGPD determines which national authority is responsible for directing the procedure and issuing the final decision, with the one-stop-shop mechanism. However, this main supervisor authority must not fail to consider and apply its national law. In this sense, the main supervisor authority is, in general, the authority of the Member State where the main establishment is located: therefore, the application of the Portuguese law to the processing activities on a main establishment located on other Member State territory will be, in principle, incompatible with the Article 56(1) of GDPR. And following the same reasoning, it will also be incompatible the application of the Portuguese law to an establishment, which cannot be considered as the main one, that is located in Portugal (CNPD, 2019).

Moreover, it was also against the Article 20(1), considering that it wasn't fully compliant with the GDPR's dispositions on Articles 13 and 15. Furthermore, the CNPD done some clarifications regarding the Articles 23, 28(3)(a), 37(1)(a), (h) and (k), and (2), 38(1)(b), and (2), 39(1) and (3), 61(2) and 62(2), stating that the CNPD itself will not apply those Articles (CNPD, 2019).

Furthermore, once again the legislation remained technologically neutral. However, it is aligned with the already published Resolution of the Council of Ministers 41/2018 - Resolução do Conselho de Ministros n.º 41/2018, in the original (Conselho de Ministros, 2018), being mandatory that Resolution to be complied with by public authorities and a model to be followed by private organizations/bodies.

4. CLOUD COMPUTING

For this study purposes, they will be considered the ISO/IEC standards related with cloud computing, namely the ISO/IEC 17788, ISO/IEC 17789, ISO/IEC 19941 and ISO/IEC 19944, since the certification process as defined by the European Data Protection Board (2018c) makes reference to the ISO standards, (i.e. for national accreditation bodies, which will need to take into account certification the certification criteria with a view to the accreditation of certification bodies in accordance with EN-ISO/IEC 17065/2012; the ISO 17000:2004, for conformity assessment , using its vocabulary and general principles. However, when needed, other references might be used.

Even though cloud computing is empowered by virtualization technology, that dates back to 1967 (Zissis & Lekkas, 2012), the "cloud" term only appeared 90s, in reference to the capability of dynamic traffic switching to balance utilization and to indicate that the ICT infrastructure is virtualized (Expert Group Report, 2010).

As described on ISO/IEC 17788, cloud computing is

> a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. The cloud computing paradigm is composed of key characteristics, cloud computing roles and activities, cloud capabilities types and cloud service categories, cloud deployment models and cloud computing cross cutting aspects"(ISO/IEC, 2014a, Chapter 6.1).

Therefore, cloud computing can be considered a new paradigm in computing, that allows users to temporarily access the computing services/platforms/infrastructure on the network, provided as a service by the CSP, at possibly one or more levels of abstraction. It is rapidly changing the landscape of ICT and consequently, various business models have evolved to integrate this technology into software applications, programming platforms, data storage, computing infrastructures and hardware as a service (Armbrust et al., 2010; Dukaric & Juric, 2013; Jansen & Grance, 2011; Shawish & Salama, 2014; Talia, 2011; WeDo Technologies, 2011; Youseff, Butrico, & Silva, 2008).

Clouds are of particular commercial interest considering several factors: 1) the growing tendency to outsource IT as to reduce management overhead and to extend existing, limited IT infrastructures; 2) clouds facilitate the entrance for new service providers to offer their respective capabilities to a wide market with a minimum of entry costs and infrastructure requirements; 3) the special capabilities of cloud infrastructures allow providers to experiment with novel service types whilst reducing the risk of wasting resources (Expert Group Report, 2010). Nevertheless, it is important to keep in mind that the security of personal information needs to be ensured - in particular when data are stored “in the cloud” (Reding, 2011).

4.1. **Definition and Main Characteristics**

Cloud computing is a vague technical terminology and it has been coined as an umbrella term to describe a category of sophisticated on-demand computing services (Vaquero, Rodero-Merino, Caceres, & Lindner, 2009; Voorsluys, Broberg, & Buyya, 2011). It can be used in several applications and promoted by several entities corresponding to different technical figures, being based on a mix-up of old and new concepts used in various research fields (Höfer & Karagiannis, 2010; Youseff et al., 2008). In fact, there seems to be some confusion as to what cloud computing exactly is and when it is useful (Armbrust et al., 2010; Jansen & Grance, 2011). In this sense, there is a lack of information and understanding about the classification of cloud systems, their correlation and their interdependence, which limits advances in this field. An ontology in this domain of knowledge would then be required (Youseff et al., 2008) as some authors are already proposing a unified taxonomy (Dukaric & Juric, 2013; Jansen & Grance, 2011).

In this sense, the ISO/IEC 17788 standard provides an overview of cloud computing along with a set of terms and definitions, being considered as a terminology foundation for cloud computing standards (ISO/IEC, 2014a).

4.1.1. Terminology

The following terminology is defined on the ISO/IEC 17788 and ISO/IEC 17789 standards and those are the ones that will be considered for this study purposes:

1) activity: “a specified pursuit or set of tasks” (ISO/IEC, 2014b, Chapter 3.2.1);
2) application capabilities type: “cloud capabilities type in which the CSC can use the CSP’s applications” (ISO/IEC, 2014a, Chapter 3.2.1);
3) architecture: “fundamental concepts or properties of a system in its environment embodied in its elements, relationships and in the principles of its design and evolution” (ISO/IEC, 2014b, Chapter 3.1.1);
4) cloud application portability: “ability to migrate an application from one cloud service to another cloud service” (ISO/IEC, 2014a, Chapter 3.2.2);

5) cloud capabilities type: “classification of the functionality provided by a cloud service to the CSC, based on resources used. The cloud capabilities types are application capabilities type, infrastructure capabilities type and platform capabilities type” (ISO/IEC, 2014a, Chapter 3.2.4);
6) cloud computing: “paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Examples of resources include servers, operating systems, networks, software, applications, and storage equipment” (ISO/IEC, 2014a, Chapter 3.2.5);
7) cloud data portability: “data portability from one cloud service to another cloud service” (ISO/IEC, 2014a, Chapter 3.2.6);
8) cloud deployment model: “way in which cloud computing can be organized based on the control and sharing of physical or virtual resources. The cloud deployment models include community cloud, hybrid cloud, private cloud and public cloud” (ISO/IEC, 2014a, Chapter 3.2.7);
9) cloud service: “one or more capabilities offered via cloud computing invoked using a defined interface” (ISO/IEC, 2014a, Chapter 3.2.8);
10) cloud service category: “group of cloud services that possess some common set of qualities. A cloud service category can include capabilities from one or more cloud capabilities types” (ISO/IEC, 2014a, Chapter 3.2.10);
11) cloud service customer: “party which is in a business relationship for the purpose of using cloud services. A business relationship does not necessarily imply financial agreements” (ISO/IEC, 2014a, Chapter 3.2.11);
12) cloud service customer data: “class of data objects under the control, by legal or other reasons, of the CSC that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the CSC via the published interface of the cloud service” (ISO/IEC, 2014a, Chapter 3.2.12);
13) cloud service derived data:

class of data objects under CSP control that are derived as a result of interaction with the cloud service by CSC. Cloud service derived data includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the cloud service has such configuration and customization capabilities (ISO/IEC, 2014a, Chapter 3.2.13);

14) cloud service partner: “party which is engaged in support of, or auxiliary to, activities of either the CSP or the CSC, or both” (ISO/IEC, 2014a, Chapter 3.2.14);
15) cloud service product: “a cloud service, allied to the set of business terms under which the cloud service is offered. Business terms can include pricing, rating and service levels” (ISO/IEC, 2014b, Chapter 3.2.2).
16) cloud service provider: “party which makes cloud services available” (ISO/IEC, 2014a, Chapter 3.2.15);
17) cloud service user: “natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services” (ISO/IEC, 2014a, Chapter 3.2.17);
18) community cloud: “cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection” (ISO/IEC, 2014a, Chapter 3.2.19);
19) data portability: “ability to easily transfer data from one system to another without being required to re-enter data. It is the ease of moving the data that is the essence here. This might be achieved by the source system supplying the data in exactly the format that is accepted by the target system” (ISO/IEC, 2014a, Chapter 3.2.21);
20) functional component: “a functional building block needed to engage in an activity, backed by an implementation” (ISO/IEC, 2014b, Chapter 3.2.3)
21) hybrid cloud: “cloud deployment model using at least two different cloud deployment models” (ISO/IEC, 2014a, Chapter 3.2.23);
22) Infrastructure as a Service (IaaS): “cloud service category in which the cloud capabilities type provided to the CSC is an infrastructure capabilities type. The CSC does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The CSC may also have limited ability to control certain networking components (e.g., host firewalls)” (ISO/IEC, 2014a, Chapter 3.2.24);
23) infrastructure capabilities type: “cloud capabilities type in which the CSC can provision and use processing, storage or networking resources” (ISO/IEC, 2014a, Chapter 3.2.25);
24) measured service: “metered delivery of cloud services such that usage can be monitored, controlled, reported and billed” (ISO/IEC, 2014a, Chapter 3.2.26);

25) multi-tenancy: “allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another” (ISO/IEC, 2014a, Chapter 3.2.27);

26) on-demand self-service: “feature where a CSC can provision computing capabilities, as needed, automatically or with minimal interaction with the CSP” (ISO/IEC, 2014a, Chapter 3.2.29);

27) Platform as a Service (PaaS): “cloud service category in which the cloud capabilities type provided to the CSC is a platform capabilities type” (ISO/IEC, 2014a, Chapter 3.2.30);

28) platform capabilities type: “cloud capabilities type in which the CSC can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the CSP” (ISO/IEC, 2014a, Chapter 3.2.31);

29) private cloud: “cloud deployment model where cloud services are used exclusively by a single CSC and resources are controlled by that CSC” (ISO/IEC, 2014a, Chapter 3.2.32);

30) public cloud: “cloud deployment model where cloud services are potentially available to any CSC and resources are controlled by the CSP” (ISO/IEC, 2014a, Chapter 3.2.33);

31) resource pooling: “aggregation of a CSP’s physical or virtual resources to serve one or more CSCs” (ISO/IEC, 2014a, Chapter 3.2.34);

32) reversibility: “process for CSCs to retrieve their CSC data and application artefacts and for the CSP to delete all CSC data as well as contractually specified cloud service derived data after an agreed period” (ISO/IEC, 2014a, Chapter 3.2.35);

33) role: “a set of activities that serves a common purpose” (ISO/IEC, 2014b, Chapter 3.2.7);

34) Software as a Service (SaaS): “cloud service category in which the cloud capabilities type provided to the CSC is an application capabilities type” (ISO/IEC, 2014a, Chapter 3.2.36);

35) tenant: “one or more cloud service users sharing access to a set of physical and virtual resources” (ISO/IEC, 2014a, Chapter 3.2.37).

As there is no standardization of cloud computing services, each CSP uses different technologies, protocols and formats, being the clouds themselves quite opaque regarding their internal processes, which hampers interoperability or migration to other services (Höfer & Karagiannis, 2011; Murtaza & Al Masud, 2012). A unified interface that provides integrated access to cloud computing services is therefore non-existent, even though there are portals and gateways that can provide this unified interface to the web-based user (Youseff et al., 2008).

As the relationships between cloud computing services are ambiguous, their applicability in their interoperability is being debated (Expert Group Report, 2010; Moghaddam, Ahmadi, Sarvari, Eslami, & Golkar, 2015; Youseff et al., 2008). Thus, several efforts to develop standards for cloud computing are being made (Grossman, 2008; ISO/IEC, 2017a).

Before proceeding, a distinction between cloud and cloud computing must be made.

Cloud is the term for server-based offerings for data processing (The Cloud Privacy Check (CPC), 2017), being defined as the hardware and the software present in a data centre, which is a scalable structure that supports and connects diverse computational services (Höfer & Karagiannis, 2011; Knorr & Gruman, 2010).

On the other hand, cloud computing is an expansion of utility computing, with virtual servers (Knorr & Gruman, 2010). Thus, cloud computing refers to both the applications provided to Internet services and to the hardware and software systems in the data centres providing the same services, unifying SaaS and utility computing services (Armbrust et al., 2009, 2010). Therefore, cloud computing may be considered a style of computing paradigm in which typically real-time scalable resources can be accessible from a web browser via the Internet to users (Shawish & Salama, 2014).

In a cloud computing environment, the traditional role of the service provider is divided in two elements: infrastructure providers, who manage cloud platforms and allocate resources according to a usage-based cost model; and CSPs, who lease resources from one or more infrastructures to serve end-users (Höfer & Karagiannis, 2010; Zhang, Cheng, & Boutaba, 2010). The CSPs make services accessible to users through Internet-based interfaces (Höfer & Karagiannis, 2011; Shawish & Salama, 2014; Vaquero et al., 2009).

4.1.2. Main characteristics

The ISO/IEC 17788[141] indicates that cloud computing is constituted by the following main characteristics:

1) Broad network access: a feature where the physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms. Thus, cloud computing offers an increased level of convenience in that users can access physical and virtual resources from wherever they need to work, as long as it is network accessible;

[141] See Chapter 6.2 of the standard.

2) Measured service: a feature where the metered delivery of cloud services is such that usage can be monitored and billed in accordance, which is important to optimize and validate the delivered cloud service. The CSCs only pays for the resources that they use;
3) Multi-tenancy: a feature where physical or virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from and inaccessible to one another. Typically, and within the context of multi-tenancy, the group of cloud service users that form a tenant will all belong to the same CSC organization. There might be cases where the group of cloud service users involves users from multiple different CSCs, particularly in the case of public cloud and community cloud deployments;
4) On-demand self-service: a feature where a CSC can provision computing capabilities, as needed, automatically or with minimal interaction with the CSP. This offers users a relative reduction in costs, time, and effort needed to take an action, since it grants the user the ability to do what they need, when they need it, without requiring additional human user interactions or overhead;
5) Rapid elasticity and scalability: A feature where physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources. For the CSC, the physical or virtual resources available for provisioning often appear to be unlimited and can be purchased in any quantity at any time automatically, subject to constraints of service agreements. Therefore, the CSCs no longer need to worry about limited resources nor capacity planning;
6) Resource pooling: a feature where a CSP’s physical or virtual resources can be aggregated in order to serve one or more CSCs. The CSPs can support multi-tenancy while at the same time using abstraction to mask the complexity of the process from the CSCs. From the CSC’s perspective, all they know is that the service works, while they generally have no control or knowledge over how the resources are being provided or where the resources are located. This offloads some of the customer's original workload, such as maintenance requirements, to the provider (ISO/IEC, 2014a).

These characteristics were corroborated by other authors, adding others: 1) the high-scale use of computing resources, with the provision of services ubiquitously, with the allocation of consumers' computing needs at a single point; 2) its purpose in general terms; 3) the provision of secure services; 4) the payment adjusted to its use; 5) adherence to standards, which go through the agreement of service levels with the end-user/customer; 6) permanent availability; 7) environmental benefits; 8) they can be used for every purpose from disaster recovery/business continuity through to a fully outsourced ICT service for an organisation (Al-Anzi, Yadav, & Soni, 2014; Armbrust et al., 2010; Blokdijk & Menken, 2009; Dukaric & Juric, 2013; Expert Group Report, 2010; Grossman, 2008; Höfer & Karagiannis, 2011; Jadeja & Modi, 2012; Jula, Sundararajan, & Othman, 2014; Mell & Grance, 2011; Murtaza & Al Masud, 2012; Pallis, 2010; Qian, Luo, Du, & Guo, 2009; Rittinghouse & Ransome, 2010; Schubert & Jeffery, 2012; Shawish & Salama, 2014; Sindhu & Sindhu, 2017; Talia, 2011; Vaquero et al., 2009; Youseff et al., 2008; Zissis & Lekkas, 2012).

These features have resulted in enormous potential for further technological advancements, with reduced costs, while giving use of other underutilized resources in data centres (Murtaza & Al Masud, 2012; Talia, 2011; Youseff et al., 2008).

The majority of cloud computing infrastructure consists of time tested and highly reliable services built on servers with varying levels of virtualized technologies, which are delivered via large data centres operating under SLAs that require 99.99% or better uptime (Blokdijk & Menken, 2009; Rittinghouse & Ransome, 2010).

The architecture for cloud computing has been defined by many researchers. Basically, the whole system can be divided into the core stack and the management. In the core stack, there are three layers:

1. Resource - this layer is the infrastructure layer which is composed of physical and virtualized computing, storage and networking resources;
2. Platform – this is the most complex part which could be divided into many sub-layers (e.g. a computing framework manages the transaction dispatching and/ or task scheduling; a storage sub-layer provides unlimited storage and caching capability);
3. Application – based on the underlying resource and components, the application could support large and distributed transactions and management of huge volume of data (Qian et al., 2009; Shawish & Salama, 2014).

4.

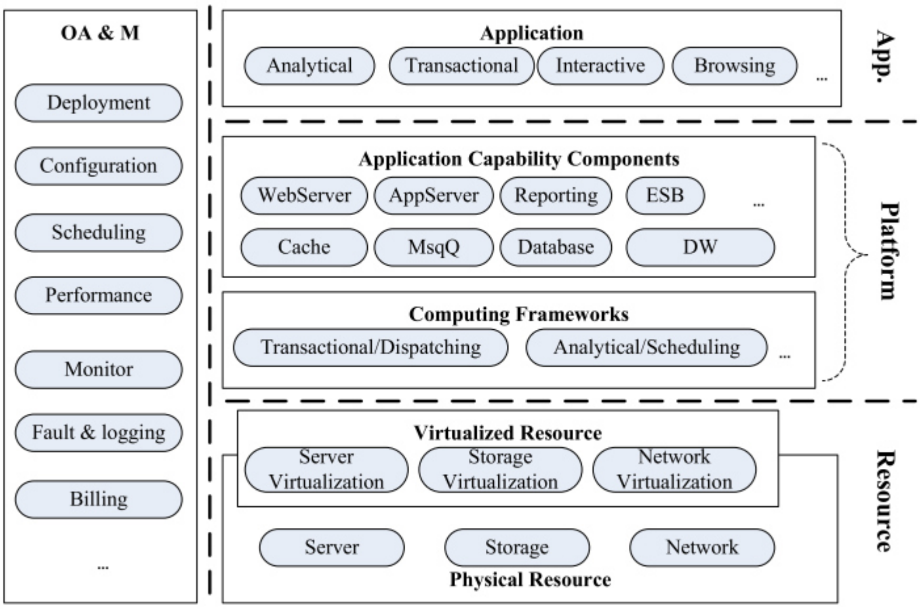

Figure 1: Cloud computing architecture.(Qian et al., 2009)

4.1.3. Roles

Within the context of cloud computing, it is often necessary to differentiate requirements and issues for certain parties, who play roles (and sub-roles). Roles, in turn, are sets of activities and activities themselves are implemented by components. A party may play more than one role at any given point in time and may only engage in a specific subset of activities of that role. All cloud computing related activities can be categorized into three main groups: 1) activities that use services; 2) activities that provide services; and 3) activities that support services (ISO/IEC, 2014a, 2014b).

The major roles of cloud computing are:

1) Cloud service customer (CSC): a party which is in a business relationship for the purpose of using cloud services. The business relationship is with a CSP or a cloud service partner. A CSC may use cloud services, perform business administration, and administer use of cloud services. Usually, CSCs act as controllers under the GDPR;
2) Cloud service partner: a party which is engaged in support of, or auxiliary to, activities of either the CSP or the CSC, or both. Cloud service partner's activities vary depending on the type of partner and their relationship with the CSP and the CSC;
3) Cloud service provider (CSP): a party which makes cloud services available. The CSP focuses on activities necessary to provide a cloud service and activities necessary to ensure its delivery to the CSC, as well as cloud service maintenance. The CSP includes an extensive set of activities

(e.g., provide service, deploy and monitor service, manage business plan, provide audit data, etc.) as well as numerous sub-roles (e.g., business manager, service manager, network provider, security and risk manager, etc.).Usually, CSPs act as processors under the GDPR (ISO/IEC, 2014a, 2014b; Russo et al., 2018)

Considering security and the protection of PII, the CSC has the main duties:

- To ensure appropriate security for CSC data that is placed into a cloud computing environment;
- To put in place plans for data backup and recovery, and potentially for data duplication and failover;
- To administer security policies;
- To define encryption and integrity technologies to apply to the CSC data both at rest and also in motion;
- To define the handling of any PII in the CSC data (ISO/IEC, 2014b).

Moreover, the connection of existing ICT components and applications with the target cloud service(s) involves:

assessing the impact of cloud service(s) on existing processes, systems and services; mapping business data between CSC's existing ICT systems and cloud services; invoking cloud service operations from existing ICT components and applications, with the supply of input data and the handling of output data; provisioning of access rights for CSC's cloud service users; defining and implementing security related requirements, including the confidentiality and integrity of data flows; integrating customer facilities for the administration of user accounts, security roles, identities and permissions with the equivalent facilities for the cloud services; creating and monitoring specific user accounts and identities for the use of management interfaces for cloud services; integrating logging and security incident management between cloud services and CSC monitoring and management infrastructure (ISO/IEC, 2014b, Chapter 8.2.2.11).

Considering security and the protection of PII, the CSP has the main duties:

- To manage assets and inventory activity, which involves: keeping track of all compute, storage, network and software assets and the relationship between them; and ensuring that new assets are fit for purpose and have been properly checked from a security and manageability standpoint and can include the disposal of assets that are no longer required. This can include appropriate secure disposal of any assets that might hold data;
- To provide audit data activity, which is to deliver the collection and provision of data relevant to an audit request, such as that relating to security controls or to service performance and this

activity involves creating and sending appropriate audit information from logs, etc.; and redacting information from any log records or other data that might contain sensitive information or PII;

- To assure that the cloud service adheres to appropriate standards relating to security and business compliance;
- To manage security and risks activity, which is focused on the management of security and risks associated with the development, delivery, use and support of cloud services, which includes:
    - defining information security policy, considering the service requirements, statutory and regulatory requirements and contractual and SLA obligations;
    - defining information security risks relating to the cloud service and the approach to those risks in order to achieve the business goals of the CSP;
    - selecting design point and associated information security controls required to address risks associated with the service and design point chosen. The controls typically include: identity and access management; discover, categorize, protect data and information assets; information systems acquisition, development and maintenance; secure infrastructure against threats and vulnerabilities; problem and information security incident management; security governance and compliance; physical and personnel security; security of networks and communications; isolation (between tenants in a multi-tenant situation);
- To ensure that controls are in place for the deployed service and the underlying infrastructure;
- To design, implement and evaluate the system and application security;
- To manage, design, implement and evaluate the security of cloud services of peer CSPs;
- To evaluate the effectiveness of the implemented controls and make changes based on experience;
- To assure that operating and business support systems provide data access to CSP staff based on the particular CSCs tenants they provide a service to;
- To ensure compliance activity focuses on implementing regulatory and standards compliance (ISO/IEC, 2014b).

The next Figure represents an overview of the main aspects that constitute a cloud system.

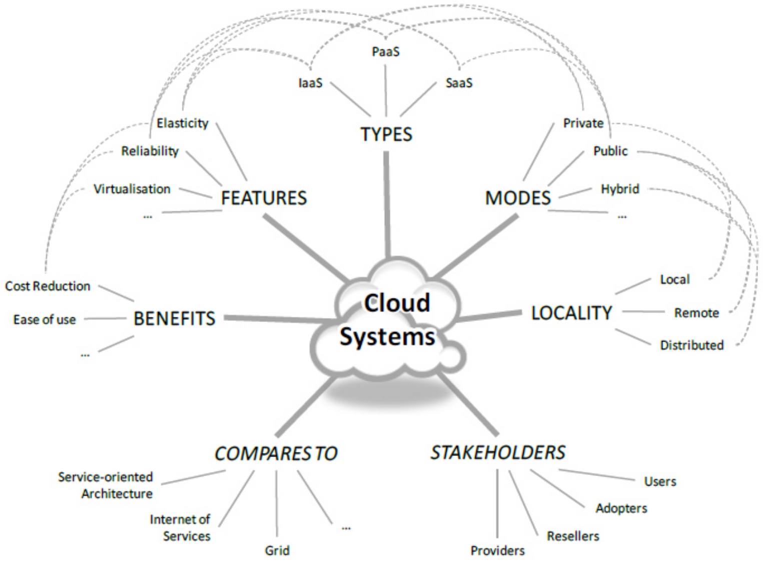

Figure 2: Non-exhaustive view on the main aspects forming a cloud system (Expert Group Report, 2010)

4.2. Cloud Capabilities and Service Models

A cloud capabilities type is a classification of the functionality provided by a cloud service to the CSC, based on the resources used. There are three different cloud capabilities types, which follow the principle of separation of concerns (i.e. they have minimal functionality overlap between each other): 1) application capabilities type; 2) infrastructure capabilities type; and 3) platform capabilities type. (ISO/IEC, 2014a).

The cloud capabilities types are:

- Application capabilities type: a cloud capabilities type in which the CSC can use the CSP's applications;
- Infrastructure capabilities type: a cloud capabilities type in which the CSC can provision and use processing, storage or networking resources;
- Platform capabilities type: a cloud capabilities type in which the CSC can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the CSP (ISO/IEC, 2014a, Chapter 6.4).

The cloud capabilities types should not be confused with other categorizations of cloud services (ISO/IEC, 2014a).

A cloud service category is a group of cloud services that has common qualities; a cloud service category may include capabilities from one or more cloud capabilities types (ISO/IEC, 2014a). Clouds are used through a service-oriented interface that implements the "as a service" paradigm, that is to provide cloud services on demand, which might include computing, storage, and software (Armbrust et al., 2010; Grossman, 2009; Voorsluys et al., 2011).

Cloud service categories include:

- Infrastructure as a Service (IaaS): A cloud service category in which the cloud capabilities type provided to the CSC is an infrastructure capabilities type;
- Platform as a Service (PaaS): A cloud service category in which the cloud capabilities type provided to the CSC is a platform capabilities type;
- Software as a Service (SaaS): A cloud service category in which the cloud capabilities type provided to the CSC is an application capabilities type (Armbrust et al., 2010; Dukaric & Juric, 2013; Expert Group Report, 2010; Grossman, 2009; Höfer & Karagiannis, 2010; ISO/IEC, 2014a; Sindhu & Sindhu, 2017).

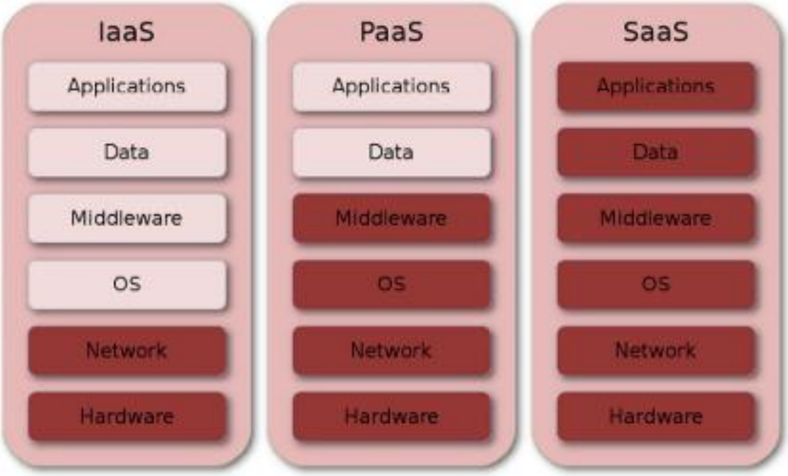

Figure 3: Difference between cloud types, considering service models (Bartolini, Santos, & Ullrich, 2018)

4.2.1. Software as a Service

On the SaaS model, the consumer can use the provider's already-created applications, which are accessible anytime and from anywhere, running on a cloud infrastructure (Expert Group Report, 2010; Höfer & Karagiannis, 2010; Information Commissioner of Slovenia, 2012; Mell & Grance, 2011; Shawish & Salama, 2014; Sindhu & Sindhu, 2017; Vaquero et al., 2009).

Applications are accessible from various client devices, eliminating the need to install and run the application on the user's system (Information Commissioner of Slovenia, 2012; Jadeja & Modi, 2012; Jula et al., 2014; Mell & Grance, 2011; Shawish & Salama, 2014; Zissis & Lekkas, 2012). Therefore, applications are accessible to a high number of customers using a multiuser architecture (Rittinghouse & Ransome, 2010). The consumer does not manage or control the underlying cloud infrastructure, except for limited user-specific application configuration settings (Höfer & Karagiannis, 2010; Jansen & Grance, 2011; Mell & Grance, 2011). For the customer, there are no costs in servers or software licensing and for the service provider, with just one product to maintain, costs are relatively low compared to the costs incurred with a conventional hosting model (Jansen, 2011; Rittinghouse & Ransome, 2010). As previously referred, this is considered to be the most mature type of cloud computing (Kshetri, 2012).

With SaaS, users greatly rely on their CSPs for security, since the customer has minimal control or extensibility. In accordance, the provider must ensure that multiple companies or users are unable to see each other's data without permission, it must protect the underlying infrastructure from break-ins and it generally has responsibility for all authentication and encryption. In this sense, it's difficult for the CSC to be certain that the right measures are being taken (Al-Anzi et al., 2014; Jansen & Grance, 2011; Shawish & Salama, 2014).

4.2.2. Platform as a Service

On the PaaS model, the consumer is offered with a software platform where systems run on (Vaquero et al., 2009).

The service providers offer APIs that enable developers to exploit functionality over the Internet, as the CSPs deliver development environments. The CSC can deploy onto the cloud infrastructure consumer-created or acquire applications created using programming languages, libraries, services, and tools supported by the CSP. The CSC does not manage or control the underlying cloud infrastructure but has control over the deployed applications and configuration settings for the application-hosting environment. A general model is implemented on which developers build applications designed to run on the CSP's infrastructure, being delivered to users via an Internet browser (Expert Group Report, 2010; Höfer & Karagiannis, 2010; Jadeja & Modi, 2012; Jansen, 2011; Jansen & Grance, 2011; Jula et al., 2014; Mell & Grance, 2011; Rittinghouse & Ransome, 2010; Shawish & Salama, 2014; Sindhu & Sindhu, 2017; Zissis & Lekkas, 2012).

This model allows a quick and cost-effective development and deployment of applications (Kshetri, 2012), though these services are limited by the vendor's design and capabilities (Rittinghouse & Ransome, 2010).

With PaaS, the CSP might give some control to the people building applications, which means that developers might be able to create their own authentication systems and data encryption. However, any security below the application level will still be in the CSP's hands and the platform provider must be able to offer assurances that the data remains inaccessible between applications (Shawish & Salama, 2014). Therefore, the CSP is responsible for security and monitoring, since it provides runtime, middleware, OS, networking, servers, storage and virtualization (Al-Anzi et al., 2014).

4.2.3. Infrastructure as a Service

On the IaaS model, services typically offer a virtualization platform environment (Expert Group Report, 2010; Höfer & Karagiannis, 2010). Clients buy the resources and the CSP can manage processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The CSC does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (Al-Anzi et al., 2014; Höfer & Karagiannis, 2010; Jansen, 2011; Jansen & Grance, 2011; Jula et al., 2014; Mell & Grance, 2011; Sindhu & Sindhu, 2017; Zissis & Lekkas, 2012). The CSCs rent virtual servers, called instances, for the time needed, and then deploy their own software on the virtual machines and control and manage them. The number of instances can be dynamically scaled to fulfil the CSCs' need and billing is based on this amount, the duration and additional services used, such as additional storage space (Höfer & Karagiannis, 2010).

Therefore, infrastructure providers manage a large set of computing resources, such as storing and processing capacity, and through virtualization they can split, assign and dynamically resize these resources to build ad-hoc systems as required by CSCs (Vaquero et al., 2009).

IaaS is centred around a model of service delivery that provisions a standardized infrastructure, optimized for the CSC's applications, with simplified statements of work and à la carte service-level choices, which make it easy to tailor a solution to a CSC's specific application requirements (Rittinghouse & Ransome, 2010). The CSC need not to purchase the required servers, data centre or the network resources: they only need to pay for the time they use the service. As a result, CSCs can achieve a much faster service delivery with less cost (Jadeja & Modi, 2012; Rittinghouse & Ransome, 2010). Also, CSPs often have data centres in multiple locations to offer quick access all over the world and web interfaces that allow monitoring of the cloud service (Höfer & Karagiannis, 2010).

With IaaS, the developer has much better control over the security environment, because applications run on virtual machines separated from other virtual machines running on the same physical machine, which makes the process safer, as long as there is no gaping security hole in the virtual machine manager. This control makes it easier to ensure that developers properly address security and compliance concerns (Shawish & Salama, 2014).

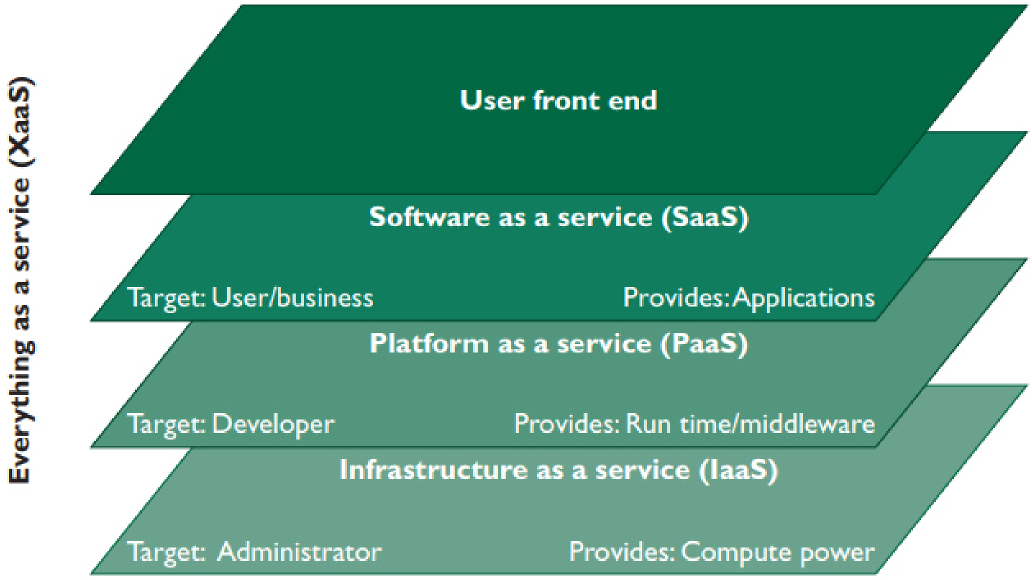
Everything as a service (XaaS)
User front end
Software as a service (SaaS)
Target: User/business
Provides: Applications
Platform as a service (PaaS)
Target: Developer
Provides: Run time/middleware
Infrastructure as a service (IaaS)
Target: Administrator
Provides: Compute power

Figure 4: A general layered architecture of cloud infrastructures (Pallis, 2010)

4.3. Deployment Models

"Cloud deployment models represent how cloud computing can be organized based on the control and sharing of physical or virtual resources" (ISO/IEC, 2014a, Chapter 6.5). They broadly characterize the management and disposition of computational resources for delivery of services to CSCs, as well as the differentiation between classes of CSCs. There are 4 models as the cloud may be characterized as private, community, public or hybrid (Expert Group Report, 2010; Information Commissioner of Slovenia, 2012; ISO/IEC, 2014a; Jansen & Grance, 2011; Mell & Grance, 2011; Murtaza & Al Masud, 2012).

On the private cloud, the infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises (Expert Group Report, 2010; ISO/IEC, 2014a; Jansen & Grance, 2011; Jula et al., 2014; Mell & Grance, 2011; Murtaza & Al Masud, 2012; Shawish & Salama, 2014). All services, as well as infrastructure are under control of the CSP, whereas management can be implemented through a third party. The services may be available on the internet or over the virtual private networks (Information Commissioner of Slovenia, 2012; ISO/IEC, 2014a).

On the community cloud, the infrastructure is provisioned for exclusive use by a specific community of CSCs from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises (ISO/IEC, 2014a; Jula et al., 2014; Mell & Grance, 2011; Murtaza & Al Masud, 2012; Shawish & Salama, 2014). Community clouds can either aggregate public clouds or dedicated resource infrastructures (Expert Group Report, 2010).

On the public cloud, the infrastructure and resources are provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider (ISO/IEC, 2014a; Jansen & Grance, 2011; Mell & Grance, 2011; Murtaza & Al Masud, 2012; Shawish & Salama, 2014). The cloud owner provides public services in most cases on the Internet based on predefined rules, policies, and a pricing model (Jula et al., 2014), reducing costs and effort to build up the needed infrastructure (Expert Group Report, 2010). Public clouds have very broad boundaries, where CSC access to public cloud services has few, if any, restrictions (ISO/IEC, 2014a).

Finally, on the hybrid cloud, the infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are connected by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) (ISO/IEC, 2014a; Jansen & Grance, 2011; Jula et al., 2014; Mell & Grance, 2011; Murtaza & Al Masud, 2012; Shawish & Salama, 2014). This model allows to achieve a maximum of cost reduction through outsourcing whilst maintaining the desired degree of control over sensitive data (Expert Group Report, 2010).

4.4. Cloud computing cross cutting aspects

Cross cutting aspects are behaviours or capabilities which need to be coordinated across roles and implemented consistently in a cloud computing system, as they might impact multiple roles, activities, and components, in a way that it is not possible to clearly assign them to individual roles or components (ISO/IEC, 2014a).

Key cross cutting aspects include:

- Auditability: the capability of collecting and making available necessary evidence related to the operation and use of a cloud service, for the purpose of conducting an audit. The audit depends upon available data and evidence relating to the usage, environment, availability and performance of services and associated resources. Such data and evidence include records and logs of activities and conditions of the operational environments of all parties of the governing agreements. These records and logs need to be collected and maintained in a secure manner;
- Availability: the property of being accessible and usable upon demand by an authorized entity. The "authorized entity" is typically a CSC;
- Governance: the system by which the provision and use of cloud services are directed and controlled, being related with the requirement for transparency and the need to rationalize governance practices with SLAs and other contractual elements of the CSC to CSP relationship;
- Interoperability: the ability of a CSC to interact with a cloud service and exchange information according to a prescribed method and obtain predictable results;
- Maintenance and versioning: maintenance refers to changes to a cloud service or the resources it uses in order to fix faults or to upgrade/extend capabilities for business reasons; versioning implies the appropriate labelling of a service so that it is clear to the CSC that a version is in use;
- Performance: a set of behaviours relating to the operation of a cloud service, having metrics defined in a SLA;

- Portability: the ability of CSCs to move their data or their applications between multiple CSPs at low cost and with minimal disruption;
- Protection of PII: protect the processing of PII in relation to cloud services. Cloud computing poses additional confidentiality challenges to CSCs using cloud services, and also for CSPs, since in many jurisdictions there are strict rules and regulations applied to the handling of PII – any use of cloud services to store and process PII often must conform to those rules and regulations;
- Regulatory: there are different regulations that may influence the use and delivery of cloud services, which might include statutory, regulatory, and legal requirements that vary by market sector and jurisdiction. These differences can change the responsibilities of both CSCs and CSPs. Compliance with such requirements is often related to governance and risk management activities;
- Resiliency: ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation;
- Reversibility: a process for the CSC to retrieve their CSC data and application artefacts and for the CSP to delete all CSC data as well as contractually specified cloud service derived data after an agreed period;
- Security: includes physical security and application security, as well as requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, non-repudiation, audit, security monitoring, incident response, and security policy management;
- Service levels and service level agreement: the cloud computing SLA is a service level agreement between a CSP and a CSC based on a taxonomy of cloud computing specific terms to set the quality of the cloud services delivered. It characterizes quality of the cloud services delivered in terms of: 1) a set of measurable properties specific to cloud computing and 2) a given set of cloud computing roles (CSC and CSP and related sub-roles) (ISO/IEC, 2014a, 2014b).

Some cross cutting aspects like security, protection of PII, and governance have been identified as major concerns and in some cases an impediment to the adoption of cloud computing (ISO/IEC, 2014a).

4.5. **Privacy, Data Protection and the Cloud**

Despite the acknowledged benefits of cloud computing in both economic and societal terms, the wide scale implementation of cloud computing services can enhance of data protection risks (Article 29 Data Protection Working Party, 2012).

In 2012, the European Commission stated that some actions where needed in order to be enlightened about the applicable legal framework to the cloud computing environment and, ideally, to be easy to verify compliance with the legal framework (e.g. through standards and certification) and by developing it further (European Commission, 2012b).

Certain aspects of data protection are an integral part of the related framework but in the context of cloud computing they do not present any specificity. The areas that are exposed the most are the following: legal and regulatory obligations; contracts, data security, and transfer of data to third countries (which is related with legal and regulatory obligations and contracts/service agreements) (Information Commissioner of Slovenia, 2012; Jansen & Grance, 2011). The lacking control over data location and missing origin poses security and legalistic issues: also there are other potential security holes arising from the fact that the resources are shared between multiple tenants and the location of the resources is potentially unknown (European Commission, 2012b; Expert Group Report, 2010; Sindhu & Sindhu, 2017).

On the other hand, addressing the specific challenges of cloud computing would mean a faster and harmonized adoption of the technology by organizations, resulting in accelerated productivity growth and increased competitiveness across the whole economy (European Commission, 2012b). However, if the usage of cloud services can bring significant rewards, it also imposes new types of risks (European Commission, 2019). By introducing personal data to the systems managed by a CSP, CSCs are no longer in exclusive control of these data and, therefore, cannot deploy the technical and organizational measures needed to ensure the availability, integrity, confidentiality, transparency, isolation, intervenability and portability of the data (Article 29 Data Protection Working Party, 2012).

The main privacy/data protection risks related with cloud computing services are:

1) for the cloud service user: being forced or persuaded to be tracked or give personal information against their will, or in a way in which they feel uncomfortable;
2) for the organization using the cloud service: noncompliance to enterprise policies and legislation, loss of reputation and credibility;
3) for implementers of cloud platforms: exposure of sensitive information stored on the platforms (potentially for fraudulent purposes), legal liability, loss of reputation and credibility, lack of user trust and take-up;
4) for providers of applications on top of cloud platforms: legal noncompliance, loss of reputation, ‘function creep’ using the personal information stored on the cloud, i.e. it might later be used for purposes other than the original cloud service intention;

5) for the data subject: exposure of personal information (Pearson, 2009, p. 4).

However, the attitude on cloud computing services can significantly vary among organizations, because of inherent differences as the intended purpose, assets held, legal obligations, exposure to the public, threats faced, and risk tolerance (Jansen & Grance, 2011). In this sense, accountability could be a mechanism to reduce end user privacy/data protection risk and enhance end user control (Jaatun, Pearson, Gittler, Leenes, & Niezen, 2016; Pearson & Charlesworth, 2009). Kemp also provided a checklist that could help to achieve compliance regarding GDPR for cloud services (Kemp, 2018); other authors are designing cloud platforms that could ensure GDPR compliance (Crompton & Jensen, 2019). Another possible solution to overcome those barriers could be through the promotion of a cloud certification scheme. However, nowadays, the compliance with existing certification schemes is a big challenge for CSPs, mainly due to the high market fragmentation of cloud and security certification schemes(Fundación Tecnalia Research & Innovation, 2018). Even though Portugal has defined a cybersecurity strategy, nothing related to cloud security certification is mentioned (Fundación Tecnalia Research & Innovation, 2018).

Finally, a Code of Conduct for GDPR Compliance was already published by the CSA, aiming to provide CSPs and CSCs a solution for GDPR compliance and to provide transparency guidelines regarding the level of data protection offered by the CSP, even if it wasn’t approved by a proper supervisor authority (Cloud Security Alliance, 2018). There is also the EU Code of Conduct, which sets out clear requirements and recommends procedures to raise the level of data protection in cloud services, based on GDPR. However, since for the time being the appointed Monitoring Body has no accreditation pursuant to Article 41 of GDPR, this Monitoring Body shall not verify any Cloud Service as compliant with this Code as a code of conduct pursuant to Article 40 GDPR (EU Cloud CoC, 2019).

4.5.1. Legal and regulatory obligations

Law awareness in cloud computing is a hot topic because the adoption of cloud computing is in an advanced state and the boost to adopt cloud computing by organizations is particularly felt (Di Martino, Cretella, & Esposito, 2015). At the same time, the traditional legal framework might be seriously jeopardized by the advent of cloud computing and so far no specific pan-European regulation has been elaborated embracing cloud computing (Bartolini et al., 2018).

The lack of clear territorial boundaries in the digital world leads to specific legal problems and general problems of perception when managing one's privacy (ENISA Ad Hoc Working Group on Privacy & Technology, 2008).

Various types of security and privacy laws and regulations exist at the national, state, and local levels, making compliance an issue for cloud computing (European Commission, 2012b; Gray, 2013; Jansen & Grance, 2011; Pearson, Shen, & Mowbray, 2009). In fact, there is a big difference between the rules applicable to countries belonging to EU and those outside the EU (Di Martino et al., 2015).

Moreover, cloud computing is related with several barriers in numerous European and national regulations (Casalicchio & Palmirani, 2015). For instance, just on the European context there are at least eleven instruments of EU law having a bearing on breaches, five in the Area of Freedom, Security and Justice (AFSJ) and six in the internal market (Porcedda, 2018). One with main importance to cloud computing is the NIS Directive, that lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market (European Parliament and the Council of the European Union, 2016) and transposed to the Portuguese context under the Law 46/2018 (Assembleia da República, 2018).

In all cases outside the European jurisdiction, the defined adequate level of privacy protection does not take into account the possibility of access of national security agencies (ENISA Ad Hoc Working Group on Privacy & Technology, 2008). Thus, the rise of the cloud has significantly challenged established legal paradigms (Schwarz, 2014).

Also, the discrepancies of European and American legislation create risks that must be mitigated when dealing with global cloud providers, inter alia through a combination of provider due diligence, contractual provisions and technical security controls (European Commission, 2019).

The GDPR provides a general framework that is relevant in this context (Bartolini et al., 2018), since it at aims to reform data protection rules in the EU in order to strengthen individuals' rights while ensuring a free flow of personal data, and provide a coherent data protection framework to support effective implementation considering the challenges resulting from globalisation and the use of new technologies. To the CSPs that means responsibility, since they have to demonstrate their willingness and capacity in handling people's information (Jaatun et al., 2016) in two different ways at least: with contractual responsibilities as data processors and with new measures with the aim of enforcing the rights of data subjects (Vidovic, 2016).

Thus, CSPs are becoming more sensitive to legal and regulatory concerns even if organizations are ultimately accountable for the security and privacy of data held by a CSP on their behalf (Jansen & Grance, 2011). The problem is to understand how to comply with privacy laws and regulations when choosing cloud-based services (Di Martino et al., 2015; Pearson & Charlesworth, 2009), considering the international scale of information processing, the development of personal information processing as a networked event and the change in management processes to allow outsourcing of computing resources (Schwarz, 2014).

CSPs need to design their processes to ensure that their obligations and practices can be documented, considering technical and procedural measures, which could provide appropriate contextual safeguards to PII processing in the cloud (Di Martino et al., 2015).

Even so, maintaining the desired or mandatory levels of protection of data and privacy required by current legislation in a cloud computing infrastructure is a serious challenge, as well is meeting the restrictions on cross-border data transfer, considering the multidirectional nature of data flows, which occur as a networked series of processes (Di Martino et al., 2015; Schwarz, 2014). Therefore, many CSPs have datacentres in more than one EEA Member State (Hon & Millard, 2018).

Regulative institutions are important, since cloud computing poses various challenges for companies that have responsibilities to meet stringent compliance related to frameworks that weren’t designed considering cloud’s characteristics. However, some regulations governing the cloud are impractical and unclear. Moreover, current regulations governing cloud security, which are derived from previous generations of technologies, arguably favour CSPs (Kshetri, 2012) .

Thus, the variety of legislations makes it necessary to implement a framework for managing legal compliance checking, making it possible to achieve two main goals: 1) to detect *ex-ante* the needed measures to prevent a cloud service from infringing laws, regulations, policies, contracts or SLAs; 2) to alert CSPs in case the legislation should introduce new service requirements, new privacy or security policy specifications or new business processes (Casalicchio & Palmirani, 2015).

Considering the impact of GDPR on the cloud computing environment, several considerations must be made:

1) Usually, the CSP qualifies as the processor;
2) The controller is harder to identify in cloud computing, and depends on what data is stored and by whom;

3) Under an extensive interpretation of personal data, most of the information stored on the cloud by the customer might be considered personal data and fall under the protection of the GDPR and the scope of Articles 17 and 20;
4) The privacy terms of many cloud computing service contracts are not transparent enough, do not disclose the necessary information to the users, and might not integrate all the legal requirements of the GDPR (such as the right of access or the right to data portability);
5) GDPR does not provide for the case of a transfer of the assets, a merger or acquisition, or a split-up (or division). However, adequate protection should be granted to the data subjects, as such operations can seriously put personal data at risk (Bartolini et al., 2018; Hon, Millard, & Walden, 2012; Vidovic, 2016).

4.5.2. Contracts/service agreements

The qualification of a cloud computing contract within the existing legal framework is of key importance, since it may determine which legal provisions are applicable to it, and contracts for online services must be valid under the applicable contract law.(DLA Piper UK LLP, 2015; European Data Protection Board, 2019b).

The general basis on which CSPs and CSCs enter into a relationship falls into two clear categories, depending on whether the CSP is offering a paid service or a free one. However, this distinction is not a clear one, since some “free” services may impose non-monetary costs on the CSC, such as contextual advertising or even the imposition of license terms that allow the CSP to re-use the CSCs data for its own purposes. Paid services also fall into a spectrum between those entered into on the basis of the standard-form contract of the provider and those where the contract terms are fully negotiated (Bradshaw, Millard, & Walden, 2011). Thus, the EDPB provided guidelines to processing of personal data in the context of contracts for online services, irrespective of how the services are financed (European Data Protection Board, 2019b).

Usually service contracts are generic and standardized, made out by the CSP and balanced in its favor. No personalization is allowed or, if so, with little bilateral opportunity to change the terms (Article 29 Data Protection Working Party, 2012; Bartolini et al., 2018; Casalicchio & Palmirani, 2015; European Commission, 2012b; Schwarz, 2014). This is often achieved by means of “click-wrap agreements”[142],

[142] Click-wrap agreements are a set of terms set forth by the vendor of the software or service, followed by the option for the user to accept the whole agreement with a single click. (Bartolini et al., 2018, p. 375)

which are drafted entirely by the CSP, and any operation performed by the CSC entails an implicit agreement of all the terms and as such the CSC is not able to participate in the definition of the contractual clauses (Bartolini et al., 2018). It is important to point out that contracts for digital services may incorporate express terms that impose additional conditions about advertising, payments or cookies, amongst other things. However, a contract cannot expand the categories of personal data or types of processing operation that the controller needs to carry out for the performance of the contract (European Data Protection Board, 2019b).

Specifications for public cloud services and service arrangements are generally called service agreements or service contracts. A service agreement defines the terms and conditions for access and use of the services offered by the cloud provider and it also establishes the period of service, conditions for termination, and disposition of data upon termination. The complete terms and conditions for a cloud service agreement are usually stipulated in multiple documents, which can typically include a Service Level Agreement[143] (SLA), privacy policy[144], acceptable use policy [145], and terms of use [146,] (Bradshaw et al., 2011; Jansen & Grance, 2011). SLAs constitute an important part of the contract, as they set the boundaries within which the cloud service must be provided in terms of availability, response time in case of failures, security, data management, among other key issues (DLA Piper UK LLP, 2015). As for the terms of service, most of them are silent, or suggest that the provider is not a controller of that data, or even explicitly provide for processor status (Hon et al., 2012).

On the Portuguese context, the rules in force for service contracts are applicable for these cloud services, since there are no specific provisions/regulation on this matter (Silva, 2016), being applicable the Decree-Law 220/95 (Decreto-Lei n.º 220/95, de 31 de agosto, in the original), as well as the Decree-Law 7/2004 (Decreto-Lei n.º 7/2004, de 7 de janeiro, in the original).

Before entrusting data to a CSP, the CSC needs to carefully read of their terms and conditions to understand deeply how the data will be treated on the cloud (Di Martino et al., 2015), since contractual terms may vary significantly between CSPs (Bartolini et al., 2018). Also, the European Commission already referred that problems with contracts were detected, being insufficiently specific and unbalanced (European Commission, 2012b).

[143] This document specifies the level of service the CSP aims to deliver together with the process for compensating CSCs if the actual service fails. Accordingly, SLAs are associated only with paid-for services (Bradshaw et al., 2011).

[144] This document describes the CSP's approach to process and protect the CSC's personal information (Bradshaw et al., 2011).

[145] This document details the permitted and/or forbidden uses of the service (Bradshaw et al., 2011; DLA Piper UK LLP, 2015).

[146] This document details the relationship between the CSC and CSP and it usually contains the commercial terms of the service, where applicable, including legal clauses such as choice of law and disclaimers (Bradshaw et al., 2011).

Purpose limitation and data minimization principles are particularly relevant in contracts for online services, which typically are not negotiated on an individual basis and nowadays controllers easily collect and process more personal data than ever before. When processing is not in fact necessary for the performance of a contract, such processing can take place only if it relies on another appropriate legal basis. In order to be in line with transparency obligations, controllers should know what the applicable legal basis is. Moreover, the controller should consider another legal basis for processing when it cannot demonstrate that a contract exists, that the contract is valid pursuant to applicable national contract laws, and/or that the processing is objectively necessary for the performance of the contract (European Data Protection Board, 2019b).

The contractual limitation also affects SaaS providers, since often they cannot dictate terms to large IaaS/PaaS subproviders (Hon & Millard, 2018).

Besides the need to protect the parties within the contract, when businesses draft cloud agreements, they may not adequately protect the interests of third parties. The logic of EU law is that contracts, left alone, will be unable to manage the resulting privacy/data protection and security externalities for CSCs (Schwarz, 2014). Even if often the contractual documentation determines which security measures the CSP will ensure, it is also possible that the contract remains silent on this point. Therefore, in case of a dispute, the parties will need to verify whether applicable law states any specific security requirements (DLA Piper UK LLP, 2015).

Overall, the most common and significant legal issues that can arise in contracts related with cloud computing services are:

1) Data privacy security and confidentiality: the confidentiality, availability and integrity of data must be ensured by means of appropriate organizational and technical measures [147]. These also include the protection of systems and data from the risks of unauthorized or arbitrary destruction, arbitrary loss, technical faults, forgery, theft and unlawful use, as well as from unauthorized modification, copying, access or other unauthorized processing;
2) Location of data: some CSP form contracts expressly reserve the right to store CSC data in any country in which they do business. While dispersed geographical storage is beneficial from a data protection and backup perspective, it can raise law issues for some kind of data [148];

[147] This is also a GDPR provision.

[148] This has particular relevance if the countries where the data is stored are outside the EU.

3) Suspension and termination of the service: the vendor will return or destroy any copies of data once the cloud service is no more used by the customer, but this cannot be assumed [149]. Considering the termination of contract, where GDPR's Article 6, n.° 1, b) is the basis for some or all processing activities, the controller should anticipate what happens if that contract is terminated, since, as a general rule, the processing of that data will no longer be necessary for the performance of that contract and thus the controller will need to stop processing
4) Ownership of data: the contract should expressly make clear that all data belongs to the CSC and that the vendor acquires no rights or licenses to use the data for its own purposes (Di Martino et al., 2015; DLA Piper UK LLP, 2015; European Data Protection Board, 2019b).

4.5.3. Data security

In addition to the core security objectives of availability[150], confidentiality[151] and integrity[152], it also should be considered the data protection principles, responsibilities, and security of processing as indicated on GDPR, as well as data protection by default and data protection by design (ENISA, 2018b).

Security is one of the most often-cited objections to cloud computing but with the growing maturity of the cloud computing environment, security concerns are being more consistently addressed (Shawish & Salama, 2014).

The transformational nature of the cloud is associated with significant security and privacy risks and a significant gap remains between vendors' claims and users' views of the cloud's security, privacy and transparency (Kshetri, 2012). If the cloud industry still states that clouds are more secure than whatever the user might be using, the fact is that due primarily to concerns related to security, privacy and confidentiality, its perceived costs may outweigh the benefits (Kshetri, 2012; Talbot, 2010).

Trust, security and privacy always pose challenges in any internet provided service, but due to the specific nature of clouds, additional aspects related to their characteristics, such as multitenancy arise and control over data location etc. enhance those concerns (Expert Group Report, 2010; Sindhu & Sindhu, 2017).

Even though cloud services provide a high potential for increasing efficiency in the business world, they also have some limitations, that could affect data protection:

[149] This is also stipulated on GDPR.

[150] "Property of being accessible and usable on demand by an authorized entity" (ISO/IEC, 2018a, Chapter 3.7).

[151] "Property that information is not made available or disclosed to unauthorized individuals, entities, or processes" (ISO/IEC, 2018a, Chapter 3.10)

[152] "Property of accuracy and completeness" (ISO/IEC, 2018a, Chapter 3.36)

1) Business Continuity and Service Availability: Organizations worry about whether utility computing services will have adequate availability, and this makes some wary of cloud computing. However, existing SaaS products have set a high standard in this regard and users expect similar availability from new services, which is difficult to do. Besides the technical limitations, a CSP could suffer outages for non-technical reasons, including going out of business or being the target of regulatory action. The management of a cloud computing service by a single company is a single point of failure, since even if the company has multiple data centres in different geographic regions using different network providers, it may have common software infrastructure and accounting systems, or the company may even go out of business (Armbrust et al., 2010; Expert Group Report, 2010);
2) Data Lock-in: a major concern of CSC is about having their data locked-in by a certain provider. CSC may want to move data and applications out from a provider that does not meet their requirements. The storage APIs for cloud computing are still essentially proprietary, or at least have not been the subject of active standardization. Thus, customers cannot easily extract their data and programs from one site to run on another (Armbrust et al., 2010; Article 29 Data Protection Working Party, 2012; Bartolini et al., 2018; Shawish & Salama, 2014);
3) Risk due to involvement of a third party: with the CSP, a third party becomes involved in the processing of personal data, which, from the point of view of the affected person whose rights are to be protected, represents an increase in the risk that unauthorized persons (such as hackers) might be able to access the data being processed. Even so, properly devised cloud services are actually capable of providing better protection against unauthorized accessing of personal data than traditional outsourcing infrastructures (Talbot, 2010; The Cloud Privacy Check (CPC), 2017);
4) Loss of control: an increase in the number of people authorized to access the processed data means an increase in the challenge of committing all involved persons to act according to data protection laws, as well as the challenge of verifying the observance of all data protection obligations. The term "loss of control" refers to the fact that the affected person often does not know who the authorized third parties are or has no way of monitoring them (Blokdijk & Menken, 2009; Jansen & Grance, 2011; Takabi, Joshi, & Ahn, 2010; Talbot, 2010; The Cloud Privacy Check (CPC), 2017). A cloud provider may use its physical control over data from different clients to link personal data. If administrators are facilitated with sufficiently privileged access rights (high-risk roles), they could link information from different clients (Article 29 Data Protection

Working Party, 2012; ENISA, 2017b). Furthermore, cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers (Sindhu & Sindhu, 2017);

5) Secure Data Storage: storing large amounts of data that is oriented around user privacy, identity, and application-specific preferences in centralized locations raises many concerns about data protection. These concerns, in turn, give rise to questions regarding the legal framework that should be implemented for a cloud-oriented environment (Rittinghouse & Ransome, 2010). Moreover, large amounts of data storage might also mean large amounts of data loss in case of a breakdown (Talbot, 2010). Storing of data on remote cloud servers gives the following three states that are of particular concern within the operational context of cloud computing: 1) the transmission of personal sensitive data to the cloud server; 2) the transmission of data from the cloud server to clients' computers; and 3) the storage of clients' personal data in cloud servers which are remote server not owned by the clients (Ahmed & Hossain, 2014; Sindhu & Sindhu, 2017);

6) Data Confidentiality/Auditability: one of the most serious concerns is the possibility of confidentiality violations (Jansen, 2011; Shawish & Salama, 2014). CSC face security threats both from outside and inside the cloud, but many of the security issues involved in protecting clouds from outside threats are similar to those already facing large data centres. In the cloud, however, this responsibility is divided among potentially many parties, including the CSC, the CSP, and any third-party vendors that users rely on for security-sensitive software or configurations. The primary security mechanism in clouds is virtualization, which protects against most attempts by users to attack one another or the underlying cloud infrastructure. However, not all resources are virtualized and not all virtualization environments are bug-free. Auditability could be added as an additional layer beyond the reach of the virtualized guest OS, providing facilities more secure than those built into the applications themselves and centralizing the software responsibilities related to confidentiality and auditability into a single logical layer (Armbrust et al., 2010; ENISA, 2017b). It's becoming important to know who created data, who modified it and how, and so on, for several reasons as traceback, auditing, and history-based access control (ENISA, 2017b; Takabi et al., 2010);

7) Data Mishandling: the CSP might mishandle data or be forced to give it up in response to a subpoena (Talbot, 2010). Personal data being processed in the cloud may be subject to law enforcement requests from law enforcement agencies of the EU Member States and of third

countries. There is a risk that personal data could be disclosed to (foreign) law enforcement agencies without a valid EU legal basis and thus a breach of EU data protection law would occur (Article 29 Data Protection Working Party, 2012).

8) Liability: Most CSPs come with no assurance or promise of a given level of security and privacy. CSPs have also allegedly demonstrated a tendency to reduce their liability by proposing contracts with the service provided as is with no warranty (Kshetri, 2012). It is expected that CSC will use contracts and courts, rather than clever security engineering, to guard against provider malfeasance (Armbrust et al., 2010). Also, a CSP may not provide the necessary measures and tools to assist the controller to manage the data (Article 29 Data Protection Working Party, 2012);
9) Data Transfer Bottlenecks: applications continue to become more data-intensive and if we assume applications may be "pulled apart" across the boundaries of clouds, this may complicate data placement and transport. The high costs can quickly add up, making data transfer costs an important issue. One opportunity to overcome the high cost of Internet transfers is, for instance, to ship disks (Armbrust et al., 2010; Expert Group Report, 2010);
10) Performance Unpredictability: multiple virtual machines (VMs) can share CPUs and main memory surprisingly well in cloud computing, but that network and disk I/O sharing is more problematic (Armbrust et al., 2010);
11) Bugs in Large-Scale Distributed Systems: one of the difficult challenges is removing errors in these very large-scale distributed systems, since usually these bugs cannot be reproduced in smaller configurations, so the debugging must occur at scale in the production data centers (Armbrust et al., 2010).
12) Lack of integrity caused by sharing of resources: a cloud is made up of shared systems and infrastructures. CSPs process personal data emanating from a wide range of sources in terms of data subjects and organisations and it is a possibility that conflicting interests and/or different objectives might arise (Article 29 Data Protection Working Party, 2012);
13) Lack of intervenability due to the complexity and dynamics of the outsourcing chain: the cloud service offered by one provider might be produced by combining services from a range of other providers, which may be dynamically added or removed during the duration of the client's contract (Article 29 Data Protection Working Party, 2012);
14) Lack of transparency: insufficient information about a cloud service's processing operations poses a risk to controllers as well as to data subjects because they might not be aware of potential

threats and risks and thus cannot take appropriate measures (Article 29 Data Protection Working Party, 2012).

Therefore, the lifecycle of an information system must be diligently managed to ensure that security concerns are proactively addressed at all stages (European Commission, 2019).

The common security objectives within a multiuser distributed environment proposes unique security challenges, dependent on the level at which the user operates, application, virtual or physical. The security objectives within a distributed system are:

1) to ensure the availability of information communicated between or held within participating systems;
2) to maintain the integrity of information communicated between or held within participating systems, i.e. preventing the loss or modification of information due to unauthorized access, component failure or other errors;
3) to maintain the integrity of the services provided, confidentiality and correct operation;
4) to provide control over access to services or their components to ensure that users may only services for which they are authorized;
5) to authenticate the identity of communicating partners (peer entities) and where necessary to ensure non-repudiation of data origin and delivery;
6) where appropriate, to provide secure interworking with the non-open systems world;
7) to ensure the confidentiality of information held on participating systems;
8) clear separation of data and processes on the virtual level of the cloud, ensuring zero data leakage between different applications;
9) To maintain the same level of security when adding or removing resources on the physical level (Zissis & Lekkas, 2012, p. 587)

5. ISO/IEC STANDARDS

5.1. Introduction

ISO and IEC form the specialized system for worldwide standardization (ISO/IEC, 2011, 2018b, 2019a). ISO is an independent, non-governmental international organization with a membership of 164 national standards bodies, bringing together experts to share knowledge in order to develop voluntary, consensus-based, market relevant International Standards, which support innovation and provide solutions to global challenges (ISO, n.d.-a).

National bodies that are members of ISO or IEC participate in the development of International Standards[153] through technical committees established by the respective organization to deal with specific fields of technical activity (ISO/IEC, 2018b, 2019a; ISO, n.d.-a). Nowadays, the Portuguese System for Quality (Instituto Português da Qualidade, in the original) is the national body member of ISO (ISO, n.d.-e).

ISO and IEC technical committees collaborate in fields of mutual interest, as well as with other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work (ISO/IEC, 2011, 2015, 2018b, 2019a). In fact, regulators and governments count on ISO standards to help develop better regulation, due to the involvement of globally-established experts (ISO, n.d.-b). Therefore, ISO standards provide a strong basis that can be applied in the development of national and international regulation, being essential tools for reducing barriers to international trade and save time (ISO/IEC, 2015; ISO, n.d.-f). As the benefits of using standards to support public policies have become recognized, many economies have developed policies to actively encourage their use (ISO, n.d.-g).

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2 (ISO/IEC, 2011, 2018d, 2018b, 2019a). The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote (ISO/IEC, 2011).

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1 (ISO/IEC, 2018b, 2019a; ISO, n.d.-a). Accordingly, ISO/IEC 29100 was prepared by Joint

[153] International standard - standard that is adopted by an international standardizing/standards organization and made available to the public [176]–[178]

Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques (ISO/IEC, 2018b; ISO, n.d.-a). Moreover, ISO/IEC 27018:2019 was prepared by Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques (ISO/IEC, 2019a). As a second edition, it cancels and replaces the first edition (ISO/IEC 27018:2014), of which it constitutes a minor revision (ISO/IEC, 2019a).

ISO provides conformity assessment tools, in order to consider possible conformity assessment routes and, therefore, to select the solution that better suits the desired goals (ISO, n.d.-c).

There are several key concepts and definitions that underpin conformity assessment [154] (e.g. functional approach) and that are key to understand what conformity assessment is and why it matters to consumers, manufactures, services providers and regulators (ISO, n.d.-d).

Regulations[155] often have some direct or indirect interaction with standards and conformity assessment. Also, some regulations may only specify parts of standards and can include requirements for how compliance is to be demonstrated and communicated (ISO/IEC, 2015; ISO, n.d.-d).

Thus, by relying on conformity assessment in accordance with International Standards and Guides, compliance in relation to the products, processes, services, management systems, persons or organisations is well-founded and legitimate (ISO, n.d.-d). The functional approach [156] is a basic concept inherent to the conformity assessment and can be used as a starting point when developing conformity assessment frameworks to support regulations. (ISO, n.d.-d).

[154] Conformity Assessment is the process for demonstrating that features of products/services meet the requirements of standards, regulations and other specifications. There are different conformity assessment techniques (i.e. assessment, auditing, calibration, evaluation, examination, inspection and testing). These conformity assessment activities can result in different claims of conformity such as supplier's declaration of conformity, certification or accreditation. (ISO, n.d.-d)

[155] It is important to enhance that a regulation is different from a technical regulation: the second provides technical requirements, either directly or by referring to or incorporating the content of a standard, technical specification or code of practice. (ISO, n.d.-h)

[156] The functional approach here described is a specific approach concerning the conformity assessment as described by ISO, being non-related with the functional approach regarding the comparative method from law research.

5.2. ISO/IEC 29100 Privacy Framework and the ISO/IEC 27000 ISMS family of standards

5.2.1. ISO/IEC 29100 Privacy Framework

The ISO/IEC 29100:2011 Privacy Framework amended by the ISO/IEC 29100:2018 document[157] provides a high-level framework for the protection of PII within ICT systems. Being general in nature, it places organizational, technical, and procedural aspects in an overall privacy framework (ISO/IEC, 2011). This framework has as objective to help organizations define their privacy safeguarding requirements[158] related to PII within an ICT environment by: "specifying a common privacy terminology; defining the actors and their roles in processing PII; describing privacy safeguarding requirements; and referencing known privacy principles" (ISO/IEC, 2011, p. vi).

The following components make up the privacy framework described in this International Standard: 1) actors and roles; 2) interactions; 3) recognizing PII; 4) privacy safeguarding requirements; 5) privacy policies; and 6) privacy controls (ISO/IEC, 2011).

The ISO/IEC 29101:2018 describes a high-level architecture framework and associated controls for the safeguarding of privacy in ICT systems that store and process PII (ISO/IEC, 2018c). The framework described in this standard: "1) provides a consistent, high-level approach to the implementation of privacy controls for the processing of PII in ICT systems; 2) provides guidance for planning, designing and building ICT system architectures that safeguard the privacy of PII principals by controlling the processing, access and transfer of PII; and 3) shows how PETs can be used as privacy controls" (ISO/IEC, 2018c, p. v). Moreover, it helps an organization to define its privacy safeguarding requirements as they relate to PII processed by any ICT system (ISO/IEC, 2018c).

The ISO/IEC 29151:2017 has as objective to enable organizations to put in place a set of controls as part of their overall PII protection programme. They can be used in a framework for maintaining and improving compliance with privacy-related laws and regulations, managing privacy risks and meeting the expectations of PII principals, regulators or clients, in accordance with the privacy principles described in ISO/IEC 29100. It is a specification that offers guidance for PII controllers on a broad range of information

[157] For further considerations, it will be used the expression ISO/IEC 29100, being already considered the amendment made in 2018.

[158] In some countries, privacy safeguarding requirements are synonymous with data protection/privacy requirements and are subject of data protection/privacy legislation (ISO/IEC, 2018c).

security and PII protection controls that are applied in many different organizations that deal with protection of PII (ISO/IEC, 2017c).

5.2.2. ISO/IEC 27000 ISMS family of standards

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets (ISO/IEC, 2018a). Therefore, "the ISMS family of standards includes standards that: a) define requirements for an ISMS and for those certifying such systems; b) provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain, and improve an ISMS; c) address sector-specific guidelines for ISMS; and d) address conformity assessment for ISMS"(ISO/IEC, 2018a, Chapter 0.2).

The most commonly used standards within this family are ISO/IEC 27001:2013 and the related ISO/IEC 27002:2013. The first one specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization, as well as it includes requirements for the assessment and treatment of information security risks considering the needs of the organization (ISO/IEC, 2013a). The second provides guidelines for organizational information security standards and information security management practices, including the selection, implementation and management of controls, taking into consideration the organization's information security risk environment(s) (ISO/IEC, 2013b). Even though they are the more commonly used, they do not specifically consider privacy nor data protection. Therefore, both standards ISO/IEC 27018:2019 and ISO/IEC 27701:2019 will be subject to further analysis taking into account privacy management as well as protection of PII on public clouds (ISO/IEC, 2019a, 2019b).

The ISO/IEC 27701:2019 "specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization" (ISO/IEC, 2019b, Chapter 1).

The intention of ISO/IEC 27018 is to create a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor. It has the following objectives:

> to help the public CSP to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract; to enable the public cloud PII processor to be transparent in relevant matters so that CSCs can select well-governed cloud-based PII processing services; to assist the CSC and the public cloud PII processor in entering

> into a contractual agreement; to provide CSCs with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual CSC audits of data hosted in a multi-party, virtualized server (cloud) environment can be impractical technically and can increase risks to those physical and logical network security controls in place (ISO/IEC, 2019a, p. vii).

ISO/IEC 27018 gives further information for organizations acting as PII processors and providing public cloud services. ISO/IEC 29151 gives additional controls and guidance for the processing of PII by PII controllers.

Therefore, requirements and controls of ISO/IEC 27701 can have some correspondence with provisions from ISO/IEC 27018 and/or ISO/IEC 29151 (ISO/IEC, 2019b).

5.2.3. Scope

5.2.3.1.ISO/IEC 29100 and ISO/IEC 29101

The ISO/IEC 29100 framework is intended to help organizations define their privacy safeguarding requirements related to PII within an ICT environment by: "specifying a common privacy terminology; defining the actors and their roles in processing PII; describing privacy safeguarding requirements; and referencing known privacy principles" (ISO/IEC, 2011, p. vi).

In some jurisdictions, this document's references to privacy safeguarding requirements might be understood as being complementary to legal requirements for the protection of PII (ISO/IEC, 2011, 2018b). Nevertheless, some jurisdictions might require compliance with one or more of the documents referenced in ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — Official Privacy Documents References or with other applicable laws and regulations. Therefore, this document is not intended to be a global model policy, nor a legislative framework (ISO/IEC, 2011, 2018b).

The purpose of WP 5 Standing Document 2 is to provide introductory guidance on privacy-related references to assist individuals, organizations and regulatory authorities in: a) identifying the adequate documentation to privacy issues, initiatives and risks. b) developing privacy policies and practices (ISO/IEC JTC 1/SC 27/WG 5 & Information, 2017).

It is important to point out that Portugal is one of the considered countries on the above described document, being considered as important laws and regulations concerning personal data: 1) Article 35 of the Constitution of the Portuguese Republic - use of information technology; 2) Law 67/98 - Personal

Data Protection Act[159]; 3) Law 103/2015 - adds article 45-A - The insertion of false data - to Law 67/98[160]; 4) Law 2/94 - Establishes the control and monitoring mechanisms of the Schengen Information System; 5) Law 68/98 - National entity in the Joint Supervisory Body of EUROPOL; 6) Law 36/2003 - Regulates the status and powers of the national member of EUROJUST[161]; 7) Law 43/2004[162] - Law on the organization and operation of CNPD (ISO/IEC JTC 1/SC 27/WG 5 & Information, 2017).

Regarding electronic communications, the same document refers: 1) Decree-Law 7/2004 - E-Commerce; 2) Law 41/2004 - Regulates the protection of personal data in the electronic communications sector - (amended and republished); 3) Law 46/2012 - Amends Law 41/2004 and Decree-Law 7/2004; 4) Regulation (EU) No 611/2013 - Measures applicable to the notification of breaches of personal data in accordance with Directive 2002/58 / EC of the European Parliament and of the Council on privacy and electronic communications; 5) Law 32/2008 - Transposes the Data Retention Directive on the retention of electronic communications data; 6) Law 5/2004 - Provides for the creation of a database of debtor subscribers of electronic communications services (altered and republished) (ISO/IEC JTC 1/SC 27/WG 5 & Information, 2017).

For video surveillance, there are the following references: 1) Law 34/2013 – Use of video surveillance systems by private security and autoprotection services[163]; 2) Ordinance 273/2013 - Regulates Law 34/2013; 3) Law 1/2005[164] – Regulates video surveillance systems in use by the law enforcement forces in public places; 4) Decree-Law 207/2005 – Regulates the means of roads electronic surveillance used by the security forces; 5) Law 51/2006 – Regulates the use of road surveillance systems by the EP and the road concessionaires; 6) Law 33/2007 - Regulates the installation and use of video surveillance systems in taxis; 7) Ordinance 1164-A / 2007 - Approves the model of video surveillance notice in taxis (ISO/IEC JTC 1/SC 27/WG 5 & Information, 2017). It is also referred the Law 7/2009, which approves the Labor Code, the Law 7/2007, which creates citizen's card and governs its issuance and use; Law 109/2009 - Cybercrime Law and Law 12/2005, regarding personal health genetic information (ISO/IEC JTC 1/SC 27/WG 5 & Information, 2017).

The increasing number of ICTs that process PII enhances the importance to have international information security standards that provide a common understanding for the protection of PII. Thus, the ISO/IEC

[159] Already replaced by Law 58/2019.

[160] Already replaced by Law 58/2019.

[161] Already replaced by Law 20/2014.

[162] With the alterations provided by the Law 58/2019.

[163] Already replaced by Law 46/2019.

[164] With the alterations provided by the Law 9/2012.

29100 is intended to improve existing security standards by adding a focus to the processing of PII (ISO/IEC, 2011).

Considering the same global context that brought the need of GDPR, or even broader since it surpasses the European context, such as the increasing commercial use and value of PII, the sharing of PII across legal jurisdictions, and the growing complexity of ICT systems, it may become difficult for an organization to ensure privacy and to achieve compliance with the various applicable laws (ISO/IEC, 2011). Consequently, this standard aims to: 1) help in the design, implementation, operation, and maintenance of ICT systems that handle and protect PII; 2) outgrowth innovative solutions to enable the protection of PII within ICT systems; and 3) improve organizations' privacy programs through the use of best practices (ISO/IEC, 2011). Moreover, this framework can serve as a basis for additional privacy standardization initiatives, such as for: "1) a technical reference architecture; 2) the implementation and use of specific privacy technologies and overall privacy management; 3) privacy controls for outsourced data processes; 4) privacy risk assessments; or 5) specific engineering specifications" (ISO/IEC, 2011, p. vi).

The ISO/IEC 29100 is applicable to "natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII" (ISO/IEC, 2011, Chapter 1).

The ISO/IEC 29101 "defines a privacy architecture framework that: specifies concerns for ICT systems that process PII; lists components for the implementation of such systems; and provides architectural views contextualizing these components" (ISO/IEC, 2018c, Chapter 1). It is primarily focused on ICT systems that are designed to interact with PII principals, being applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating ICT systems that process PII (ISO/IEC, 2018c). Thus, this architecture framework focuses on the protection of PII and since this is partly a security objective, ICT systems processing PII should also adhere to information security engineering guidelines (ISO/IEC, 2018c). Therefore, some information security components that are critical for safeguarding PII processed within ICT systems will also be considered.

It is important to refer that an ICT system can contain components from the privacy architecture framework as well as other components that do not process PII, but instead handle other functionality in the ICT system like providing accessibility or rendering special user interfaces (ISO/IEC, 2018c). Such components are out of the scope of the present study.

5.2.3.2.ISO/IEC 29134

The ISO/IEC 29134 gives guidelines for a process on privacy impact assessments, and a structure and content of a PIA report, being applicable to all types and sizes of organizations. It is particularly relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII (ISO/IEC, 2017b).

5.2.3.3.ISO/IEC 29151

The ISO/IEC 29151 establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of PII. It specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII that may be applicable within the context of an organization's information security risk environment(s), being applicable to all types and sizes of organizations acting as PII controllers (ISO/IEC, 2017c).

5.2.3.4.ISO/IEC 27701

The ISO/IEC 27701 specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a PIMS in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002. Therefore, it specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing, being applicable to all types and sizes of organizations, as well as both PII controllers and/or PII processors (ISO/IEC, 2019b).

5.2.3.5.ISO/IEC 27018

The ISO/IEC 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect PII in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment, specifying guidelines based on ISO/IEC 27002 and taking into consideration the regulatory requirements for the protection of PII (ISO/IEC, 2019a). Moreover, it is applicable to all types and sizes of organizations, which are PII processors, via cloud computing under contract to other organizations (ISO/IEC, 2019a). Nevertheless, the guidelines in ISO/IEC 27018 can also be relevant to organizations acting as PII controllers. Considering that PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors, this document does not cover such additional obligations (ISO/IEC, 2019a).

5.2.4. Definitions

The following concepts, that will be subject to a further analysis when compared to the GDPR's definitions, are mainly stipulated on ISO/IEC 29100, but relevant definitions part of the other standards will also be considered (ISO/IEC, 2011):

1) acceptance statement – "formal management declaration to assume responsibility for risk ownership, risk treatment and residual risk" (ISO/IEC, 2017b, Chapter 3.1)
2) anonymity – "characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly" (ISO/IEC, 2011, Chapter 2.1);
3) anonymization – "process by which PII is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party" (ISO/IEC, 2011, Chapter 2.2);
4) anonymized data – "data that has been produced as the output of a personally identifiable information anonymization process" (ISO/IEC, 2011, Chapter 2.3);
5) asset – "anything that has value to anyone involved in the processing of personally identifiable information (PII). In the context of a privacy risk management process, an asset is either PII or a supporting asset." (ISO/IEC, 2017b, Chapter 3.2);
6) chief privacy officer (CPO) – "senior management individual who is accountable for the protection of personally identifiable information (PII) in an organization" (ISO/IEC, 2017c, p. 1);
7) consent – "PII principal's freely given, specific and informed agreement to the processing of their PII" (ISO/IEC, 2011, Chapter 2.4);
8) data breach – "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data transmitted, stored or otherwise processed" (ISO/IEC, 2019a, Chapter 3.1);
9) device – "combination of hardware and software, or solely software, that allows a user to perform actions" (ISO/IEC, 2017b, Chapter 3.5);
10) identifiability – "condition which results in a PII principal being identified, directly or indirectly, on the basis of a given set of PII" (ISO/IEC, 2011, Chapter 2.5);
11) joint PII controller - PII controller that determine the purposes and means of the processing of PII jointly with one or more other PII controllers (ISO/IEC, 2019b, p. 1);
12) opt-in – "process or type of policy whereby the PII principal is required to take an action to express explicit, prior consent for their PII to be processed for a particular purpose" (ISO/IEC, 2011,

Chapter 2.8). On the other hand, there is also the term "opt-out", which is often used with the privacy principle "consent and choice" and it describes a process or type of policy whereby the PII principal is required to take a separate action in order to withhold or withdraw consent, or oppose a specific type of processing. The use of an opt-out policy presumes that the PII controller has the right to process the PII in the intended way and this right can be implied by some action of the PII principal different from consent (ISO/IEC, 2011);

13) organization:

> person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives. The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private (ISO/IEC, 2017b, Chapter 3.11);

14) personally identifiable information (PII) – "any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person" (ISO/IEC, 2018b, Chapter 2.9). Just a note was added on ISO/IEC 27018: "A public cloud PII processor is typically not in a position to know explicitly whether information it processes falls into any specified category unless this is made transparent by the CSC." (ISO/IEC, 2019a, Chapter 3.2);

15) PII controller:

privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing PII other than natural persons who use data for personal purposes. A PII controller sometimes instructs others (e.g., PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller (ISO/IEC, 2011, Chapter 2.10).

16) PII principal – "natural person to whom the PII relates. Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal" (ISO/IEC, 2011, Chapter 2.11). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the PII controller holding the data, or by any other party, to establish the link between the set of PII and the natural person (ISO/IEC, 2018b);

17) PII processor – “privacy stakeholder that processes PII on behalf of and in accordance with the instructions of a PII controller” (ISO/IEC, 2011, Chapter 2.12);

18) privacy breach – “situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements” (ISO/IEC, 2011, Chapter 2.13);

19) privacy controls – measures that treat privacy risks by reducing their likelihood or their consequences, including organizational, physical and technical measures (e.g., policies, procedures, guidelines, legal contracts, management practices or organizational structures). Control is also used as a synonym for safeguard or countermeasure (ISO/IEC, 2011, Chapter 2.14);

20) privacy enhancing technology (PET)

privacy control, consisting of ICT measures, products, or services that protect privacy by eliminating or reducing PII or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system. Examples of PETs include, but are not limited to, anonymization and pseudonymization tools that eliminate, reduce, mask[165], or de-identify PII or that prevent unnecessary, unauthorized and/or undesirable processing of PII (ISO/IEC, 2011, Chapter 2.15);

21) privacy impact – “anything that has an effect on the privacy of a PII principal and/or group of PII principals. The privacy impact could result from the processing of PII in conformance or in violation of privacy safeguarding requirements.”(ISO/IEC, 2017b, Chapter 3.6);

22) privacy impact assessment – “overall process of identifying, analyzing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of PII, framed within an organization's broader risk management framework” (ISO/IEC, 2017b, Chapter 3.7, 2018b, Chapter 2.20);

23) privacy information management system (PIMS) – “information security management system which addresses the protection of privacy as potentially affected by the processing of PII” (ISO/IEC, 2019b, Chapter 3.2);

24) privacy policy – “overall intention and direction, rules and commitment, as formally expressed by the PII controller related to the processing of PII in a particular setting” (ISO/IEC, 2011, Chapter 2.16);

25) privacy preferences – “specific choices made by a PII principal about how their PII should be processed for a particular purpose” (ISO/IEC, 2011, Chapter 2.17);

[165] Masking is the process of obscuring elements of PII (ISO/IEC, 2011)

26) privacy principles – “set of shared values governing the privacy protection of PII when processed in ICT systems” (ISO/IEC, 2011, Chapter 2.18);

27) privacy risk – “effect of uncertainty[166] on privacy” (ISO/IEC, 2011, Chapter 2.19);

28) privacy risk map – “diagram that indicates the level of impact and likelihood of privacy risks identified. The map is typically used to determine the order in which the privacy risks should be treated.” (ISO/IEC, 2017b, Chapter 3.8);

29) privacy safeguarding requirements – “set of requirements an organization has to take into account when processing PII with respect to the privacy protection of PII” (ISO/IEC, 2011, Chapter 2.21);

30) privacy stakeholder – “natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to PII processing” (ISO/IEC, 2011, Chapter 2.22);

31) process – “set of interrelated or interacting activities which transforms inputs into outputs” (ISO/IEC, 2017b, Chapter 3.4)

32) processing of PII – “operation or set of operations performed upon PII, which include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII” (ISO/IEC, 2011, Chapter 2.23);

33) pseudonymization:

process applied to PII which replaces identifying information with an alias. Pseudonymization can be performed either by PII principals themselves or by PII controllers. Nevertheless, pseudonymization does not exclude the possibility that there might be (a restricted set of) privacy stakeholders other than the PII controller of the pseudonymized data which are able to determine the PII principal’s identity based on the alias and data linked to it (ISO/IEC, 2011, Chapter 2.24);

34) public cloud service provider - party which makes cloud services available according to the public cloud model (ISO/IEC, 2019a, p. 2).

35) secondary use – processing of PII in conditions which differ from the initial ones (e.g. it could involve a new purpose for processing PII, a new recipient of the PII, etc.) (ISO/IEC, 2011, Chapter 2.25);

[166] Uncertainty “is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood” (ISO/IEC, 2011, p. 3);

36) sensitive PII:

category of PII, either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal. In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that might be defined as sensitive (ISO/IEC, 2011, Chapter 2.26);

37) severity – "estimation of the magnitude of potential impacts on the privacy of a PII principal" (ISO/IEC, 2017b, Chapter 3.12);
38) system information system – "applications, services, information technology assets, or other information handling components" (ISO/IEC, 2017b, Chapter 3.13);
39) stakeholder – "person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. It includes PII principals, management, regulators and customers. Consultation with stakeholders is integral to a PIA." (ISO/IEC, 2017b, Chapter 3.14);
40) technology – "hardware, software, and firmware systems and system elements including, but not limited to, information technology, embedded systems, or any other electro-mechanical or processor-based systems" (ISO/IEC, 2017b, Chapter 3.15);
41) third party – "privacy stakeholder other than the PII principal, the PII controller and the PII processor, and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor" (ISO/IEC, 2011, Chapter 2.27).

5.2.5. PII

To determine whether or not PII is being dealt with, the following elements should be considered: 1) identifiers; 2) other distinguishing characteristics; 3) information which is or might be linked to a PII principal; 4) pseudonymous data; 5) metadata; 6) unsolicited PII; 7) sensitive PII (ISO/IEC, 2011). Regarding identifiers, information can be considered to be PII in at least the following instances:

if it contains or is associated with an identifier which refers to a natural person (e.g., a social security number); if it contains or is associated with an identifier which can be related to a natural person (e.g., a passport number, an account number); if it contains or is associated with an identifier which can be used to establish a communication with an identified natural person (e.g., a precise geographical location, a telephone number); or if it contains a reference which links the data to any of the identifiers above (ISO/IEC, 2011, Chapter 4.4.1).

When considering other distinguishing characteristics, that means that information does not necessarily need to be associated with an identifier in order to be considered PII: any attribute which takes on a value which uniquely identifies a PII principal is to be considered as a distinguishing characteristic. Sometimes a given characteristic may distinguish a natural person from other natural persons depending on the context of use. In addition, there can also be situations in which a natural person is identifiable where a combination of several attributes taken together distinguishes this natural person from other natural persons (ISO/IEC, 2011).

In regard to information which is or might be linked to a PII principal, it needs to be decided if the information discloses something about this natural person. Nevertheless, if the relationship with an identifiable natural person may be established, such information must also be treated as PII (ISO/IEC, 2011).

Pseudonymous data are identity information replaced by aliases, in order to restrict the ability of PII controllers and processors to identify the PII principal. The substitution is considered pseudonymization[167] if:

a) the remaining attributes linked to the alias do not suffice to identify the PII principal to whom they relate; and b) the alias assignment is such that it cannot be reversed by reasonable efforts of the privacy stakeholders other than those that performed them (ISO/IEC, 2011, Chapter 4.4.4).

However, pseudonymization retains linkability, since different data associated with the same pseudonym can be linked. Attributes contained directly in the information in question and attributes that can be easily linked to this information should be considered when determining whether or not the information relates to an identifiable natural person (ISO/IEC, 2011).

Metadata refers to data that define and describe other data, in particular, to PII that can be stored in an ICT system in such a way that it is not readily visible to the system user (ISO/IEC, 2011; ISO/IEC JTC 1/SC 27, 2018).

It also might happen that PII that was unsolicited by a PII controller or PII processor (i.e. unintentionally obtained) is stored in an ICT system – unsolicited PII. The inherent risk of collecting unsolicited PII can be reduced by considering privacy safeguarding measures at the time of the design of the system (also referred to as the concept of "privacy by design") (ISO/IEC, 2011).

[167] Pseudonymization is different from with anonymization, since the second destroys linkability. During anonymization, identity information is either erased or substituted by aliases for which the assignment function or table is destroyed, which means that anonymized data is no longer PII. (ISO/IEC, 2011)

Sensitivity extends to all PII from which sensitive PII can be obtained [168].

5.2.6. Sensitive PII

Sensitivity extends to all PII from which sensitive PII can be obtained, which would include direct and/or indirect information about the PII principal's sexual orientation or health (ISO/IEC, 2011).

In some jurisdictions, what constitutes sensitive PII is explicitly defined in legislation, and it might include information revealing race, ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, sexual lifestyle or orientation, and the physical or mental health of the PII principal, information that could facilitate identity theft or otherwise result in significant financial harm to the natural person, and information that could be used to identify the PII principal's real time location (ISO/IEC, 2011).

Therefore, the processing of sensitive PII requires special precautions, since in some jurisdictions the processing of sensitive PII might be prohibited by applicable law even with the PII principal's consent, and on another ones, it might require the implementation of specific controls where certain types of sensitive PII are processed (ISO/IEC, 2011).

5.2.7. Principles

The privacy principles described in this standard were derived from existing principles developed by several countries and international organizations. The privacy principles should be implemented in ICT systems and on the development of privacy management systems to be implemented within the organization's ICT systems. Moreover, these privacy principles should be used to guide the design, development, and implementation of privacy policies and privacy controls and used as a baseline in the monitoring and measurement of performance, benchmarking and auditing aspects of privacy management programs in an organization (ISO/IEC, 2011, 2018b).

Despite the differences in social, cultural, legal, and economic factors that can limit the application of these principles in some contexts, the application of all the principles is recommended and exceptions to these principles should be limited (ISO/IEC, 2011).

The ISO/IEC 29100 is formed by 11 privacy principles: 1) consent and choice; 2) purpose legitimacy and specification; 3) collection limitation; 4) data minimization 5) use, retention and disclosure limitation; 6)

[168] The next chapter will provide detailed information about this particular PII.

accuracy and quality; 7) openness, transparency and notice; 8) individual participation and access; 9) accountability; 10) information security; 11) privacy compliance (ISO/IEC, 2011, 2018c).

5.2.7.1.Principle of consent and choice

Organizations should provide the means necessary for PII principals to exercise meaningful, informed, unambiguous and freely given consent except where the PII principal cannot freely refuse consent or where applicable law specifically allows the processing of PII without the principal's consent (ISO/IEC, 2017c), since other lawful grounds apply (ISO/IEC, 2019b).

The principle of consent implies:

- to present to the PII principal the choice whether or not to allow the processing of their PII except where the PII principal cannot freely withhold consent or where applicable law specifically allows the processing of PII without the natural person's consent. The PII principal's choice must be given freely, specific regarding the purpose for processing, unambiguous and explicit and on a knowledgeable basis;
- to obtain the opt-in consent of the PII principal for collecting or otherwise processing sensitive PII except where applicable law allows the processing of sensitive PII without the natural person's consent;
- to inform PII principals, before obtaining consent, about their rights under the individual participation and access principle;
- to provide PII principals, before obtaining consent, with the information indicated by the openness, transparency and notice principle; and
- to explain to PII principals the implications of granting or withholding consent (ISO/IEC, 2011).

The ISO/IEC 29151 has one specific control related to this principle:

Consent - organizations should provide the means necessary for PII principals to exercise meaningful, informed, unambiguous and freely given consent except where the PII principal cannot freely refuse consent or where applicable law specifically allows the processing of PII without the principal's consent (ISO/IEC, 2017c, Chapter A.3.1).

Besides, provisions should be taken to provide PII principals with the opportunity to choose how their PII is handled and to allow a PII principal to withdraw consent easily and free of charge. The privacy policy should describe how the request should be done (ISO/IEC, 2011).

Subject to applicable law, organizations should obtain consent through opt-in or implied consent. Opt-in consent is the preferred method, but since it is not always feasible, with opt-out mechanisms, organizations can assume that the PII principal has implicitly consented to the processing of their PII, unless the PII principal takes affirmative action to signal otherwise (ISO/IEC, 2017c). If consent is withdrawn, but the PII controller needs to retain certain PII for a period of time in order to comply with legal or contractual obligations or the PII processing is not based on consent but instead on another legal basis, the PII principal should be notified wherever possible (ISO/IEC, 2011).

Some jurisdictions provide PII principals with a right to object to the processing of their PII. Therefore, organizations under to such jurisdictions should ensure that they implement appropriate measures to enable PII principals to exercise this right, as well as they should document the legal and regulatory requirements related to objections by the PII principals to processing. Furthermore, they should provide information to principals regarding the ability to object in these situations (ISO/IEC, 2019b).

The choice principle, related with the consent, means that the PII controller needs to:

- provide PII principals with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice and to give consent in relation to the processing of their PII at the time of collection, first use or as soon as practicable thereafter; and
- implement the PII principal's preferences as expressed in their consent (ISO/IEC, 2011).

The ISO/IEC 29151 has one specific control related to this principle:

Choice - organizations should provide PII principals with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice with respect to the processing of their PII except where the PII principal cannot freely withhold consent or where applicable law specifically allows the processing of PII without the PII principal's consent (ISO/IEC, 2017c, Chapter A.3.2).

Applicable law in some situations provides that the consent of the PII principal does not constitute a sufficient legal basis to process PII (e.g., the consent of a minor given without a parent or guardian's approval). Also, additional requirements on transferring PII internationally are to be considered, since it is the responsibility of the PII controller to comply with these additional provisions before processing or transferring data (ISO/IEC, 2011).

5.2.7.2. Purpose legitimacy and specification principle

The purpose legitimacy and specification principle determines that:

- the purpose(s) complies with applicable law and relies on a permissible legal basis;
- the purpose(s) has to be communicated to the PII principal before the time the information is collected or used for the first time for a new purpose;
- language for this specification is both clear and appropriately adapted to the circumstances; and
- if applicable, sufficient explanations for the need to process sensitive PII should be given (ISO/IEC, 2011).

The ISO/IEC 29151 has two specific controls related to this principle:

1) Purpose legitimacy – "organizations should implement appropriate measures to ensure that PII processing complies with applicable law and relies on a permissible legal ground" (ISO/IEC, 2017c, Chapter A.4.1);
2) Purpose specification:

organizations should communicate to the PII principal from whom they are going to collect PII, the purpose(s) for which that PII is being collected and the purpose(s) for which the PII will be processed. Such communication should take place at or before the PII is collected and before the PII is processed for any purpose(s) not previously communicated to the PII principal (ISO/IEC, 2017c, Chapter A.4.2).

Some jurisdictions require the organization to be able to demonstrate that the lawfulness of processing was duly established before the processing (ISO/IEC, 2019b).

The legal basis for the processing of PII might include: "consent from PII principals; performance of a contract; compliance with a legal obligation; protection of the vital interests of PII principals; performance of a task carried out in the public interest; legitimate interests of the PII controller" (ISO/IEC, 2019b, Chapter 7.2.2). The legitimate interests of the organization should be balanced against the obligations to PII principals with regards to privacy protection (ISO/IEC, 2019b).

Whenever special categories of PII are defined, either by the nature of the PII or by the PII principals concerned, the organization should include those categories of PII in its classification schemes. The classification of PII that falls into these categories has to consider the legal and regulatory obligations that the organization must follow, so the organization needs to be aware of the classification(s) that apply to the PII processing being performed (ISO/IEC, 2019b).

Stricter rules can apply to the purpose of processing sensitive PII. Moreover, a purpose can require a legal basis or a specific authorization by a data protection authority or a government authority. If the purpose(s) for processing PII does not conform to applicable law, processing should not take place (ISO/IEC, 2011, 2019b).

5.2.7.3.Collection limitation and data minimization principles

The collection limitation principle imposes a restriction on the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s). It means that both the amount and the type of PII collected should be limited to that which is necessary to fulfil the legitimate purpose(s) specified by the PII controller. Also, organizations should document the type of PII collected, as well as their justification for doing so as part of their information-handling policies and practices (ISO/IEC, 2011).

The data minimization principle means designing and implementing data processing procedures and ICT systems in order to:

- minimize the PII which is processed and the number of privacy stakeholders and people to whom PII is disclosed or who are allowed to process it;
- ensure adoption of a "need-to-know" principle;
- use or offer as default options, wherever possible, interactions and transactions which do not involve the identification of PII principals, as well as reduce the observability of their behaviour and limit the linkability of the PII collected; and
- securely dispose of PII whenever it is practical to do so, in particular when the purpose for PII processing has expired and where there are no legal requirements to keep it.(ISO/IEC, 2011, 2018b).

The ISO/IEC 29151 has two specific controls related to this principle:

1) Collection limitation – "organizations should implement appropriate measures to limit the collection of the type and amount of PII to the minimum elements for the purposes described in the notice and to that which is within the bounds of applicable laws and regulations" (ISO/IEC, 2017c, Chapter A.5);
2) Data minimization – "organizations should implement appropriate measures to minimize the amount of PII being processed to that which is strictly necessary for the legitimate interests of the PII controller" (ISO/IEC, 2017c, Chapter A.6).

The organization should limit the collection of PII to what is adequate, relevant and necessary in relation to the identified purposes, including the amount of PII that the organization collects indirectly. Thus, the "need-to-know" principle should be adopted and data minimization techniques must be applied. Processing of PII, including the disclosure, the period of PII storage; and who is able to access their PII, should be limited by default to the minimum necessary relative to the identified purposes (ISO/IEC, 2019b).

Mechanisms used to minimize PII vary depending on the type of processing and the systems used for the processing and, in accordance, the organization should document any mechanisms used to implement data minimization (ISO/IEC, 2019b).

5.2.7.4. Use, retention and disclosure limitation principle

The use, retention and disclosure limitation principle states that:

- the use, retention and disclosure (including transfer) of PII should be limited to that which is necessary in order to fulfil specific, explicit and legitimate purposes;
- the use of PII should be limited to the purposes specified by the PII controller prior to collection, unless a different purpose is explicitly required by applicable law;
- the PII should be retained only as long as necessary to fulfil the stated purposes, and thereafter securely destroying or anonymizing it; and
- any PII should be locked (i.e. archived, secured and exempted the PII from further processing) when and for as long as the stated purposes have expired, but where retention is required by applicable laws (ISO/IEC, 2011).

The ISO/IEC 29151 has three specific controls related to this principle:

1) Use, retention and disclosure limitation – "organizations should implement appropriate measures to limit the processing of PII for legitimate and intended purposes and to retain PII only as long as necessary to fulfil the stated purposes or to abide by applicable laws" (ISO/IEC, 2017c, Chapter A.7.1);
2) Secure erasure of temporary files – "temporary files and documents that may contain PII should be disposed of within a specified, documented period" (ISO/IEC, 2017c, Chapter A.7.2);
3) Recording of PII disclosures – "Disclosures of PII to third parties should be recorded, including which PII has been disclosed, to whom, at what time and for which purpose" (ISO/IEC, 2017c, Chapter A.7.4).

5.2.7.5. Accuracy and quality principle

The accuracy and quality principle indicates that should be:

- ensured that the PII processed is accurate, complete, up-to-date, adequate and relevant for the purpose of use;
- ensured the reliability of PII collected from a source other than from the PII principal before it is processed;
- verified, through appropriate means, the validity and correctness of the claims made by the PII principal prior to making any changes to the PII, where it is appropriate to do so;
- established PII collection procedures to help ensure accuracy and quality; and
- established control mechanisms to periodically check the accuracy and quality of collected and stored PII (ISO/IEC, 2011).

The ISO/IEC 29151 has one specific control related to this principle:

Accuracy and quality – "organizations should implement appropriate measures to ensure that PII collected from a PII principal, either directly or indirectly, is of appropriate quality" (ISO/IEC, 2017c, Chapter A.8).

5.2.7.6.Openness, transparency and notice principle

The openness, transparency and notice principle implies to:

- provide PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices regarding the processing of PII;
- include in notices the fact that PII is being processed, its purpose, the types of privacy stakeholders to whom the PII might be disclosed, and the identity of the PII controller including information on how to contact the PII controller;
- disclose the choices and means offered by the PII controller to PII principals for the purposes of limiting the processing of, and for accessing, correcting and removing their information; and
- give notice to the PII principals when major changes in the PII handling procedures occur (ISO/IEC, 2011).

The ISO/IEC 29151 has two specific controls related to this principle:

1) Privacy notice – "organizations should implement appropriate measures to provide PII principals with appropriate notice of the purposes of PII processing" (ISO/IEC, 2017c, Chapter A.9.1);

2) Openness and transparency – “organizations should implement appropriate measures to provide PII principals with appropriate information about their PII processing policies, procedures and practices with respect to the handling of PII” (ISO/IEC, 2017c, Chapter A.9.2).

Privacy stakeholders who process PII should make specific information about their policies and practices relating to their management of PII available to the public and all contractual obligations that impact PII processing should be documented and communicated internally as appropriate. The extent of those obligations which are not confidential should also be communicated externally (ISO/IEC, 2011).

It should be made clear to the PII principal:

- the specified PII required for the specified purpose;
- the specified purpose for PII collection;
- the specified processing (including collection, communication and storage mechanisms);
- information about the lawful basis for the processing;
- information on where the PII was obtained, if not obtained directly from the PII principal;
- information on obligations and right to PII principals;
- contact details for the PII controller or its representative;
- the types of authorized natural persons who will access the PII and to whom the PII can be transferred; and
- the specified PII retention and disposal requirements (ISO/IEC, 2011, 2018b, 2019b).

5.2.7.7. Individual participation and access principle

The individual participation and access principle indicates to:

- give PII principals the ability to access and review their PII, being their identity firstly authenticated with an appropriate level of assurance, and such access is not prohibited by law;
- allow PII principals to verify the accuracy and completeness of the PII and have it amended, corrected or removed as appropriate and possible in the specific context;
- provide any amendment, correction or removal to PII processors and third parties to whom PII had been disclosed, where they are known; and
- establish procedures to enable PII principals to exercise these rights in a simple, fast and efficient way, which does not involve undue delay or cost (ISO/IEC, 2011, 2018b).

The ISO/IEC 29151 has three specific controls related to this principle:

1) PII principal access – “appropriate measures should be implemented by organizations to provide PII principals with the ability to have access to their PII, and to obtain rectification of the PII or deletion of the PII” (ISO/IEC, 2017c, Chapter A.10.1);
2) Redress and participation

unless prohibited by relevant legislation or regulation, organizations should implement appropriate measures to provide PII principals with the ability to correct, amend or delete PII maintained by organizations. Organization should also establish a mechanism by which any corrections, amendments or deletions are notified to PII processors and, as far as possible, to third parties to whom PII had been disclosed (ISO/IEC, 2017c, Chapter A.10.2);

3) Complaint management – “organizations should implement appropriate measures to efficiently handle complaints received from PII principals” (ISO/IEC, 2017c, Chapter A.10.3).

The PII controller should apply controls to ensure that PII principals only access to their own PII, unless the natural person accessing is acting under authority on behalf of a PII principal. Applicable law can provide the natural person with the right to access, review and object to the processing of PII under certain circumstances (ISO/IEC, 2011).

5.2.7.8.Accountability principle

The accountability principle, enhancing duty of care and the adoption of concrete and practical measures for the protection of PII, requires to:

- document and communicate as appropriate all privacy-related policies, procedures and practices;
- assign to a specified individual within the organization (who might subdelegate) the task of implementing the privacy-related policies, procedures and practices;
- when transferring PII to third parties, ensure that the third-party recipient will guarantee an equivalent level of privacy protection through contractual or other means such as mandatory internal policies (applicable law can contain additional requirements regarding international data transfers);
- provide suitable training for the personnel of the PII controller who will have access to PII;
- set up efficient internal complaint handling and redress procedures for use by PII principals;
- inform PII principals about privacy breaches that can lead to substantial damage to them (unless prohibited) as well as the measures taken for resolution;

- notify all relevant privacy stakeholders about privacy breaches as required in some jurisdictions and taking into consideration the level of risk;
- allow an aggrieved PII principal access to appropriate and effective sanctions and/or remedies, such as rectification, expungement or restitution if a privacy breach has occurred; and
- consider procedures for compensation for situations in which it will be difficult or impossible to restitute the natural person's privacy status back to a position as if nothing had occurred (ISO/IEC, 2011).

The ISO/IEC 29151 has six specific controls related to this principle:

1) Governance – "organizations should implement appropriate measures to establish efficient governance related to PII processing" (ISO/IEC, 2017c, Chapter A.11.1):
2) Privacy impact assessment – "if an organization is processing PII, then the organization should establish the procedures necessary to conduct a PIA" (ISO/IEC, 2017c, Chapter A.11.2);
3) Privacy requirement for contractors and PII processors – "organizations should implement appropriate measures to ensure contractors and PII processors have implemented adequate levels of PII protection" (ISO/IEC, 2017c, Chapter A.11.3);
4) Privacy monitoring and auditing – "organizations should implement appropriate measures to periodically monitor and audit privacy controls and the effectiveness of internal privacy policy" (ISO/IEC, 2017c, Chapter A.11.4);
5) PII protection awareness and training – "organizations should implement appropriate measures to provide suitable training for the personnel of the PII controller" (ISO/IEC, 2017c, Chapter A.11.5);
6) PII protection reporting – "organizations should develop, disseminate as appropriate and update reports to senior management and other personnel with responsibility for monitoring PII protection in order to demonstrate accountability with specific statutory and regulatory PII protection programme mandates" (ISO/IEC, 2017c, Chapter A.11.6).

Organizations involved in the processing of PII should establish a policy for the use and protection of PII and it should include appropriate statements concerning support for and commitment to managing compliance with applicable PII protection legislation, contractual requirements and other internal policies (ISO/IEC, 2017c).

The top management of the organization involved in the processing of PII should establish a documented privacy policy, which should: 1) be appropriate to the purpose of the organization; 2) be transparent about the organization's collection and processing of PII; 3) provide the framework for setting objectives for the protection of PII; 4) define rules for making decisions in questions of protection of PII; 5) define criteria on privacy risk acceptance; 6) include a commitment to satisfy applicable privacy safeguarding requirements[169]; 7) include a commitment to continual improvement; 8) be communicated within the organization; and 9) be available to interested parties, as appropriate (ISO/IEC, 2011, 2017c).

These policies can be determined to a large extent by the PII controller in relation with the PII processor. The privacy policy should be supplemented by more detailed rules and obligations of the different privacy stakeholders involved in the processing of PII, including the determination of procedures. In addition, the controls that are used to enforce the privacy policy in a particular context should be clearly documented (ISO/IEC, 2011).

The term "privacy policy" can be used to refer to both internal and external privacy policies[170]: as for the first, it documents the objectives, rules, obligations, restrictions and/or controls an organization has adopted to satisfy the privacy safeguarding requirements that are relevant to its processing of PII; as for the second, it provides outsiders to the organization with a notice of the organization's privacy practices, as well as other relevant information such as the identity and official address of the PII controller, contact points from which PII principals might obtain additional information, etc. (ISO/IEC, 2011).

Measures to address a privacy breach should be proportionate to the risks associated with the breach and they should be implemented as quickly as possible (ISO/IEC, 2011).

Organizations should be capable of providing an organized and effective response to a privacy incident in accordance with their privacy incident response plan. An organizational privacy incident response plan should include:

> a) the definition of privacy incident and the scope of privacy incident response; b) the establishment of a cross-functional privacy incident response team that develops, implements, tests, executes and reviews the privacy incident response plan (approval of the plan should rest with senior management within the organization); c) clearly defined roles, responsibilities and authorities for all members of the privacy incident response team; d) procedures for clarifying the legal grounds for cooperation with external organizations (national and international) in the event of a cross-

[169] Might also be known as data protection/privacy requirements (ISO/IEC, 2018c).

[170] External privacy policies may also be designated as notices.

> border incident; e) procedures to ensure prompt reporting by all individuals subject to the internal privacy policy (e.g., employees, contractors) of any privacy incident to information security officials and the individual accountable for PII protection (sometimes referred to as the CPO), in accordance with organizational incident management direction; f) an incident impact assessment (tasks) to determine the nature and extent of any potential or actual harms to affected individuals (e.g., embarrassment, inconvenience or unfairness) or to the organization; g) a process to identify measures that need to be taken to mitigate the harms identified above and to reduce the likelihood of their recurrence; and h) procedures to determine whether notice to affected individuals and other designated entities (e.g., regulators) is required, the timing for such notice and the form of that notice and, where appropriate, to provide that notice (ISO/IEC, 2017c, Chapter 16.1.2).

Moreover, when PII is compromised, the rights and interests of the PII principal cannot be protected without immediate measures and jurisdictions may impose specific requirements related to the reporting or notification of security incidents involving PII. When a security incident related to PII occurs, the details of the incident, including the organizations' proposed response, should be notified as soon as possible to relevant authorities (data protection authorities, law enforcement agencies) and individuals affected by the incident Organizations should provide affected PII principals access to appropriate and effective remedies, if a privacy breach has occurred (ISO/IEC, 2017c)..

Accountability as a whole includes establishing redress procedures: they provide a means for the PII principal to hold the PII controller accountable for PII misuse. Redress works best when based on transparency and honesty and required types of redress measures can be governed by law. Where redress processes are in place, PII principals might feel more confident because the perceived risk for the natural person about the outcome is effectively reduced (ISO/IEC, 2011).

5.2.7.9.Information security principle

The information security principle indicates to:

- protect PII with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and protect it against risks throughout the whole of its life cycle;

- choose PII processors that provide enough guarantees regarding organizational, physical and technical controls for the processing of PII and ensuring compliance with these controls;
- base these controls on applicable legal requirements, security standards, the results of systematic security risk assessments, and the results of a cost/benefit analysis;
- implement controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that might be affected, and the context in which it is held;
- limit access to PII to those individuals who require such access to perform their duties, and limit the access to the needed PII those individuals require to access to in order to perform their duties;
- resolve risks and vulnerabilities that are discovered through privacy risk assessments and audit processes; and
- subject the controls to periodic review and reassessment in an ongoing security risk management process (ISO/IEC, 2011).

The ISO/IEC 29151 has one specific control related to this principle:

Information security – "PII in the care and custody of the organization should be protected by appropriate controls, in accordance with the results of a threat risk assessment or PIA" (ISO/IEC, 2017c, Chapter A.12).

5.2.7.10. Privacy compliance principle

Finally, the privacy compliance principle requires to:

- verify and demonstrate that the processing meets data protection and privacy safeguarding requirements by regularly conducting audits;
- have proper internal controls and independent supervision mechanisms in place that assure compliance with relevant privacy law and with their security, data protection and privacy policies and procedures; and
- develop and maintain privacy risk assessments in order to evaluate whether program and service delivery initiatives involving PII processing comply with data protection and privacy requirements (ISO/IEC, 2011).

The ISO/IEC 29151 has two specific controls related to this principle:

1) Compliance – "organizations should implement appropriate measures to ensure PII processing meets compliance requirements" (ISO/IEC, 2017c, Chapter A.13.1);
2) Cross border data transfer restrictions in certain jurisdictions – "organization should implement appropriate measures to ensure that any transfers of PII across borders meets relevant compliance requirements" (ISO/IEC, 2017c, Chapter A.13.2).

One or more supervisory authorities might be responsible for monitoring compliance with applicable data protection law, which would also require to cooperate with these supervisory authorities and observing their guidelines and requests, in order to comply with this principle (ISO/IEC, 2011).

5.2.8. Actors

There are four types of actors who can be involved in the processing of PII: PII principals, PII controllers, PII processors and third parties (ISO/IEC, 2011). However, third parties are considered out of scope of the architecture framework specified in ISO/IEC 29101 (ISO/IEC, 2018c).

5.2.8.1.PII Principal

PII principals, who may also be designated as natural persons or data subjects, provide their PII for processing to PII controllers and PII processors and, when it is not otherwise provided by applicable law, they give consent and determine their privacy preferences for how their PII should be processed[171], (ISO/IEC, 2011).

It is not necessary that the natural person is directly identified by name in order to be considered a PII principal. If the natural person to whom the PII relates can be identified indirectly he or she is considered to be the PII principal for that PII set. To determine whether or not a natural person should be considered identifiable, all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person should be considered. ICT systems should support mechanisms that make the PII principal aware of such PII and provide the PII principal with appropriate controls over the sharing of that information (ISO/IEC, 2011).

5.2.8.2.PII Controller

[171] It might be as well important to refer that additional provisions can be defined for processing PII other than consent or compliance with the law, as stated before on the consent and choice principle (e.g., the performance of a contract, the vital interest of the PII principal, etc.).

A PII controller determines the purpose and the means of the processing of PII. The PII controller should ensure adherence to the privacy principles described in this framework during the processing of PII under its control (ISO/IEC, 2011). Thus, the PII controller is responsible for the protection of PII and the fair and lawful handling of it at all times, throughout the organization, as well as for PII processing outsourced to PII processors (ISO/IEC, 2018c).

There might be more than one PII controller for the same PII set or set of operations performed upon PII. In this case, the different PII controllers shall work together and ensure the privacy principles are followed to during the processing of PII. A PII controller can also decide to have all or part of the processing operations carried out by a different privacy stakeholder (e.g. a PII processor) on its behalf (ISO/IEC, 2011).

The PII controller is ultimately responsible for implementing privacy controls in an ICT system, since they are intended to ensure that the privacy safeguarding requirements set for a specific PII principal, transaction, or scenario are addressed and consistently fulfilled. Implemented privacy controls should be documented. Moreover, there also should be provided audit documents that verify that the controls exist, that they have been implemented correctly and that they are functioning properly (ISO/IEC, 2018c).

Moreover, PII controllers should carefully assess whether or not they are processing sensitive PII and implement reasonable and appropriate privacy and security controls based on the requirements set forth in the relevant jurisdiction as well as any potential adverse effects for PII principals as identified during a privacy risk assessment (ISO/IEC, 2011).

Controllers have several obligations considering privacy principles. The ISO/IEC 27701 provides a relation between privacy principles and controls to be followed. Considering that some controls appear in more than one principle, they will be described on the principle on which they have a stronger bound with.

There are five specific controls related with the principle of consent and choice:

1) Determine when and how consent is to be obtained – “the organization should determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals” (ISO/IEC, 2019b, Chapter A.7.2.3);
2) Obtain and record consent – “the organization should obtain and record consent from PII principals in such a way that it can provide on request details of the consent provided” (ISO/IEC, 2019b, Chapter A.7.2.4);
3) Providing mechanism to modify or withdraw consent – “the organization should provide a mechanism for PII principals to modify or withdraw their consent” (ISO/IEC, 2019b, Chapter A.7.3.4);

4) Providing mechanism to object to PII processing – “the organization should provide a mechanism for PII principals to object to the processing of their PII” (ISO/IEC, 2019b, Chapter A.7.3.5);
5) PII controllers' obligations and third parties – “the organization should inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII [consent related], and implement appropriate policies, procedures and/or mechanisms to do so” (ISO/IEC, 2019b, Chapter A.7.3.7).

The organization should clearly document when consent needs to be obtained and the requirements for obtaining consent, stating the purpose(s) for processing with information and how consent is obtained. Some jurisdictions have specific requirements for how consent is collected and recorded. Moreover, certain types of data collection and certain types of PII principals can be subject to additional requirements. The organization should take into account such requirements and document how mechanisms for consent meet those requirements (ISO/IEC, 2019b).

Furthermore, the organization should obtain and record consent from PII principals in such a way that it can provide on request details of the consent provided. The information delivered to the PII principal before the consent process should follow the guidance provided under the control A.7.3.3. – Providing information to PII principals (ISO/IEC, 2019b).

The consent should be freely given, specific regarding the purpose for processing, and unambiguous and explicit (ISO/IEC, 2019b).

Moreover, the organization should inform PII principals of their rights related to withdrawing consent at any time and provide the mechanism to do so. The mechanism used for withdrawal depends on the system, but it should be consistent with the mechanisms used for obtaining consent when possible. The organization should define a response time and requests should be handled in accordance (ISO/IEC, 2019b).

Modifying consent can include placing restrictions on the processing of PII. Therefore, the organization should record any request to withdraw or change consent in a similar way to the recording of the consent itself and any change of consent should be disseminated to authorized users and to relevant third parties. The organization should adopt appropriate measures, considering the available technology, to inform third parties of any modification or withdrawal of consent, or objections pertaining to the shared PII. Also, some jurisdictions impose a legal requirement to inform these third parties of these actions (ISO/IEC, 2019b).

The organization should determine and maintain active communication channels with third parties, monitoring their acknowledgement of receipt of the information (ISO/IEC, 2019b).

There are three controls related with the purpose legitimacy and specification principle:

1. Identify and document purpose – "the organization should identify and document the specific purposes for which the PII will be processed" (ISO/IEC, 2019b, Chapter A.7.2.1);
2. Identify lawful basis – "the organization should determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes" (ISO/IEC, 2019b, Chapter A.7.2.2);
3. Automated decision making – "the organization should identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII" (ISO/IEC, 2019b, Chapter A.7.3.10).

The organization should ensure that PII principals understand the purpose for which their PII is processed, being this documented and communicated to PII principals (ISO/IEC, 2019b).

When a decision based solely on automated processing of PII significantly affects PII principals, there might be specific obligations to PII controllers, considering the jurisdiction that applies (ISO/IEC, 2019b).

There are three controls regarding the collection imitation principle and the data minimization principle[172]:

1) Limit collection – "the organization should limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes" (ISO/IEC, 2019b, Chapter A.7.4.1);
2) Limit processing – "the organization should limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes" (ISO/IEC, 2019b, Chapter A.7.4.2);
3) PII minimization objectives – "the organization should define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives" (ISO/IEC, 2019b, Chapter A.7.4.4).

The organization should limit the collection of PII to what is adequate, relevant and necessary in relation to the identified purposes, including the amount of PII that the organization indirectly collects (such as web logs, system logs, etc.) (ISO/IEC, 2019b).

Moreover, privacy by default implies that, "where any optionality in the collection and processing of PII exists, each option should be disabled by default and only enabled by explicit choice of the PII principal" (ISO/IEC, 2019b, Chapter 7.4.1).

[172] These two principles will be analysed together, since they are closely related.

Limiting the processing of PII should be managed through information security and privacy policies and documented procedures. Processing of PII should be limited by default to the minimum necessary relative to the identified purposes, using for that purpose data minimization techniques, which should be documented (ISO/IEC, 2019b).

There are five controls considering the use, retention and disclosure limitation principle:

1) PII de-identification and deletion at the end of processing – "the organization should either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s)" (ISO/IEC, 2019b, Chapter A.7.4.5);
2) Temporary files – "the organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period" (ISO/IEC, 2019b, Chapter A.7.4.6);
3) Retention – "the organization should not retain PII for longer than is necessary for the purposes for which the PII is processed" (ISO/IEC, 2019b, Chapter A.7.4.7);
4) Disposal – "the organization should have documented policies, procedures and/or mechanisms for the disposal of PII" (ISO/IEC, 2019b, Chapter A.7.4.8);
5) Records of PII disclosure to third parties – "the organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time" (ISO/IEC, 2019b, Chapter A.7.5.4).

The organization should have mechanisms to erase the PII when the processing has ended or, alternatively, some de-identification techniques can be used (ISO/IEC, 2019b).

Moreover, the organization should perform periodic checks so unused temporary files are deleted within the identified time period (ISO/IEC, 2019b).

The organization should develop and maintain retention schedules, considering legal, regulatory and business requirements, for the PII it retains, considering that the retention period should be no longer than is necessary. Where such requirements conflict, a business decision needs to be taken, based on a risk assessment, and documented in the appropriate schedule (ISO/IEC, 2019b).

The choice of PII disposal techniques depends on several factors (such as the nature and extent of the PII to be disposed of, whether or not there is metadata associated with the PII, and the physical characteristics of the media on which the PII is stored), as disposal techniques differ in their properties and outcomes (ISO/IEC, 2019b).

Finally, PII can be disclosed during normal operations and its disclosure should be recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. These records should include the source of the disclosure and the source of the authority to make the disclosure (ISO/IEC, 2019b).

There is one control considering the accuracy and quality principle:

1) Accuracy and quality – "the organization should ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII" (ISO/IEC, 2019b, Chapter A.7.4.3).

The organization should implement policies, procedures and/or mechanisms to minimize, as well as to respond to, PII inaccuracies in the processing of PII. These policies, procedures and/or mechanisms should be included in the documented information and should apply throughout the PII lifecycle (ISO/IEC, 2019b).

There are two controls considering the openness, transparency and notice principle:

1. Determining information for PII principals – "the organization should determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision" (ISO/IEC, 2019b, Chapter A.7.3.2);
2. Providing information to PII principals – "the organization should provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII" (ISO/IEC, 2019b, Chapter A.7.3.3).

The organization should determine the legal, regulatory and/or business requirements for when information is to be provided to the PII principal (e.g. prior to processing, within a certain time from when it is requested, etc.) and for the type of information to be provided. Depending on the requirements, the information can take the form of a notice, which may include:

> information about the purpose of the processing; contact details for the PII controller or its representative; information about the lawful basis for the processing; information on where the PII was obtained, if not obtained directly from the PII principal; information about whether the provision of PII is a statutory or contractual requirement, and where appropriate, the possible consequences of failure to provide PII; information on obligations to PII principals (...) and how PII principals can benefit from them, especially regarding accessing, amending, correcting, requesting erasure, receiving a copy of their PII and objecting to the processing; information on how the PII principal can withdraw consent; information about transfers of PII; information about recipients or categories of

recipients of PII; information about the period for which the PII will be retained; information about the use of automated decision making based on the automated processing of PII; information about the right to lodge a complaint and how to lodge such a complaint; information regarding the frequency with which information is provided (e.g. "just in time" notification, organization defined frequency, etc.) (ISO/IEC, 2019b, Chapter 7.3.2).

Also, the organization should provide updated information if the purposes for the processing of PII change (ISO/IEC, 2019b).

Finally, the organization should provide the above information to PII principals in a timely, concise, complete, transparent, intelligible and easily accessible form, using clear and plain language, as appropriate to the target audience and, where appropriate, the information should be given at the time of PII collection. It should also be permanently accessible (ISO/IEC, 2019b).

There are four controls considering the individual participation and access principle:

1) Determining and fulfilling obligations to PII principals – "the organization should determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations" (ISO/IEC, 2019b, Chapter A.7.3.1);
2) Access, correction and/or erasure – "the organization should implement policies, procedures and/or mechanisms to meet their obligations to PII principals to access, correct and/or erase their PII" (ISO/IEC, 2019b, Chapter A.7.3.6);
3) Providing copy of PII processed – "the organization should be able to provide a copy of the PII that is processed when requested by the PII principal" (ISO/IEC, 2019b, Chapter A.7.3.8);
4) Handling requests – "the organization should define and document policies and procedures for handling and responding to legitimate requests from PII principals" (ISO/IEC, 2019b, Chapter A.7.3.9).

Obligations to PII principals and the means to support them vary from one jurisdiction to another. Therefore, the organization should ensure that it provides the appropriate means to meet the obligations to PII principals in an accessible and timely manner, being these obligations and their compliance documented and communicated to the PII principal, along with an up-to-date contact point where they can address their requests. The contact point should be provided in a similar way to that used to collect PII and consent (ISO/IEC, 2019b).

Also, the organization should implement policies, procedures and/or mechanisms for enabling PII principals to obtain access to, correct and erase of their PII, if requested and without undue delay and in accordance with the response time defined by the organization. Any corrections or erasures should be disseminated through the system and/or to authorized users, and should be passed to third parties to whom the PII has been transferred (ISO/IEC, 2019b).

The organization should implement policies, procedures and/or mechanisms to deal with eventual disputes about the accuracy or correction of the data by the PII principal. These policies, procedures and/or mechanisms should include informing the PII principal of what changes were made, and of reasons why corrections cannot be made (where this is the case). However, the organization should determine if the applicable jurisdiction impose restrictions on when and how a PII principal can request correction or erasure of their PII (ISO/IEC, 2019b).

The organization should provide a copy of the PII that is processed in a structured, commonly used, format accessible by the PII principal. It is important to keep in mind that some jurisdictions define cases where portability can be applied, either to the PII principals or to recipient PII controllers (typically structured, commonly used and machine readable) (ISO/IEC, 2019b).

Requests may be of different nature and should be handled within the appropriate defined response times. Some jurisdictions allow the organization to charge a fee in certain cases or even define response times, depending on the complexity and number of the requests, as well as requirements to inform PII principals of any delay. The appropriate response times should be defined in the privacy policy (ISO/IEC, 2019b).

There are six controls considering the accountability principle:

1) Contracts with PII processors – "the organization should have a written contract with any PII processor that it uses, and should ensure that their contracts with PII processors address the implementation of the appropriate controls" (ISO/IEC, 2019b, Chapter A.7.2.6);
2) Joint PII controller – "the organization should determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller" (ISO/IEC, 2019b, Chapter A.7.2.7);
3) Records related to processing PII – "the organization should determine and securely maintain the necessary records in support of its obligations for the processing of PII" (ISO/IEC, 2019b, Chapter A.7.2.8);
4) Identify basis for international PII transfer – "the organization should identify and document the relevant basis for transfers of PII between jurisdictions" (ISO/IEC, 2019b, Chapter A.7.5.1);

5) Countries and organizations to which PII can be transferred – "the organization should specify and document the countries and international organizations to which PII can possibly be transferred" (ISO/IEC, 2019b, Chapter A.7.5.2);
6) Records and transfer of PII – "the organization should record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals" (ISO/IEC, 2019b, Chapter A.7.5.3).

In case of establishing a relationship with a PII processor, the PII controller should have a written contract with any supplier acting as a PII processor, and the contract should clearly allocate roles and responsibilities between the PII controller and the PII processor, as well as it should contain appropriate clauses relating to PII protection in order to hold the PII processor accountable for the processing performed. Moreover, the contract should provide at least:

an appropriate declaration on the scale, nature and purpose of the processing under contract; support duties of the PII processor on giving PII principals the ability to access and review their PII and handling any complaints raised by PII principals (...); other organizational measures to be taken in order to fulfil legal or regulatory requirements; authorization of the PII controller to conduct audits on the premises of the PII processor; reporting obligations in cases of data breaches, unauthorized processing or other non-performance of contractual terms and condition, including identification of the points of contact in both parties; method of instruction from the PII controller to the PII processor; measures applying on termination of the contract, especially with regard to the secure deletion of PII on premise (ISO/IEC, 2017c, Chapter 15.1.2).

PII processors should be evaluated on the basis of experience, trustworthiness and their ability to meet PII protection requirements as applicable by legislation, regulation, or in contracts or other legal agreements (ISO/IEC, 2017c).

The PII controller should ensure that their PII processors do not undertake any further subcontracting of processing (i.e., make use of sub-processors) without prior approval of the PII controller (ISO/IEC, 2017c). Moreover, the PII processor should inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, in the case of having general written authorization, thereby giving the customer the opportunity to object to such changes (ISO/IEC, 2019b).

The PII controller should ensure that their PII processors do not process the PII for any purposes other than those specified in the contract or other legal agreement (ISO/IEC, 2017c).

The PII controller should ensure that their PII processors securely dispose of PII, in accordance with the PII controller's policies or other direction (ISO/IEC, 2017c).

In case of a joint PII controller scenario, roles and responsibilities for the processing of PII should be determined in a transparent manner. These roles and responsibilities should be documented in a contract or any similar binding document that contains the terms and conditions for the joint processing of PII, which may include:

purpose of PII sharing/joint PII controller relationship; identity of the organizations (PII controllers) that are part of the joint PII controller relationship; categories of PII to be shared and/or transferred and processed under the agreement; overview of the processing operations (e.g. transfer, use); description of the respective roles and responsibilities; responsibility for implementing technical and organizational security measures for PII protection; definition of responsibility in case of a PII breach (e.g. who will notify, when, mutual information); terms of retention and/or disposal of PII; liabilities for failure to comply with the agreement; how obligations to PII principals are met; how to provide PII principals with information covering the essence of the arrangement between the joint PII controllers; how PII principals can obtain other information they are entitled to receive; and a contact point for PII principals (ISO/IEC, 2019b, Chapter 7.2.7).

The records of the processing of PII, who should have an owner who is responsible for its accuracy and completeness, should include:

> the type of processing; the purposes for the processing; a description of the categories of PII and PII principals (e.g. children); the categories of recipients to whom PII has been or will be disclosed, including recipients in third countries or international organizations; a general description of the technical and organizational security measures; and a PIA report (ISO/IEC, 2019b, Chapter 7.2.8).

PII transfer can be subject to legislation and/or regulation depending on the jurisdiction or international organization to which data is to be transferred (and its origin), which may include that information transfer agreements are reviewed by a designated supervisory authority. Thus, the organization should document compliance to such requirements as the basis for transfer (ISO/IEC, 2019b).

The identities of the countries and international organizations to which PII can possibly be transferred in normal operations should be made available to customers, which should include the identities of the countries arising from the use of subcontracted PII processing. Organizations should record transfers of PII under these circumstances, as well as when there are transfers from third parties of PII which has been modified as a result of PII controllers' managing their obligations, or transfers to third parties to implement legitimate requests from PII principals, including requests to erase PII. Organizations should have a policy defining the retention period of these records (ISO/IEC, 2019b).

There is one control considering the information security principle:

1) PII transmission controls – "the organization should subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination" (ISO/IEC, 2019b, Chapter A.7.4.9).

Transmission of PII needs to be controlled, by ensuring that only authorized individuals have access to transmission systems and by following the appropriate processes (including the retention of audit logs) to ensure that PII is transmitted without compromise to the correct recipients (ISO/IEC, 2019b).

There is one control considering the privacy compliance principle:

1) Privacy impact assessment – "the organization should assess the need for, and implement where appropriate, a PIA whenever new processing of PII or changes to existing processing of PII is planned" (ISO/IEC, 2019b, Chapter A.7.2.5).

PII processing generates risks for PII principals, which should be assessed through a PIA. Some jurisdictions define cases for which a PIA is mandated and criteria can include automated decision making which produces legal effects on PII principals, large scale processing of special categories of PII or systematic monitoring of a publicly accessible area on a large scale (ISO/IEC, 2019b).

The organization should determine the elements that are necessary for the completion of a PIA, which may include a list of the types of PII processed, where the PII is stored and where it can be transferred. Data flow diagrams and data maps can also be helpful in this context (ISO/IEC, 2019b).

5.2.8.3.PII Processor

A PII processor carries out the processing of PII on behalf of a PII controller, acts on behalf of, or in accordance with the instructions of the PII controller, observes the stipulated privacy requirements and implements the corresponding privacy controls. Furthermore, in some jurisdictions, the PII processor is bound by a legal contract to the PII controller (ISO/IEC, 2011).

A distinction between PII processors and third parties must be made, because the legal control of the PII remains with the original PII controller when it is sent over to the PII processor, whereas a third party can become a PII controller in its own right once it has received the PII in question (ISO/IEC, 2011).

Processors also have several obligations considering privacy principles. The ISO/IEC 27701 provides a relation between privacy principles and controls to be followed. Considering that some controls appear in more than one principle, they will be described on the principle on which they have a stronger bound with. When applicable, there will also be provided controls related with the processing activities of a public cloud PII processor, considering the ISO/IEC 27018.
There is one control related with the consent and choice principle:

Customer obligations – "the organization should provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations" (ISO/IEC, 2019b, Chapter 8.2.5).

Moreover, when the actor is a public cloud PII processor, the following control also applies:

Obligation to co-operate regarding PII principals' rights – "the public cloud PII processor should provide the CSC with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them" (ISO/IEC, 2019a, Chapter A.2.1).

The information needed by the customer can include the permission and execution of audits conducted by the customer or another auditor mandated or otherwise agreed by the customer (ISO/IEC, 2019b). Where the PII controller depends on the public cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract (ISO/IEC, 2019a).
There are four controls related with the purpose legitimacy and specification principle:

1) Customer agreement:

the organization should ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations [PII controller or processor] (taking into account the nature of processing and the information available to the organization). The contract between the organization and the customer should include, where applicable, the following: privacy by design and privacy by default; achieving security of processing; notification of breaches involving PII to a supervisory authority; notification of breaches involving PII to customers and PII principals; conducting PIAs; the assurance of assistance by the PII processor if prior consultations with relevant PII protection authorities are needed; the subject matter and duration of the processing, the nature and purpose of the processing, the type of PII and categories of PII principals, considering the applicable jurisdiction (ISO/IEC, 2019b, Chapter 8.2.1);

2) Organization's purposes:

the organization should ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer. The contract between the organization and the customer should include, but not be limited to, the objective and time frame to be achieved by the service. The organization should allow the customer to verify their compliance with the purpose specification and limitation principles to ensures that no PII is processed by the organization or any of its subcontractors for other purposes than those expressed in the documented instructions of the customer (ISO/IEC, 2019b, Chapter 8.2.2);

3) Marketing and advertising use:

the organization should not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization should not make providing such consent a condition for receiving the service (ISO/IEC, 2019b, Chapter 8.2.3);

4) Infringing instruction – "the organization should inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation" (ISO/IEC, 2019b, Chapter 8.2.4).

If the actor is a public cloud PII processor, the following controls also apply:

1) Public cloud PII processor's purpose – "PII to be processed under a contract should not be processed for any purpose independent of the instructions of the CSC" (ISO/IEC, 2019a, Chapter A.3.1);
2) Public cloud PII processor's commercial use – "PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service" (ISO/IEC, 2019a, Chapter A.3.2).

The contract between the PII processor and the customer should include the following wherever relevant, and depending on the customer's role (PII controller or PII processor) (this list is neither definitive nor exhaustive):

> privacy by design and privacy by default; achieving security of processing; notification of breaches involving PII to a supervisory authority; notification of breaches involving PII to customers and PII principals; conducting PIAs; and the assurance of assistance by the PII processor if prior consultations with relevant PII protection authorities are needed (ISO/IEC, 2019b, Chapter 8.2.1).

Also, some jurisdictions demand that the contract include the subject matter, the nature, the purpose and the duration of the processing the type of PII and categories of PII principals (ISO/IEC, 2019b).

In order to achieve the customer's purpose, there can be technical reasons why it is appropriate for the organization to determine the method for processing PII, consistent with the general instructions of the customer but without the customer's express instruction (ISO/IEC, 2019b).

The organization should allow the customer to verify their compliance with the purpose specification and limitation principles. Compliance of PII processors with the customer's contractual requirements should be documented, especially where marketing and/or advertising is planned, and organizations should not insist on the inclusion of marketing and/or advertising uses where express consent has not been fairly obtained from PII principals (ISO/IEC, 2019b).

Considering the contract between the public cloud PII processor and the CSC, instructions may include the objective and time frame to be achieved by the service. To achieve the CSC's purpose, the public cloud PII processor may have technical reasons to determine the method for processing PII, consistent with the general instructions of the CSC but without the CSC's express instruction. Nevertheless, the public cloud PII processor should provide the CSC with all relevant information, in due time, to allow the CSC to ensure the public cloud PII processor's compliance with purpose specification and limitation principles and ensure that no PII is processed by the public cloud PII processor or any of its sub-contractors for further purposes independent of the instructions of the CSC (ISO/IEC, 2019a).

There are no controls available for the collection limitation principle (ISO/IEC, 2019b, 2019a).

There is one control related with data minimization principle:

1) Temporary files – "the organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period" (ISO/IEC, 2019b, Chapter B.8.4.1).

If the actor is a public cloud PII processor, the following control also apply:

1) Secure erasure of temporary files – "temporary files and documents should be erased or destroyed within a specified, documented period" (ISO/IEC, 2019a, Chapter A.5.1).

Information systems can create temporary files in the normal course of their operation. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they cannot be deleted. A "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used (ISO/IEC, 2019b, 2019a). PII processing information systems should implement a periodic check that unused temporary files above a specified age are deleted (ISO/IEC, 2019a).

There are three controls related with the use, retention and disclosure limitation principle:

1) Records of PII disclosure to third parties – "the organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and when" (ISO/IEC, 2019b, Chapter B.8.5.3);
2) Notification of PII disclosure requests – "the organization should notify the customer of any legally binding requests for disclosure of PII" (ISO/IEC, 2019b, Chapter 8.5.4);
3) Legally binding PII disclosures – "the organization should reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer" (ISO/IEC, 2019b, Chapter 8.5.5).

If the actor is a public cloud PII processor, the following controls also apply:

1) PII disclosure notification

the contract between the public cloud PII processor and the CSC should require the public cloud PII processor to notify the CSC, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited (ISO/IEC, 2019a, Chapter A.6.1);

2) Recording of PII disclosures – "disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time" (ISO/IEC, 2019a, Chapter A.6.2).

PII can be disclosed during the organization's operations. These disclosures should be recorded (ISO/IEC, 2019b, 2019a)

Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure (ISO/IEC, 2019b, 2019a). In these cases, the organization should notify the customer of any such request within agreed timeframes and according to an agreed procedure, which can be included in the customer contract. However, in some cases, the legally binding requests include the requirement for the organization not to notify anyone about the event (ISO/IEC, 2019b).

The public cloud PII processor should provide contractual guarantees that it will "reject any requests for PII disclosure that are not legally binding; consult the corresponding CSC where legally permissible before making any PII disclosure; and accept any contractually agreed requests for PII disclosures that are authorized by the corresponding CSC" (ISO/IEC, 2019a, Chapter A.6.1).

There are no controls available for the accuracy and quality principle (ISO/IEC, 2019b, 2019a).

There are three controls related with the openness, transparency and notice principle:

1) Disclosure of subcontractors used to process PII – "the organization should disclose any use of subcontractors to process PII to the customer before use" (ISO/IEC, 2019b, Chapter B.8.5.6);
2) Engagement of a subcontractor to process PII – "the organization should only engage a subcontractor to process PII according to the customer contract" (ISO/IEC, 2019b, Chapter B.8.5.7);
3) Change of subcontractor to process PII – "the organization should, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes" (ISO/IEC, 2019b, Chapter B.8.5.8).

If the actor is a public cloud PII processor, the following control also apply:

1) Disclosure of sub-contracted PII processing – "the use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant CSCs before their use" (ISO/IEC, 2019a).

Provisions for the use of subcontractors to process PII should be included in the customer's contract. Information disclosed should cover the fact that subcontracting is used and the names of relevant subcontractors, as well as the countries and international organizations to which subcontractors can transfer data and the means by which subcontractors are obliged to meet or exceed the obligations of the organization (ISO/IEC, 2019b).

Accordingly, provisions for the use of sub-contractors to process PII should be transparent in the contract between the public cloud PII processor and the CSC (ISO/IEC, 2019a).

Where the organization subcontracts some or all of the processing of that PII to another organization, a written authorization from the customer is required prior to the PII processed by the subcontractor, which can be in the form of appropriate clauses in the customer contract, or can be a specific "one-off" agreement (ISO/IEC, 2019b). As for public cloud services, the contract should specify that subcontractors can only be commissioned if the CSC agrees to at the beginning of the service. The public cloud PII processor should inform the CSC in a timely fashion of any intended changes in this regard so that the CSC can object to such changes or to terminate the contract. Information disclosed should cover the fact that sub-contracting is used and the names of relevant sub-contractors, the countries in which sub-contractors can process data and the means by which subcontractors are obliged to meet or exceed the obligations of the public cloud PII processor, but not any business-specific details (ISO/IEC, 2019a).

The organization should have a written contract with any subcontractors that it uses for PII processing on its behalf, and should ensure that their contracts with subcontractors address the implementation of appropriate controls, taking account of the information security risk assessment process and the scope of the processing of PII performed by the PII processor. A contract can define the responsibilities of each party differently but, to be consistent with this document, all controls should be considered and included in the documented information (ISO/IEC, 2019b).

Where the organization changes the subcontractor that is processing PII, then written authorization from the customer is required for the change, prior to the PII processed by the new subcontractor. Once again, this can be in the form of appropriate clauses in the customer contract, or can be a specific "one-off" agreement (ISO/IEC, 2019b).

There is one control related with the individual participation and access principle:

1) Obligations to PII principals – "the organization should provide the customer with the means to comply with its obligations related to PII principals" (ISO/IEC, 2019b, Chapter B.8.3.1).

Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals, the relevant information or technical measures should be specified in a contract (ISO/IEC, 2019b).

There are four controls related with the accountability principle:

1) Records related to processing PII –" the organization should determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer" (ISO/IEC, 2019b, Chapter B.8.2.6);
2) Return, transfer or disposal of PII – "the organization should provide the ability to return, transfer and/or disposal of PII in a secure manner. It should also make its policy available to the customer" (ISO/IEC, 2019b, Chapter B.8.4.2);
3) Identify basis for international PII transfer – "the organization should inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract" (ISO/IEC, 2019b, Chapter B.8.5.1);

4) Countries and organizations to which PII can be transferred – “the organization should specify and document the countries and international organizations to which PII can possibly be transferred” (ISO/IEC, 2019b, Chapter B.8.5.2).

If the actor is a public cloud PII processor, the following controls also apply:

1) Notification of a data breach involving PII – “the public cloud PII processor should promptly notify the relevant CSC in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII” (ISO/IEC, 2019a, Chapter A.10.1);
2) Retention period for administrative security policies and guidelines – “copies of security policies and operating procedures should be retained for a specified, documented period on replacement (including updating)” (ISO/IEC, 2019a, Chapter A.10.2);
3) PII return, transfer and disposal – “the public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the CSC” (ISO/IEC, 2019a, Chapter A.10.3).

Some jurisdictions can require the organization to record information such as categories of processing carried out on behalf of each customer; transfers to third countries or international organizations; and a general description of the technical and organizational security measures (ISO/IEC, 2019b).

At some point in time, PII can need to be disposed of, which can involve returning the PII to the customer, transferring it to another organization or to a PII controller, deleting or otherwise destroying it, de-identifying it or archiving it (ISO/IEC, 2019b, 2019a). The capability for the return, transfer and/or disposal of PII should be managed in a secure manner (ISO/IEC, 2019b).

The organization should provide the assurance necessary to allow the customer to ensure that PII processed under a contract is erased (by the organization and any of its subcontractors), as soon as they are no longer necessary for the identified purposes of the customer. In accordance, the organization should develop and implement a policy in respect to the disposal of PII and should make this policy available to customer when requested. The policy should cover the retention period for PII before its disposal after termination of a contract, to protect the customer from losing PII through an accidental lapse of the contract (ISO/IEC, 2019b, 2019a).

PII transfer between jurisdictions can be subject to legislation and/or regulation depending on the jurisdiction or organization to which PII is to be transferred (and from where it originates). Therefore, the organization should document compliance with such requirements as the basis for transfer and should inform the customer of any transfer of PII, including transfers to suppliers; other parties; other countries or international organizations (ISO/IEC, 2019b).

In case of international transfer of PII, agreements such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the countries involved and the circumstances in which such agreements apply, should be identified (ISO/IEC, 2019b).

Provisions covering the notification of a data breach involving PII should form part of the contract between the public cloud PII processor and the CSC, which should specify how the public cloud PII processor will provide the information necessary for the CSC to fulfil his obligation to notify relevant authorities and also define the maximum delay in notification of a data breach involving PII. This notification obligation does not extend to a data breach caused by the CSC or PII principal or within system components for which they are responsible (ISO/IEC, 2019a).

In the event that a data breach involving PII has occurred, a record should be maintained with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, the steps taken to resolve the incident (including the person in charge and the data recovered), the fact that the incident resulted in loss, disclosure or alteration of PII, a description of the data compromised, if known; and if notifications were performed, the steps taken to notify the CSC and/or regulatory agencies (ISO/IEC, 2019a).

In some jurisdictions, relevant legislation or regulations can require the public cloud PII processor to directly notify appropriate regulatory authorities of a data breach involving PII (ISO/IEC, 2019a).

Review of current and historical policies and procedures can be required. A minimum retention period of five years is recommended in the absence of a specific legal or contractual requirement (ISO/IEC, 2019a).

There is one control related with the information security principle:

1) PII transmission controls – "the organization should subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination" (ISO/IEC, 2019b, Chapter B.8.4.3).

If the actor is a public cloud PII processor, the following controls also apply:

1) Confidentiality or non-disclosure agreements – "individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation" (ISO/IEC, 2019a, Chapter A.11.1);

2) Restriction of the creation of hardcopy material – "the creation of hardcopy material displaying PII should be restricted" (ISO/IEC, 2019a, Chapter A.11.2);
3) Control and logging of data restoration – "there should be a procedure for, and a log of, data restoration efforts. The log of data restoration efforts should contain: the person responsible, a description of the restored data, and the data that were restored manually". (ISO/IEC, 2019a, Chapter A.11.3);
4) Protecting data on storage media leaving the premises – "PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned)" (ISO/IEC, 2019a, Chapter A.11.4);
5) Use of unencrypted portable storage media and devices – "portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented" (ISO/IEC, 2019a, Chapter A.11.5);
6) Encryption of PII transmitted over public data-transmission networks – "PII that is transmitted over public data-transmission networks should be encrypted prior to transmission" (ISO/IEC, 2019a, Chapter A.11.6);
7) Secure disposal of hardcopy materials – "where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc." (ISO/IEC, 2019a, Chapter A.11.7);
8) Unique use of user IDs - if more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes (ISO/IEC, 2019a, Chapter A.11.8);
9) Records of authorized users – "an up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained" (ISO/IEC, 2019a, Chapter A.11.9);
10) User ID management – "de-activated or expired user IDs should not be granted to other individuals" (ISO/IEC, 2019a, Chapter A.11.10);
11) Contract measures

contracts between the CSC and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor (ISO/IEC, 2019a, Chapter A.11.11);

12) Sub-contracted PII processing:

contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor (ISO/IEC, 2019a, Chapter A.11.12);

13) Access to data on pre-used data storage space – "the public cloud PII processor should ensure that whenever data storage space is assigned to a CSC, any data previously residing on that storage space is not visible to that CSC" (ISO/IEC, 2019a, Chapter A.11.13).

Transmission of PII needs to be controlled, typically by ensuring that only authorized individuals have access to transmission systems, and by following the appropriate processes to ensure that PII is transmitted without compromise to the correct recipients. Requirements for transmission controls can be included in the PII processor-customer contract or advice may be required from the customer prior to transmission (ISO/IEC, 2019b).

A confidentiality agreement between the public cloud PII processor, its employees and its agents should ensure that employees and agents do not disclose PII for purposes independent of the instructions of the CSC and the obligations of the confidentiality agreement should survive termination of any relevant contract (ISO/IEC, 2019a).

There is one control related with the privacy compliance principle:

1) Customer obligations (as previously referred on consent and choice principle).

If the actor is a public cloud PII processor, the following controls also apply:

1) Geographical location of PII – "the public cloud PII processor should specify and document the countries in which PII can possibly be stored" (ISO/IEC, 2019a, Chapter A.12.1);
2) Intended destination of PII – "PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination" (ISO/IEC, 2019a, Chapter A.12.2).

The identities of the countries where PII can possibly be stored should be made available to CSCs, including those arising from the use of sub-contracted PII processing. Where specific contractual agreements apply to the international transfer of data, such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the agreements and the countries or circumstances in which such agreements apply should also be identified. The public cloud PII processor should inform the CSC in a timely fashion of any intended changes in this regard so that the CSC can object to such changes or to terminate the contract (ISO/IEC, 2019a).

5.2.8.4.CPO

The ISO/IEC describes the chief privacy officer (CPO) as a "senior management individual who is accountable for the protection of personally identifiable information (PII) in an organization" (ISO/IEC, 2017c, Chapter 3.1.1). Nevertheless, according to the ISO/IEC 27701, the organization should "appoint one or more persons responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII"(ISO/IEC, 2019b, Chapter 6.3.1.1).

The responsible should:

> be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks; be involved in the management of all issues which relate to the processing of PII; be expert in data protection legislation, regulation and practice; act as a contact point for supervisory authorities; inform top-level management and employees of the organization of their obligations with respect to the processing of PII; provide advice in respect of privacy impact assessments conducted by the organization (ISO/IEC, 2019b, Chapter 6.3.1.1).

In some jurisdictions such a person is called a data protection officer. On those, it is defined when such a position is required, along with its position and role, and indicated that this position can be fulfilled by a staff member or outsourced (ISO/IEC, 2019b).

5.2.9. PIA

The ISO/IEC 29134 provides guidance on how to make PIAs.

A PIA is "an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes PII and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk" (ISO/IEC, 2017b, p. vi).

Usually, this assessment includes documentation about measures taken for risk treatment, for example, measures arising from the use of the ISMS in ISO/IEC 27001 (ISO/IEC, 2017b).

A PIA is a process that begins at the earliest possible stages of an initiative, when there are opportunities to influence its outcome and ensure privacy by design and it continues until, and even after, the project has been deployed (ISO/IEC, 2017b).

A PIA can be carried out for the purpose of:

> identifying privacy impacts, privacy risks and responsibilities; providing input to design for privacy protection (sometimes called privacy by design); reviewing a new information system's privacy risks and assessing its impact and likelihood; providing the basis for the provision of privacy information to PII principals on any PII principal mitigation action recommended; maintaining later updates or upgrades with additional functionality likely to impact the PII that are handled; sharing and mitigating privacy risks with stakeholders, or providing evidence relating to compliance" (ISO/IEC, 2017b, Chapter 5.1).

A PIA helps to identify privacy issues early and/or to reduce costs in management time, legal expenses and potential media or public concern by considering privacy issues early. It may also help an organization to avoid costly or embarrassing privacy mistakes. Thus, a PIA contributes to an organization's demonstration of its compliance with relevant privacy and data protection requirements in the event of a subsequent complaint, privacy audit or compliance investigation (ISO/IEC, 2017b).

Also, a PIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions on privacy issues about the project and it assists in anticipating and responding to the public's privacy concerns (ISO/IEC, 2017b).

In some jurisdictions, a PIA may be necessary to meet legal and regulatory requirements (ISO/IEC, 2017b).

Controls necessary to treat the risks identified during the PIA may be derived from multiple sets of controls, including ISO/IEC 27002 (for security controls) and ISO/IEC 29151 (for PII protection controls) or comparable national standards, or they may be defined by the person responsible for conducting the PIA, independently of any other control set (ISO/IEC, 2017b).

Typically, the responsibility for ensuring that a PIA is undertaken should lie with the person in charge of PII protection or, on his/her absence, with the project manager developing the new technology, service or other initiative that may impact privacy. Accountability for ensuring the PIA is undertaken and the quality of the result should lie with the top management of the PII controller (ISO/IEC, 2017b).

The organization's management should decide if and when a new or updated PIA is required. When it is, the organization's management, in conjunction with the assessor to be, should define its scope. The organization should also decide on and document the scale of the PIA, the process to be used to perform the PIA, and on the target audiences, hence the nature and contents of the PIA reports to be produced (ISO/IEC, 2017b).

An organization should conduct a new or updated PIA if it perceives impacts on privacy from

a new or prospective technology, service or other initiative where PII is, or is to be, processed, a decision that sensitive PII (see ISO/IEC 29100:2011, 2.26) is going to be processed, changes in applicable privacy related laws and regulations, internal policy and standards, information system operation, purposes and means for processing data, new or changed data flows, etc., and business expansion or acquisitions (ISO/IEC, 2017b, Chapter 6.2).

When defining risk criteria, the assessor should consider:

> legal and regulatory factors that impact the safeguarding of the natural person's privacy and the protection of their PII; external factors such as industry guidelines, professional standards, company policies and customer agreements; factors predetermined by a specific application or in a specific use case context; other factors that can affect the design of information systems and the associated privacy safeguarding requirements (ISO/IEC, 2017b, Chapter 6.3.1).

On the other hand, by establishing the context, the organization defines the relevant internal and external parameters to be taken into account when managing privacy risk and setting the scope and privacy risk criteria for the remaining process. Therefore, an appropriate description of the programme, process, or information system to be addressed should be made and its related stakeholders should be identified, in order to be consulted (ISO/IEC, 2017b).

During the PIA, information flows of PII should be identified, as well as potential user behavior, in order to determine the relevant privacy safeguarding requirements and privacy risks that need to be addressed. Risk analysis includes identifying the PII and supporting assets that may be at risk, the vulnerabilities associated with those assets, the threats that might exploit those vulnerabilities, the likelihood and impact of that happening, as well as any existing controls that might influence the risk. Moreover, privacy risk analysis involves consideration of the causes and sources of privacy risk, their positive and negative consequences, and the likelihood those consequences can occur. The assessor should identify factors that affect consequences and likelihood. Thus, the assessor should take into account existing controls and their effectiveness (ISO/IEC, 2017b).

Risk estimation consists in assigning values to the potential consequences (level of impact) and the threats (likelihood) of a risk. Producing a privacy risk evaluation should involve the relative prioritization of privacy risk, based on the severity of privacy impact on PII principals and on the overall impact to the organization. A privacy risk map should result from an assessment of the level of impact and the likelihood of the assessed risks (ISO/IEC, 2017b).

Considering the privacy risk map, treatment options should be decided for any risk assessed. There are four options available for privacy risk treatment: risk reduction, risk retention, risk avoidance and risk transfer (ISO/IEC, 2017b).

Finally, decisions that are made during the PIA process on the acceptance of the residual privacy risks, on non-implementation of PIA recommendations with the treatment plan and on non-publishing elements of the PIA report should be recorded, together with the conclusions which have led to these decisions (ISO/IEC, 2017b).

6. Designing a SaaS structure following the standards

In order to develop a model that can be compared to the GDPR's requirements, the components described on chapter 4.2 will be taken into consideration.

Furthermore, it will also be considered: the phases of the PII processing life cycle

6.1. Phases of the PII processing life cycle

PII has a life cycle, from creation or origination, collection, through storage, use and transfer to its eventual disposal. Even if the value of and risks to PII may vary during its life cycle, the protection of PII remains important to some extent at all stages and in all contexts of its life cycle (ISO/IEC, 2017c).

6.1.1. Collection

When collecting PII, organizations should always consider the privacy preferences and legal rights of the PII principal and privacy safeguarding requirements as stated by applicable law[173]. Factors such as the type of PII, lawful basis, privacy principles or any privacy preferences stated need to be considered throughout all stages of processing. Documentation should be associated with the PII, which might include: a) software tags that state the purpose(s) the PII can be used for; b) records describing the purpose(s) that PII can be used for; and c) records of the consent given and any specific sensitivities that should be observed. It is important to preserve tags that are relevant to processing PII during the usage, transfer, storage and disposal phases (ISO/IEC, 2018c).

Privacy controls should be implemented wherever data is tagged as PII or wherever PII is marked with additional information concerning the PII principal (ISO/IEC, 2018c).

PII collection processes should be designed to collect only the PII that is needed for the specific purpose. Organizations should take measures to avoid the inadvertent/unintended collection of PII through data entry systems. When free form text fields are necessary, the User Interface (UI) should provide: a) warnings to alert the PII principal not to enter PII other than that which is explicitly asked for; b) clear indication of those fields where PII is to be entered and what PII should be entered; and c) clear indication of those fields where PII should not be entered (ISO/IEC, 2018c).

[173] In case, GDPR and the Portuguese data protection law.

6.1.2. Transfer

Transfer is usually the term given for dissemination of PII from the PII controller or PII processor to other PII controllers and processors. If PII is transferred from the PII controller to another actor, transfer is sometimes also referred to as disclosure (ISO/IEC, 2018c).

Accountability and responsibility for the transferred PII should be agreed on, documented and maintained by each party involved in the PII processing (ISO/IEC, 2018c).

When relevant and appropriate, or when legally required to do so, the PII principal should be notified that transfer is taking place and should be informed of the content and purpose of the transfer. Also, where cross-border transfers are used, particular attention should be given to protection measures for the PII being transferred, considering the applicable legal requirements (ISO/IEC, 2018c).

Finally, appropriate protection mechanisms should be in place during the transfer of PII (ISO/IEC, 2018c).

6.1.3. Use

Using PII means "any form of PII processing that does not include "collect", "transfer", "store", "archive" or "dispose"" (ISO/IEC, 2018c, Chapter 6.2.3).

Protection mechanisms appropriate to the usage of PII should be applied as considered necessary by a risk analysis, which includes the use of anonymization or pseudonymization techniques prior to processing and the use of secure computation techniques during processing (ISO/IEC, 2018c).

6.1.4. Storage

PII should be stored only for the amount of time necessary to achieve the specific business purpose and with appropriate controls and mechanisms to prevent unauthorized access, modification, destruction, removal, or other unauthorized use, namely, encryption, secret sharing, pseudonymization and anonymization (ISO/IEC, 2018c).

If the PII controller or PII processor is required by applicable law to retain PII after the other purposes have expired, the PII should be locked and primary considerations in archiving PII should be to ensure that the appropriate data protection mechanisms are in place, including access management solutions (ISO/IEC, 2018c).

The PII controller should implement controls in storage systems to dispose of PII when it expires or when the purpose for the storing or processing of the PII is no longer valid (ISO/IEC, 2018c).

6.1.5. Disposal

In the final stage of the PII processing life cycle, PII gets deleted, anonymized, destroyed, returned or disposed of in some other way. It should be noted that deleting PII does not necessarily mean that the PII is ultimately disposed of because PII deleted in ICT systems can often be recovered. Specifications given by the PII principal or requirements specified by legislation (e.g., expiration date for specific PII) should be considered before PII is disposed of (ISO/IEC, 2018c).

6.2. **Privacy safeguarding requirements/Data Protection requirements**

Organizations are motivated to protect PII for several reasons: to protect the PII principal's privacy, to meet legal and regulatory requirements, to practice corporate responsibility, to enhance consumer trust, etc. Therefore, there are different factors that can influence the privacy safeguarding requirements that are relevant to a particular organization or privacy stakeholder processing PII (ISO/IEC, 2011).

Privacy safeguarding requirements are identified as part of the overall privacy risk management process being influenced by the following factors: 1) legal and regulatory factors for the safeguarding of the natural person's privacy and the protection of their PII[174]; 2) contractual factors such as agreements between and among several different actors, company policies and binding corporate rules; 3) business factors; and 4) other factors that can affect the design of ICT systems and the associated privacy safeguarding requirements (ISO/IEC, 2011, 2018b).

Privacy safeguarding requirements can relate to many different aspects of PII processing and they can also vary in specificity. They might be very general in nature, involve very specific restrictions on the processing of certain types of PII, or mandate the implementation of specific privacy controls. Moreover, the scope of the management of the personal data must be defined (ISO/IEC, 2011, 2019b).

Considering SaaS, the main security requirements are: 1) privacy in multitenant environment; 2) data protection from exposure; 3) access control; 3) communication protection; 4) software security; 5) service availability (Zissis & Lekkas, 2012).

The organization shall determine its role as a PII controller (including as a joint PII controller) and/or a PII processor and it shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) data protection, which may include: "applicable privacy legislation; applicable regulations; applicable judicial decisions; applicable organizational context,

[174] In Portugal, besides the GDPR, the Law 58/2019, the Resolution of the Council of Ministers 41/2018 and CNPD's interventions must be followed.

governance, policies and procedures; applicable administrative decisions; applicable contractual requirements" (ISO/IEC, 2019b, Chapter 5.2.1).

The organization shall "include among its interested parties those parties having interests or responsibilities associated with the processing of PII, including the PII principals, customers, supervisory authorities, other PII controllers, PII processors and their subcontractors" (ISO/IEC, 2019b, Chapter 5.2.2).

The design of any ICT system that involves the processing of PII should be preceded by an identification of relevant privacy safeguarding requirements. Moreover, the privacy implications of new or substantially modified ICT systems involving the processing of PII should be managed before those ICT systems are implemented (ISO/IEC, 2011). ICT systems should implement privacy controls in every phase of the PII processing life cycle (ISO/IEC, 2018c) and the organization shall "establish, implement, maintain and continually improve its PIMS" (ISO/IEC, 2019b, Chapter 5.2.4)

Organizations should routinely perform broad risk management activities and develop risk profiles related to their ICT systems (ISO/IEC, 2011) are related organizational controls.

Consequently, one deliverable may be a PIA, which is the component of risk management that focuses on ensuring compliance with privacy and data protection legislation requirements and assessing the privacy implications of new or substantially modified programs or activities. PIAs should be considered within an organization's broader risk management framework (ISO/IEC, 2011).

The organization shall apply the information security and privacy risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, related to the processing of PII, within the scope of the PIMS. Also, the organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified were to materialize (ISO/IEC, 2019b).

6.3. **Privacy controls**

After identifying privacy safeguarding requirements, organizations need to identify and implement privacy controls. The identified and implemented privacy controls should be documented as part of the organization's privacy risk assessment. In fact, the privacy risk assessment can assist organizations in identifying the specific risks of privacy breaches involved in an envisaged operation (ISO/IEC, 2011, 2017c).

Organizations should develop their privacy controls as part of a general "privacy by design" approach, rather than being implemented at a subsequent stage (ISO/IEC, 2011).

It is important to note that not all PII processing requires the same level or type of protection and organizations should distinguish among PII processing operations according to the specific risks they present to help determine which information security controls are appropriate in which instance. Risk management is a central method in this process and the identification of privacy controls should be an integral part of an organization's information security management framework (ISO/IEC, 2011).

Therefore, the selection of controls is dependent upon organizational decisions based on the criteria for risk treatment options and the general risk management approach, applied to the organization and, through contractual agreements, to its customers and suppliers, and should also be subject to all applicable national and international legislation and regulations (ISO/IEC, 2017c). Moreover, the selection and implementation of controls is also dependent upon the organization's role in the provision of infrastructure or services. Contractual agreements should clearly specify the PII protection responsibilities of all organizations involved in providing or using the services (ISO/IEC, 2017c).

Thus, the following controls were selected taking into consideration the GDPR's dispositions, the requirements of the Portuguese Data Protection Law, and the standards ISO/IEC 27002, 27701 and 27018.

Considering GDPR's dispositions, where proportionate in relation to processing activities, the organizational and technical measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation. shall include the implementation of appropriate data protection policies by the controller (GDPR, 2016).

The information security and privacy/data protection policies should include a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients they should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness (ISO/IEC, 2013b, 2019a). These policies should clearly allocate responsibilities between them (ISO/IEC, 2019b). Moreover, the policies should ensure the security of personal data, in accordance with the top management defined strategy. Considering the Portuguese context this must include: the prioritization and classification of data according to sensitivity criteria and predefined criticality; the creation; the modification; the transmission; the collection (regardless of the means or process); the destruction; the storage (including retention); the data search (Conselho de Ministros, 2018). The general rule is that retention period of personal data is the one set by law, or, in its absence, what may prove necessary for the pursuit of the purpose of the data processing. Moreover, to define the retention period, contractual obligations should also be considered. After that period, the controller should destroy or anonymize that data (Assembleia da República, 2019, Article 21).

Contractual agreements should clearly allocate responsibilities between the public cloud PII processor, its sub-contractors and the CSC, considering the type of cloud service in question. In order to ensure the public cloud PII processor is obliged to support and manage compliance is provided by the contract between the CSC and the public cloud PII processor. The contract can call for independently audited compliance, acceptable to the CSC and the public cloud PII processor should designate a point of contact for use by the CSC regarding the processing of PII under the contract (ISO/IEC, 2019a, 2019b). The contract must follow GDPR's dispositions on Article 24 or, when applicable, on the Article 26.

All information security responsibilities should be defined and allocated, and conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Moreover, appropriate contacts with relevant authorities should be maintained and identified information security incidents should be reported in a timely manner (ISO/IEC, 2013b).

Information security should be addressed in project management, regardless of the type of the project and appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained (ISO/IEC, 2013b).

Measures should be put in place to

> make relevant staff aware of the possible consequences on the public cloud PII processor (e.g. legal consequences, loss of business and brand or reputational damage), on the staff member (e.g. disciplinary consequences) and on the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII (ISO/IEC, 2019a, Chapter 7.2.2)

and "the contractual obligations for employees or contractors should reflect the organization's policies for information security" (ISO/IEC, 2013b, Chapter 7.1.2). Appropriate periodic training for personnel having access to PII should be given (ISO/IEC, 2019b)

Assets associated with "information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained" (ISO/IEC, 2013b, Chapter 8.1.1) and awareness of information assets with respect to personal data must be ensured at all times in order to make it possible to unambiguously identify the state of the information throughout its life cycle (Conselho de Ministros, 2018).

Information should be "classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification" (ISO/IEC, 2013b, Chapter 8.2.1) and the organization's information classification system should include PII as part of the scheme it implements.(ISO/IEC, 2019b). People under the organization's control must be made aware of the definition of PII and how to recognize information that is PII (ISO/IEC, 2019b). Therefore, systems must allow to classify, prioritize, search, edit and delete personal data as well as they shall have the necessary controls in place for the identification, authentication, access and validation of stored personal data (Conselho de Ministros, 2018). Moreover, if physical media is used for information transfer, a system should be put in place to

> record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, the number of physical media and, where possible, additional measures such as encryption should be implemented to ensure that the data can only be accessed at the point of destination and not in transit (ISO/IEC, 2019b, Chapter 6.5.3.3).

An access control policy should be established, documented and reviewed based on business and information security and data protection requirements and asset owners should determine appropriate access control rules, both logical and physical, access rights and restrictions for specific user roles towards their assets (ISO/IEC, 2013b).

In the context of the cloud computing services, the CSC may be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should allow the CSC to manage access by cloud service users under the CSC's control, such as by providing administrative rights to manage or terminate access (ISO/IEC, 2019a). Thus, these responsibilities should be documented (ISO/IEC, 2019b).

A formal user registration and de-registration process should be implemented to enable assignment of access rights and procedures for user registration and de-registration should address the situation where user access control is compromised (ISO/IEC, 2013b, 2019a, 2019b). Implementing individual user access IDs enables appropriately configured systems to identify who accessed PII and what additions, deletions or changes they made. As well as protecting the organization, users are also protected as they can identify what they have processed and what they have not processed and, therefore, the organization should not reissue to users any de-activated or expired user IDs for systems and services that process

PII, being done the creation of profiles with minimum privileges, accordingly with the principle of need-to-know (Conselho de Ministros, 2018; ISO/IEC, 2019b).

A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services and the allocation and use of privileged access rights should be restricted and controlled. Also, asset owners should review users' access rights at regular intervals and the access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change (ISO/IEC, 2013b). The organization should keep an accurate, up-to-date record of the user profiles created for users who are authorized to access to the information system and the PII contained therein (ISO/IEC, 2019b).

Considering the FE, there must be a user account renewal process in accordance with the same security requirements of its creation, and it should not have a life cycle longer than 180 days. The management of the user account lifecycle should take into account the segregation of existing roles and access privileges that should be associated with these functions at all times. Moreover, there must be an association of data typology with specific, individual and associated with the role profiles, with minimal privileges, where each type of profile is defined according to the type of personal data the user may access and actions the user can do on personal data (CRUD) according to the principle of need-to-know (Conselho de Ministros, 2018).

For the application layer and DB, there must be a management process to validate profiles. Also, there must be an automated or interoperable process with systems managing the roles associated with the privileges assigned to each profile. In cases of asynchronous checking of Role/Privileges, this should be done on a periodic basis, every two months at least, or when there is a change in the personnel map associated with that role. There must be an association of data typology with specific, individual and associated with the role profiles, with minimal privileges, where each type of profile is defined according to the type of personal data the user may access and actions the user can do on personal data (CRUD) according to the principle of need-to-know. Finally, there must be a process of recording attempts to access data excluded from privileges associated with the profile (any profile, including the profile of administrators), with alarmistic from a certain number of attempts (e.g. 3 attempts), to notify the DPO of the organization (Conselho de Ministros, 2018).

The allocation of secret authentication information should be controlled through a formal management process and this should be done in accordance with the attribution of access rights policy. Furthermore, the credentials should be provided to the user in an auditable way, without allowing the access to other people than the proper user (Conselho de Ministros, 2018; ISO/IEC, 2013b). The integrity of the DNS zones where the system and the surrounding ecosystem is located must be ensured, using the best practices of DNSSec and configuration of email systems (Conselho de Ministros, 2018).

Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure and the public cloud PII processor should provide secure log-on procedures for any accounts requested by the CSC for cloud service users under its control (ISO/IEC, 2013b, 2019a). Considering the FE, the authentication process should always be started and kept in secure session. It is recommended: 1) the use of TLS in its latest version; or 2) the use of password, preferably in combination with another factor (2FA). Session data with personal information should be excluded from URL variables or other user-visible variables. The login credentials should be transmitted through their HASH, Secure Hash Algorithm-256 (SHA-256), or it should be used a cipher or coding for the transmission of personal data (name or username and password in HASH and other encrypted data). Moreover, where applicable, the password must be at least 9 characters (13 characters for privileged users) and be complex - its composition should require the inclusion of 3 of the following 4 character sets: lowercase letters (a... z), capital letters (A... Z), numbers (0... 9) and special characters (˜! @ # $% ^ & * () _ + | `- = \ {} []:“; ‘<>?,. /). Alternatively, it may consist of sentences or excerpts of long text known to the user, without a “space” character (Conselho de Ministros, 2018).

As for the application layer and the database, the password must be at least 13 characters and be complex - its composition should require the inclusion of 3 of the following 4 character sets: lowercase letters (a... z), capital letters (A... Z), numbers (0... 9) and special characters (˜! @ # $% ^ & * () _ + | `- = \ {} []:“; ‘<>?,. /). Alternatively, it may consist of sentences or excerpts of long text known to the user, without a 'space' character. All users with administrator rights must use 2FA (Conselho de Ministros, 2018). Furthermore, the communication between the application layer and the FE and the DB must be done with a secure session, with previous authentication. If the layers are physically or logically separated, the authentication process must be done and guaranteed by validating the static IP address + hostname + MacAdress + authentication factors or by using certificates (Conselho de Ministros, 2018).

The public cloud PII processor should provide information to the CSC regarding the circumstances in which it uses cryptography to protect the PII it processes and it should also provide information to the CSC about any capabilities it provides that can assist the CSC in applying its own cryptographic protection (ISO/IEC, 2019a).

Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment and where the use of PII for testing purposes cannot be avoided a risk assessment should be undertaken (ISO/IEC, 2013b, 2019a). There must be implemented detection, prevention and recovery controls to protect against malware, combined with appropriate user awareness (ISO/IEC, 2013b). This must include: threat detection in the perimeter of the system (e.g. firewall rules, Intrusion Detection System - IDS, etc.); extension of this protection to all devices with access to personal data in corporate systems; an end-to-end encryption mechanism whenever there is a need to remotely access the FE, such as using VPN technology. Furthermore, the FE must be developed and implemented in accordance with the best security practices, guaranteeing the protection against the most common attacks, such as SQLi, code injection, etc. The application layer and the DB must be segregated from the network or environment visible or accessible from the exterior. Also, the DB must include masking, anonymization or encryption of data that is transmitted or accessed (Conselho de Ministros, 2018).

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. This policy must include the organization's requirements for backup of information, software and systems, recovery and restoration of PII, and it should define the retention and data protection requirements, which may include contractual and/or legal requirements for the erasure of PII contained in information held for backup requirements.(ISO/IEC, 2013b, 2019b).

Usually, systems based on the cloud computing model introduce additional or alternative mechanisms to off-site backups for protecting against loss of data, ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a disruptive event. Therefore, multiple copies of data in physically and/or logically diverse locations should be created or maintained for the purposes of backup and/or recovery and procedures should be put in place to allow for restoration of data processing operations within a specified, documented period after a disruptive event. The backup and recovery procedures should be reviewed at a specified, documented frequency (ISO/IEC, 2019a).

When PII needs to be restored, processes need to be in place to ensure that the PII is restored into a state where the integrity of PII can be assured, and/or where PII inaccuracy and/or incompleteness is identified and processes put in place to resolve them. The organization should have a procedure for, and a log of, PII restoration efforts, which must include, at a minimum: the name of the person responsible for the restoration and a description of the restored PII (ISO/IEC, 2019b).

PII-specific responsibilities in this respect can lie with the CSC. In these cases, the organization should ensure that the CSC has been informed of the conditions of the service regarding backup (ISO/IEC, 2019b). However, when the public cloud PII processor explicitly provides backup and restore services to the CSC, it should provide clear information to the CSC about the capabilities of the cloud service with respect to backup and restoration of the CSC's data (ISO/IEC, 2019a).

Overall, storage systems must ensure redundancy and availability, and there should be no single point of failure. In order to ensure it, the processing and storage architecture must ensure the properties of redundancy, resiliency and availability and there must be two types of backups (on and offsite), which must meet the same security requirements defined for production systems. Also, offsite backups should be stored in a location that is not exposed to the same external risks as the original location (Conselho de Ministros, 2018).

Moreover, event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed and, therefore, a process must be defined to review event logs using continuous, automated monitoring and alerting processes, or else manually where such review should be performed with a specified, documented periodicity, to identify irregularities and propose remediation efforts (ISO/IEC, 2013b). Where possible, event logs should record access to PII, including by whom, when, which PII principal's PII was accessed, and what (if any) changes were made (CRUD) as a result of the event. When the organization acts as a processor (such as public cloud PII processor), it should define criteria regarding if, when and how log information can be made available to or usable by the CSC and these criteria should be made available to the CSC. Where the organization permits its CSCs to access log records controlled by the organization, the organization should implement appropriate controls to ensure that the CSC can only access records that relate to that CSC's activities and cannot amend the logs in any way (ISO/IEC, 2019b, 2019a).

Thus, an activity log should be kept of all actions a user takes on personal data, regardless of their profile and role. Moreover, it should be ensured that activity records from different subsystems (Operating Systems, Applications, Browsers, Database Management System - DBMS, etc.) are unambiguously associated with their origin and logs must contain at least the access address (IP and Port), Host, HASH of the user account that performed the action, action taken (CRUD), personal data type where the action was taken, timestamp of the action, and the particular change made to the personal data (Conselho de Ministros, 2018).

It is important to point out that where multiple service providers are involved in providing services, there can be varied or shared roles. Thus, these roles should be clearly defined and documented and an agreement on any log access between providers should be made (ISO/IEC, 2019b).

In accordance, logging facilities and log information should be protected against tampering and unauthorized access and a procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified as specified in the retention schedule (ISO/IEC, 2013b, 2019b, 2019a). All logs should be stored in read-only mode and should, within a maximum period of 1 month, be enclosed in a single block of records and digitally signed (integrity guarantee). This must include a log of all accesses and failed access attempts (Conselho de Ministros, 2018).

Considering information transfer policies and procedures, those, as well as related controls, should be in place to protect the transfer of information through the use of all types of communication facilities and the organization should consider procedures for ensuring that rules related to the processing of PII are enforced throughout and outside of the system, where applicable (ISO/IEC, 2013b, 2019b). Also, whenever physical media are used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII (including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media) and, where possible, CSCs should be asked to put additional measures in place, such as encryption, to ensure that the data can only be accessed at the point of destination (ISO/IEC, 2019a). Under the Portuguese context, the information technologies to be implemented must allow the portability and export of personal data. Moreover, the use of compatible digital formats should be ensured, guaranteeing technical and semantic interoperability within the Public Administration, in interaction with the citizen or the company, and for the provision of content and services (Conselho de Ministros, 2018). It is also important to consider that the portability right is only applicable to the data provided by the data subject and that data portability should take place on an open format (Assembleia da República, 2019).

There should be taken into consideration the requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information, and they should be regularly reviewed and documented. The organization should ensure that individuals operating under its control with access to PII are subject to a confidentiality obligation and the confidentiality agreement, whether part of a contract or separate, should specify the length of time the obligations should be adhered to, including policies and procedures concerning data protection (ISO/IEC, 2013b, 2019b). This control goes along with GDPR's dispositions on Article 28(3)(b), and on a broader sense, with the dispositions on Article 24(1).

The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems and information involved in application services passing over public networks should be protected from any unauthorized disclosure, misuse and/or modification (ISO/IEC, 2013b). Therefore, the organization should ensure that PII that is transmitted over untrusted data transmission networks is encrypted for transmission (ISO/IEC, 2019b), as well as applied, documented and maintained principles for engineering secure systems should be established (ISO/IEC, 2013b). This include establishing policies for system development and design, which should include guidance for the organization's processing of PII needs, based on obligations to PII principals and/or any applicable legislation and/or regulation and the types of processing performed by the organization (ISO/IEC, 2019b). Policies that contribute to privacy by design and privacy by default should consider the following elements:

> a) guidance on PII protection and the implementation of the privacy principles in the software development lifecycle; b) privacy and PII protection requirements in the design phase, which can be based on the output from a privacy risk assessment and/or a privacy impact assessment; c) PII protection checkpoints within project milestones; d) required privacy and PII protection knowledge; e) by default minimize processing of PII (ISO/IEC, 2019b, Chapter 6.11.2.1).

On the Portuguese context, it is considered that client applications must be developed adopting secure development practices. Considering the FE, it is mandatory to follow the best practices on software development, such as the ones defined by OWASP. Moreover, it is mandatory the use of secure sessions with a cryptographic protocol being the latest version of TLS the one recommended. It is also mandatory to not store personal information in your browser, memory or disk to beyond the session time and only to the extent necessary. As for the application layer, it mandatory the use of secure sessions with a cryptographic protocol. Finally, for the DB, it is mandatory that the communication with application layer is done through authentication by certificate valid for a period not exceeding 2 years in the case of layers are physically or logically distinct and that personal data is encrypted if the client application has a physically and logically distinct DB layer, preferably using technology that allows interoperability between systems (Conselho de Ministros, 2018).

It is important to point out that PII should not be used for testing purposes and, instead, false or synthetic PII should be used (ISO/IEC, 2019b).

All relevant information security requirements should be established, agreed and documented with suppliers that may access, process, store, communicate, or provide IT infrastructure components for the organization's information/personal data The agreements should clearly allocate responsibilities between the organization, its partners, its suppliers and its applicable third parties (customers, suppliers, etc.) considering the type of PII processed and the minimum technical and organizational measures that the supplier needs to meet in order to the organization to meet its information security and PII protection obligations. Also, the organization should specify in contracts with any suppliers that PII is only processed on its instructions (ISO/IEC, 2013b, 2019b) These dispositions go along with GDPR's Article 28.

Considering security incidents/data breaches, management responsibilities and procedures should be established to ensure a quick, effective and orderly response, which might include a notification to required parties of PII breaches and the disclosure to authorities and/or PII principals, considering the applicable legislation and/or regulation (GDPR and Portuguese Data Protection Law) (ISO/IEC, 2013b, 2019b). These dispositions are compliant with GDPR's Articles 28, 33 and 34.

Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as:

> a description of the incident; the time period; the consequences of the incident; the name of the reporter; to whom the incident was reported; the steps taken to resolve the incident (including the person in charge and the data recovered); the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII; a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify PII principals, regulatory agencies or customers (ISO/IEC, 2019b, Chapter 6.13.1.5).

These dispositions are compatible with the GDPR's Article 33 and 34, as well as the accountability and transparency principles.

Provisions covering the notification of a breach involving PII should form part of the contract between the organization and the CSC, that should define expected and externally mandated limits for notification response times. In some jurisdictions, the PII processor should notify the PII controller of the existence of a breach without undue delay (such as the ones covered by GDPR), preferably, as soon as it is discovered so that the PII controller can take the appropriate actions (ISO/IEC, 2019b, 2019a). These dispositions are in accordance with GDPR's Article 28.

Moreover, "all relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization" (ISO/IEC, 2013b, Chapter 18.1.1) and, in accordance, the organization should identify any potential legal sanctions related to the processing of PII (ISO/IEC, 2019b). The organization should retain copies of its privacy policies and associated procedures for a period as specified in its retention schedule, which includes retention of previous versions of these documents when they are updated (ISO/IEC, 2019b).

The organization's approach to "managing information security and its implementation should be reviewed independently at planned intervals or when significant changes occur" (ISO/IEC, 2013b, Chapter 18.2.1). Where an organization is acting as a PII processor, and where individual CSC audits are impractical or can increase risks to security, the organization should make available to CSCs, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the organization's policies and procedures. Alternatively, a relevant independent audit should be an acceptable method for fulfilling the CSC's interest in reviewing the organization's processing operations, if it covers the needs of users and if results are provided in a transparent manner (ISO/IEC, 2019b, 2019a).

Finally, information systems should be regularly reviewed for compliance with the organization's information security policies and standards and this process shall include methods of reviewing those tools and components related to processing PII, such as ongoing monitoring to verify that only permitted processing is taking place; and/or specific penetration or vulnerability tests (ISO/IEC, 2013b, 2019b).

6.4. Privacy architecture framework overview

The privacy architecture framework is intended as a technical reference for developers of ICT systems that process PII, focusing on its protection (ISO/IEC, 2011). Furthermore, the functionality of the ICT system of the PII principal can be split across different ICT hardware systems owned by the PII principal and the PII controller. Similarly, the PII controller can provide the ICT system of the PII processor (ISO/IEC, 2018c).

When developing and maintaining the inventory concerning ICT systems, organizations should consider the following information elements:

> a) name of and acronym for each identified system; b) types of PII processed by those systems; c) classification of all types of PII, both as individual information elements and as combined in those information systems; d) level of potential impact, to the PII principal and the organization, of any breach of PII; e) purpose(s) for collecting the PII; f) whether PII processing will be outsourced to a PII processor; g) whether PII is transmitted to other PII controllers, and if so, to whom (or to which group of recipients); h) retention period of PII; i) geographical area where the PII was collected or processed; and j) whether trans-border data transfer is involved (ISO/IEC, 2017c, Chapter 8.1.2).

Development, testing and operational environments should be logically and, where possible, physically separate environments and appropriate access controls should be implemented to ensure access is limited to properly authorized individuals (ISO/IEC, 2017c).

Business processes in which ICT systems are employed use a wide range of communication and trust models. Therefore, the architecture framework described on ISO/IEC 29101 builds on an abstraction of these models (ISO/IEC, 2018c).

The architectural views defined on ISO/IEC 29101 are structured into three views (ISO/IEC, 2018c).

First, the component view, which describes the ICT system components in detail and separates them into layers based on their functionality and groups components that help to contribute to the proper processing of PII. The main plus of this view is that is helpful for understanding the building blocks in the privacy architecture framework (ISO/IEC, 2018c).

Second, the actor view, that looks at the components described in the component view from the perspective of the ICT system of an individual actor. This view is helpful in the design of the architecture of a specific ICT system (ISO/IEC, 2018c).

Third, the interaction view, which looks at the components from a deployment perspective. This view is helpful for understanding how components in the ICT systems of different actors interact with each other (ISO/IEC, 2018c).

6.4.1. Component view

The component view is meant to describe ICT system components that are involved in the processing of PII and the choice of components should be guided by the appropriate data protection requirements. The developer of the ICT system for a specific actor(s) should use the component view to determine the components that need to be included in the architecture of the system that they are developing, considering the already established data protection requirements (ISO/IEC, 2018c).

The component view is presented in three layers and each layer is a logical group of components that contributes to a specific goal in the processing of PII: there are the privacy settings layer, the identity management and access management layer and the PII layer (ISO/IEC, 2018c).

The architecture framework is designed with the assumption that all components interact with other components. Some of the components in the architecture framework are PETs. However, this selection of PETs is not comprehensive, and the developer of the ICT system is responsible for choosing appropriate PETs and adapting them to this architecture framework (ISO/IEC, 2018c).

6.4.1.1.Privacy settings layer

Components in the privacy settings layer handle the management of metadata about PII processing. This layer includes components that communicate the system privacy policy to the relevant actors and implement the system data protection requirements. These components let the ICT system communicate the system privacy policy and implement the corresponding data protection measures. Thus, this layer is constituted by the following components: policy and purpose communication; PII categorization; consent management; privacy preference management (ISO/IEC, 2018c).

In addition, the components in this layer should deliver to the PII controller and PII processor the privacy preferences and consent information, when applicable, that have been collected from the PII principal (ISO/IEC, 2018c).

The **component of policy and purpose communication** is responsible for relaying information about the privacy policy of the PII controller and the purpose of PII collection to the ICT systems of privacy stakeholders. The communicated information should contain at least the following:

> a) the identities of the PII controllers and any associated PII processors; b) policies regarding the transfer of PII to PII processors; c) the use of PETs (such as anonymization) with their respective goals; d) the purposes for which the PII is collected; e) identification of the PII to be collected; and f the legal rights of the PII principal to access their PII to determine the extent of the PII stored and to check for and correct any inaccuracies, and the procedures for doing so (ISO/IEC, 2018c, Chapter 8.2.2.2).

As for the PII principal, the policy and purpose communication component of the ICT system of the PII principal should:

> a) receive policy and purpose information from the corresponding component in the ICT system of the PII controller; b) interpret the received information and display or otherwise convey to the PII principal in a clearly comprehensible manner its meaning; c) offer the PII principal the opportunity to locally store the received information; and d) confirm to the PII controller that the policy and purpose information has been received by the PII principal (ISO/IEC, 2018c, Chapter 8.2.2.2).

On the other hand, the policy and purpose communication component of an ICT system under the control of the PII controller should:

a) store policy and purpose information that has been conveyed to PII principals; b) log the acts of conveying policy and purpose information to PII principals in such a way that it can be established which information was current and was conveyed to PII principals at which time, along with confirmation of receipt of this information; c) convey the current policy and purpose information to the corresponding component of the ICT system of the PII principal in such a manner that it can be used by this system directly to inform the PII principal in a complete and comprehensible manner, or that it can be mapped by said component to such a form by some pre-defined mapping; d) convey a reference to the displayed policy and purpose information to those components which handle the storage of consent information and storage of PII itself; and e) transmit updates about changes to policy and purpose information to the corresponding components of the ICT systems belonging to those PII principals who have consented to receive such information (ISO/IEC, 2018c, Chapter 8.2.2.2).

It is important to point out that the PII controller can arrange the processing of PII by various PII processors and, therefore, the purpose communication component in the ICT system of the PII controller should transmit the purpose associated with the PII provided to all relevant PII processors (ISO/IEC, 2018c).

Finally, the ICT system of the PII processor typically should present the privacy policy and processing purpose documentation in a clearly comprehensible form to everyone with access to PII governed by that policy, as it should have received digital copies of the privacy policy and the processing purpose from the ICT system of the PII controller (ISO/IEC, 2018c).

Considering the **PII categorization component**, it is important that an ICT system processing PII is aware of the categories of PII that it processes, so that it can distinguish between different types of data, in order that those are processed and stored by the ICT system in accordance with its marked sensitivity. Moreover, the ICT system should be aware of PII values that contain direct identifiers. Thus, this component should implement the functions that provide such a categorization in the ICT system (ISO/IEC, 2018c). A classification scheme may also include more specific categories, but the actual categories used should also depend upon the requirements defined in relevant data protection legislation and regulations, other legal/contractual obligations, the nature and sensitivity of the information, and the risk of harm that might arise in the event of a breach (ISO/IEC, 2017c).

When dealing with non-PII, the risk of combining non-PII to infer or derive an identity or profile of a user or an enough subset of users should be taken into consideration and evaluated. Moreover, it is also important to consider measures to minimize the possibility of unsolicited PII collection (ISO/IEC, 2018c).

The ICT system of the PII principal should be able to identify and process the PII and should process the PII in accordance with its category (ISO/IEC, 2018c).

The ICT system of the PII controller should contain a comprehensive categorization of PII used in the ICT systems and this information should be transmitted to PII processors. Also, this categorization can be used by the audit logging, PII pseudonymization, PII disclosure and PII archiving and retention components in order to determine which parts of the data contain PII (ISO/IEC, 2018c).

The ICT system of the PII processor should be capable of processing the received and categorized PII and this information should be used in PII auditing and secure PII processing (ISO/IEC, 2018c).

Consent of the PII principal is an important prerequisite of PII processing, unless such processing is otherwise permitted by law or other lawful basis, as defined on ISO/IEC 27701 and GDPR.

The **consent management component** handles related tasks including, but not limited to:

> a) obtaining the informed consent of the PII principal; b) storing consent information in the ICT systems of a privacy stakeholder; c) relating the stored consent information to the version of policy and purpose information for which the consent was given; d) checking consent prior to PII processing; and e) maintaining the status of consent information (ISO/IEC, 2018c, Chapter 8.2.2.4).

Applicable law can result in the overriding of absence or limitation of consent expressed by the PII principal. In those cases, the following procedure is recommended: a) inform the PII principal of the lawful basis on which the processing is based on; b) store the receipt of the delivered notice in the ICT systems of a privacy stakeholder; c) related the previous information to the version of the policy and purpose information; d) verity the maintenance of the processing status and the lawful basis.

When needed, the PII controller should obtain the informed consent of the PII principal and keep this information updated, since under certain circumstances, the PII principal can modify or withdraw consent and this information should be communicated to the ICT system of the PII controller. Thus, the ICT system of the PII controller should maintain up to date information about the status of consent/lawful basis. The ICT system of the PII controller should be capable of retrieving, storing, managing and maintaining the consent information/lawful basis and related notice. Moreover, the ICT system of the PII controller should transmit consent information/lawful basis to other parties in the system that require it (ISO/IEC, 2018c).

The ICT system of the PII processor should verify the existence of consent/lawful basis and related policies/notices from all PII principals associated with the PII provided to it. This information should come from the ICT system of the PII controller. Before any processing, the ICT system of the PII processor should make sure that it has current consent information about the respective PII principals or another lawful basis that supports the processing activities. The ICT system of the PII processor should be able to accept changes to the consent status when such changes are notified by the PII controller (ISO/IEC, 2018c).

Regarding the **privacy preference management**, in some situations, it is possible that the PII principal can express his/her preferences as to how his/her PII is processed by a PII controller or processor. Thus, the respective ICT systems should be able to record those preferences and make them known to the PII controller and processor as appropriate, which should be capable of understanding those preferences and, to the maximum extent possible, respect those preferences when processing PII (ISO/IEC, 2018c).

6.4.1.2.Identity management and access management layer

Components in the identity and access management layer help to identify the actors and their ICT systems and manage the related intity information. Additionally, components in this layer control how the actors access PII and provide identity information to components in other layers that require it. The components implement the following functionality:

> a) managing the identities of the privacy stakeholders; b) managing the identities of the actors who are using the ICT systems; c) providing this information to other components in the ICT systems; and d) managing the mappings between PII principal identities and pseudonyms for the pseudonymization of PII (ISO/IEC, 2018c, Chapter 8.2.3.1).

This layer is, therefore, constituted by the following components: 1) identity management system; 2) pseudonymization scheme; 3) access control; 4) authentication; and 5) authorization (ISO/IEC, 2018c).

The **identity management system** can have several purposes.

This component can manage the identities of the PII principals whose PII is processed in the ICT system, as well as it can manage the identities of the users of the ICT systems that process PII. It also can manage the identities of the ICT systems of the privacy stakeholders. Thus, the ICT systems of different privacy stakeholders can mutually authenticate each other during PII transfer (ISO/IEC, 2018c).

When the **pseudonymization scheme** is used in PII processing, the ICT systems should have functions for managing the individual pseudonymization function instances that are in use. The pseudonymization scheme component in the identity and access management layer contains information about the implemented pseudonymization scheme and its parameters; on the other hand, the related PII pseudonymization component in the PII layer is used to perform the actual transformations on PII (ISO/IEC, 2018c).

Considering **access control mechanisms,** they should ensure that access to the features in the PII-handling ICT system is only granted within the restrictions set by the data protection requirements. The functionality of this component is similar for all actors and the rules and methods for access control in each ICT system are drawn from the data protection requirements (ISO/IEC, 2018c). Nevertheless, it should be adopted the principle of segregation of duties when assigning access rights for PII processing, especially with processing identified as high risk. Access to PII being processed and access to log files concerning that processing should be implemented as separate duties (ISO/IEC, 2017c). Moreover, in order to prevent the abuse of PII, privileged access rights for PII processing should be assigned on a strictly limited basis and the granting and use of such rights should be recorded in relevant log files. All access approvals should be for a specified period and organizations should review all approvals on a regular basis and as appropriate, renew, revoke or expire approvals as appropriate (ISO/IEC, 2017c).

Authentication is an important security component of an ICT system that processes PII, since it can guarantee the confidentiality and integrity of PII collected, stored and processed by the system. Furthermore, this component might have several purposes: it can handle the authentication of the users operating the ICT system and it can handle the mutual authentication of ICT systems or their components as part of secure PII access and transfer (ISO/IEC, 2018c). Organizations should adopt strong authentication methods for processing of sensitive data (ISO/IEC, 2017c).

The rules and methods used in each deployment of the ICT system should be considered separately, considering the security objectives of the actor who uses the ICT system (ISO/IEC, 2018c).

Authorization is important in ICT systems where the access of any actor is restricted: only authorized users of the ICT system should be given access to PII. The functionality of the authorization component is similar for all actors and the rules and methods for authentication in each ICT system are derived from the data protection requirements (ISO/IEC, 2018c).

6.4.1.3.PII layer

The PII layer is constituted by the following components: 1) PII management; 2) PII transfer; 3) PII validation; 4) PII pseudonymization; 5) PII anonymization; 6) secret sharing; 7) PII encryption; 8) PII use; 9) secure computation; 10) query management; 11) PII inventory; 12) PII disclosure; 13) PII archiving and retention; 14) audit logging (ISO/IEC, 2018c).

The PII layer uses information from the privacy settings layer to apply the measures in the data protection requirements that relate to the processing of PII. Therefore, the components in the PII layer should have the following functionalities: PII collection and transfer, PII processing (including secure processing, and presentation), storing and archiving of PII; and auditing PII and logging transactions occurring on it (ISO/IEC, 2018c).

The ISO/IEC 29101 standard only proposes generic PII management requirements (ISO/IEC, 2018c).

PII management is important, considering that any ICT system processing PII should have certain basic features for managing PII in the ICT system, such as PII entry, access, update and removal (ISO/IEC, 2018c). The PII management component of the ICT system of the PII principal is focused on the collection and local processing of PII collected from the PII principal. As for the PII management component of the ICT system of the PII controller, it should be able to collect PII from the ICT systems of the PII principals and to deliver/delegate processing to PII processors. Finally, the PII management component of the ICT system of the PII processor handles the PII received from the PII controller (ISO/IEC, 2018c).

PII transfer component is responsible for PII exchanges between the ICT systems of the various privacy stakeholders, which should include mutual authentication and encryption between the source and destination points, in order to ensure confidentiality (ISO/IEC, 2018c).

PII validation is also to be considered, since the PII that is being processed should be validated for accuracy of data and adequacy of format (ISO/IEC, 2018c).

The **PII pseudonymization** component in the PII layer uses a pseudonymization scheme as described in the identity and access management layer to replace the identifiers that reveal the identity of PII principals with pseudonyms or alias that hide their true identities (ISO/IEC, 2018c).

The **anonymization** process takes PII and removes all personal identifiers or otherwise irreversibly alters it in such a way that a PII principal can no longer be identified (ISO/IEC, 2018c).

Secret sharing is a technique for distributing PII values into shares that individually reveal no information about the original value. Secret sharing enhances privacy when performed at the ICT system of the PII principal and used in conjunction with secure multiparty computation (ISO/IEC, 2018c).

PII encryption components should provide mechanisms for encrypting PII before it is stored and during the design of an ICT system it should be defined which stored PII needs to be encrypted. Depending on the data protection requirements, the encryption keys can be shared between ICT systems so each of them can decrypt the PII and access it appropriately. The component services include key management, encryption of PII within databases and encryption of stored PII such as backup files and archives (ISO/IEC, 2018c).

In order to proceed with **PII use** in computations or analyses, the ICT system of the actor should implement a PII use component, which implements the business logic of the PII processing (ISO/IEC, 2018c).

Secure computation can be used to let PII controllers and PII processors process PII without having access to the raw input values, being processed PII that has been transformed by PETs, such as encryption or secret sharing (ISO/IEC, 2018c).

The **query management** component of the ICT system of the PII controller and/or PII processor is deployed for filtering incoming queries (ISO/IEC, 2018c). Before allowing individuals to use query languages that enable automated massive retrieval of PII from databases that contain PII, organizations should review the necessity to use such languages when processing PII. Where the use of query languages is consistent with the protection requirement, organizations should provide technical measures to limit the use of such languages to the minimum necessary to fulfil the specified purpose(s) (ISO/IEC, 2017c).

The **PII inventory** component provides an overview of the PII stored in the ICT system, in accordance with the information from the PII categorization system (ISO/IEC, 2018c).

The **PII disclosure** component is responsible for managing any disclosure of PII by the PII controller and often requires the use of the PII transfer component. PII can be disclosed by the ICT system of the PII processor in a similar manner as in the ICT system of the PII controller, but this disclosure should be performed in accordance with the directions of the PII controller (ISO/IEC, 2018c).

The **PII archiving and retention** component should ensure that the archive is sufficiently protected and that archiving and retention procedures are followed (ISO/IEC, 2018c). Information systems processing PII should introduce additional or alternative mechanisms, such as off-site backups for protection against loss of PII, ensuring continuity of PII processing operations, and providing the ability to restore PII processing operations after a disruptive event, if only strictly necessary (ISO/IEC, 2017c). PETs can be used to protect archived PII from unauthorized processing. However, when the PII retention period has passed, this component should schedule the anonymization or secure removal of the PII from the system (ISO/IEC, 2018c).

The **audit logging** component should log each transaction performed on PII and this component should be integrated with every other component so that it can log all relevant activities and the audit logging component should be integrated with the authentication, authorization and PII layer modules. Secure logging techniques should be used to prevent tampering with the log entries (ISO/IEC, 2017c, 2018c). A process should be put in place to review the event log with a specified, documented periodicity to identify irregularities and propose remediation efforts. The PII controller should define procedures regarding whether, when and how log information can be made available to or usable by the administrator (ISO/IEC, 2017c). Finally, the clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source, since the correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases (ISO/IEC, 2013b, 2017c).

6.4.2. Actor view

The actor view shows how the components in the architecture framework of the ISO/IEC 29101 are deployed into the ICT systems of each privacy stakeholder (ISO/IEC, 2018c).

6.4.2.1.PII principal

The ICT system of the PII principal focuses on providing PII. Therefore, the ICT system in use by the PII principal should contain components for securing PII mainly during collection (ISO/IEC, 2018c).

6.4.2.2.PII controller

The ICT system of the PII controller should manage the collection and processing of all PII, based on the latest privacy policy, data protection requirements and any privacy preferences that have been collected from the PII principal. Thus, the privacy settings components should always contain up-to-date information about policy and purposes (ISO/IEC, 2018c).

Additionally, the PII controller manages the processing of PII by PII processors, which includes oversight and responsibility for enforcement of the applicable privacy policies and any consent limitations and privacy preferences that have been collected from the PII principal. Therefore, the PII controller must communicate this information to the PII processors, as well as to monitor their behaviour and take remedial action if the limitations and preferences are not applied. Furthermore, the controller can apply PETs to further reduce the chance that the ICT system of the PII processor can determine the PII principal associated with PII (ISO/IEC, 2018c).

6.4.2.3.PII processor

The PII processor uses its ICT system for processing PII in accordance with the instructions/agreement/contract with the PII controller. The ICT system of the PII controller communicates the policy and privacy preference information associated with the PII. Moreover, the ICT system of the PII processor should be capable of supporting PII transformed by PETs (ISO/IEC, 2018c).

6.4.3. Interaction view

The interaction view describes how the components deployed in the ICT systems of different privacy stakeholders interact and this view is constituted by three layers: 1) the privacy settings layer; 2) the identity and management access layer; and 3) PII layer (ISO/IEC, 2018c).

6.4.3.1.Privacy settings layer

The privacy settings layer includes services and information governing all aspects of PII processing and it includes the policy and purpose communication; PII categorization; consent management; and privacy preference management (ISO/IEC, 2018c).

6.4.3.2.Identity and access management layer

Some identity management services are generic and are used by all actors. However, not all the actors should share all the identity information: the principle of least privilege should be followed and each ICT system should only have access to identity information it requires. This layer includes the identity management system, the pseudonymization scheme, access control, authentication and authorization (ISO/IEC, 2018c).

6.4.3.3.PII layer

The PII layer contains globally used services such as general PII management and PII inventory. It includes, for the ICT systems of all actors: PII management, PII transfer, PII validation, PII pseudonymization, PII anonymization, secret sharing, PII encryption, PII use, PII inventory, PII archiving and retention and audit logging, Moreover, it also includes for the ICT system of the PII controller and PII processor: secure computation, query management and PII disclosure (ISO/IEC, 2018c).

7. METHODOLOGY

7.1. Preliminary considerations

The comparative law research method was chosen for the current study.

Considering that GDPR is technologically neutral, a comparison with standards that could provide further guidance on best practices and on how to technically implement controls that enhance data protection and privacy was taken into account.

Certification has as purpose to demonstrate compliance with GDPR of processing operations by controllers and processors (GDPR, 2016, Recital 100). GDPR requires the approval of certification criteria of a certification mechanism. As stated before, when drafting certification criteria the following compliance aspects in support of the assessment of the processing operation shall be taken into account, where applicable:

> the lawfulness of processing pursuant to Article 6; the principles of data processing pursuant to Article 5; the data subjects' rights pursuant to Articles 12-23; the obligation to notify data breaches pursuant to Article 33; the obligation of data protection by design and by default, pursuant to Article 25; whether a data protection impact assessment, pursuant to Article 35(7)(d) has been conducted, if applicable; and the technical and organisational measures put in place pursuant to Article 32 (European Data Protection Board, 2019a, p. 15).

Furthermore, certification criteria should:

> be uniform and verifiable; auditable in order to facilitate the evaluation of processing operations under the GDPR, by specifying in particular, the objectives and the implementing guidance for achieving those objectives; be relevant with respect to the targeted audience (e.g. B2B and business to customer (B2C); take into account and where appropriate be inter-operable with other standards (such as ISO standards, national level standards); and be flexible and scalable for application to different types and sizes of organisations including micro, small and medium sized enterprises in accordance with Article 42(1) and the risk-based approach in accordance with Recital 77 (European Data Protection Board, 2019a, p. 20).

When assessing a processing operation, the following components must be considered, where applicable: personal data; technical systems, used to process the personal data; and processes and procedures related to the processing operation(s) (European Data Protection Board, 2019a).

Since the ISO/IEC 29100 family (including ISO/IEC 29100:2011, ISO/IEC 29101:2018 and ISO/IEC 29151:2017) is a framework for the protection of PII within ICT systems, a comparison between the Regulation and the standard seemed, *a priori*, appropriate. Moreover, the documents ISO/IEC 27018:2019 and ISO/IEC 27701:2019 (which would include SaaS), are also appropriate, considering their objectives and scope.

In order to assess if SaaS structures would be GDPR compliant if a combination of the standards ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019 was applied, three steps will be followed: first, a comparison between the legal framework of GDPR and the standards will be made, in order to analyze the similarities and differences; second, it will be assessed if the compliance with the referred standards may be an accurate technical approach regarding SaaS solutions to be compliant with the GDPR; third, it will be assessed if a combination of those standards may be an accurate technical approach regarding SaaS solutions to be compliant with the Portuguese data protection law, that regulates the implementation on the national context of GDPR.

Since the aim of the comparison of the present study is descriptive and the topic of the research is the regulation of a certain societal phenomenon, the *tertium comparationis* will not be form but function of a rule, its social purpose, because there will described the similitudes regarding the regulation of a similar societal phenomenon (Brand, 2007; Oderkerk, 2018; Platsas, 2008).

So, on the present study were selected objects that, *a priori*, have comparable functions, even if with different scopes: GDPR and the standards ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019.

The most common definition of comparative law is the comparison of different legal systems of the world, being the comparative legal analysis defined as the method used by scholars, or other legal experts, in order to conduct such comparison. Generally, this comparison leads to drawing some specific conclusions about the systems compared. Experts also frequently analyze and juxtapose the international or regional system with one or more national systems that have undergone the process of international or regional harmonization of laws (Calboli, 2017). In fact, there is no agreement on the kind of methodology to be followed, nor even on the methodologies that could be followed when embarking on comparative legal research (Van Hoecke, 2015). There are many ways of conducting proper comparative law research, but the method for doing so depends strongly on the purpose for which comparative law research is performed (Hage, 2014) and efforts at developing new approaches potentially useful for legal comparisons may even be inherently valuable (Karhu, 2004).

The comparative method consists in focusing careful attention on the similarities and/or differences among the legal systems being compared (Reitz, 1998)[175]. Nevertheless, scholars are divided on whether comparative legal analysis should focus on the similarities between the legal systems that are compared, or on their differences (Calboli, 2017).

As stated by Eberle, "the key act in comparison is looking at one mass of legal data in relationship to another and then assessing how the two lumps of legal data are similar and how they are different (Eberle, 2009, p. 52).

Scholars frequently disagree on whether comparative legal analysis should primarily—or exclusively—consider the written law or whether comparative scholars should instead also consider the countries' social, cultural, and anthropological environments (Calboli, 2017). Following the legal pluralism approach, on the present study the second option will be followed. In the words of Calboli, "comparative analysis can be conducted at different levels of expertise, and in different ways, and scholars may extend their comparative analysis skills and methods incrementally and with time, as they achieve satisfactory results and become more comfortable with the methodology themselves." (Calboli, 2017, pp. 618–619).

The sources and methods of many of the supra-national systems are evolving and being shaped, becoming the object of comparative enquiries as comparative lawyers provide arguments for or against the acceptance of particular sources or the adoption of particular methodological approaches, and building blocks for a theory of sources and methods that suit their needs (Vogenauer, 2006).

The law must acknowledge its dependence on cooperation with private actors which generate specialised types of dynamic experimental knowledge which is no longer accessible to everybody. Private standards are becoming increasingly important for the law and adopting them requires new procedural rules. Soft law, private standards or "best practices" generated in professional networks become components of a legal practice which undermines the homogeneity of the legal system, and even more so the presupposition of the unity of the will of the legislator (Ladeur, 2004).

Even though a standard cannot be considered a legal system in a stricter sense, the fact is that is a norm, with a context and a proper rationale that can be applied to a system as a rule.

[175] It is not a purpose of this study to focus on the main differences between comparative law as a method and as a body of knowledge. Only the comparative method will be considered.

In performing the basic comparative job of identifying similarities and differences, the scope of comparison has to be defined. It seems necessary, or at least a good approach, for a comparative law study, to devote substantial effort to explore the degree to which there are or are not functional equivalents of the aspect under study in one legal system in the other system or systems under comparison (Reitz, 1998).

One methodological scheme of intelligibility is functionalism (Samuel, 2013; Zweigert, 1972). In fact, the only "method" proposed in comparative literature is the "functional method". It offers one concrete guideline in that it suggests to focus on (common) legal problems and legal solutions in the compared legal systems, rather than on the (diverging) rules and doctrinal frameworks (Van Hoecke, 2015). This approach considers that in law the only things which are comparable are those which fulfil the same function (Samuel, 2013; Zweigert, 1972) and function itself serves to relate different legal systems to each other; institutions, both legal and non-legal, are deemed comparable if they are functionally equivalent (Michaels, 2019), allowing rules and concepts to be appreciated for what they do, rather than for what they say (Brand, 2007). Functionalism addresses the problem that the actual function of legal institutions is a matter of sociological concern: the problems that the law is asked to resolve are similar or even identical across different legal systems. Moreover, this approach also has got as another premise the *praesumptio similitudinis*, which maintains that legal systems tend to resolve practical questions in the same way (Brand, 2007; Platsas, 2008; Van Hoecke, 2015).

According to Zweigert, "it is a basic rule of comparative law that different legal systems find equal or at least astonishing similar solutions (...) for similar problems, in spite of all differences in historical development, systematic and theoretical concepts and style of practice" (Zweigert, 1972).

Taking a functional approach means to analyze not only what rules say but what they solve in their respective legal systems, considering their context, within the procedural and institutional frameworks and socioeconomic and cultural environments. Also, it must be considered law in action, i.e., the application and interpretation of the rules and their true force and effect (Mathias Reimann, 2002). In this sense, Legrand indicates that is not the rule itself that should be the focus of comparison but what the rule signifies in terms of the political, social, economic and ideological context from which it has emerged, since rules are just the surface appearance of law, opposing to the functional approach developed by Zweigert and Kötz (Brand, 2007; Samuel, 2004).

Event though the functionalism is the preferred method of comparatists, it also has some problems that remained to be solved. They can be divided into two categories: (1) axiomatic ones that originate from the three presuppositions that underpin the functional method; and (2) shortcomings in its operation.

Considering the axiomatic problems, they may divided into 3 subcategories: 1) law as a solution of problems; 2) similarity of problems; 3) problems are solved in a similar way.

The first basic assumption of functionalism, that law is a rationally developed entity fulfilling a specific purpose is a weak starting point, since too many factors that in practice obscure the effectiveness of legal rules are not considered. Not always the law can solve problems (i.e., there might be situations where law is enacted for purely symbolical reasons; norms that would usefully address social problems may be absent in a particular system; a legal institution may serve ends or obtain results that were neither foreseen nor desired by its framers; legal institution might have lost its particular function altogether so that its existence can only be explained historically). Moreover, functional studies tend to regard the function of law as a monolithic, independent entity, even though a specific legal institution can have diverse functions (Brand, 2007). Even though law is not the solution for all problems, the fact is that there are no societies without it, at least on a broader sense, as social actors create norms and there is a plurality of collective normative systems in a society and legal norms (in the narrow sense) interact with other normative systems in a society (Moore, 1973).

As for the second premise, the similarity of problems, the method was not designed as a basis for all comparative studies. The implied universalism of this premise confines comparatists to dealing with problems defined in similar practical terms (Brand, 2007; Platsas, 2008). As soon as one system attributes a different social significance to a particular problem, the similarity of function ends. Therefore, functionalists admit that there are areas of the law which are "system conditioned" to an extent so that they are beyond the reach of their method (Brand, 2007).

Besides, it is hard to believe that many legal problems are the same in two societies except on a technical level. The underlying political, moral, and social values in different systems simply vary too much. Functionalists do not seem to realize this because they generally fail to discuss how one establishes "likeness" as a starting point for comparison and they do not propose a method for finding and evaluating differences. As a result, functional approach is unable to solve the problem of apparently similar social and economic conditions producing radically different legal solutions, or even no solutions at all (Brand, 2007). However, once again, although there are different cultures, normative systems don't cease to exist and fundamental rights are shared by nations, as there is the UDHR to prove it.

Regarding the third premise, which states that problems are solved in a similar way, the principle of the *praesumptio similitudinis* is an incentive to concentrate uncritically on similarities and thereby deepen the reductionist tendency of functionalism, being the cultural-historical specificity of legal systems neglected as long as, generally, their solutions to "problems" coincide (Brand, 2007; Platsas, 2008;

Whytock, 2009). This might be taken into consideration under specific circumstances, but with the growing tendency of the multi-level governance and the connection through the digital world, a common basis is being shared, particularly concerning fundamental rights.

As for the operational problems, they may be divided into 2 subcategories: 1) pseudo-factuality; 2) contemporality. The first one, begins by defining a social problem, which is a factual situation plus the value judgment that this situation causes consequences that need to be remedied. The answer to what makes a factual situation a problem may be different between legal systems. Functionalism does not care for this contingency (Brand, 2007). The second is that it is nearly exclusively occupied with studying contemporary legal problems (Brand, 2007).

Nevertheless, as stated before, this method offers practical guidelines, as opposed to others (Van Hoecke, 2015).

Many comparative lawyers consider that a comparative analysis should not start with a particular legal topic, but with a functional question. The recommendation is therefore that a real-life, socioeconomic problem should be the starting point (Siems, 2018).

It is important to clarify that this study will consider the point of view of the actor that designs/develops the SaaS structure and afterwards the point of view of the actor that makes available the SaaS structure to the public. Other perspectives will be left for further studies.

Considering that the GDPR is technologically neutral, it will be assessed if a public SaaS structure would be compliant with GDPR if it follows ISO/IEC standards. It will be assessed if a SaaS structure would be compliant with GDPR (and if so, afterwards with the Portuguese approach) if designed following the ISO/IEC 29100 family of standards[176], namely ISO/IEC 29100:2011[177], ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019, considering the data protection/privacy requirements needed for planning, designing and building ICT system architectures.

It is important to clarify that this study considers the point of view of the actor that designs/develops the SaaS structure and afterwards the point of view of the actor that makes available the SaaS structure to the public. Other perspectives will be left for further studies.

Thus, this dissertation has got several main research questions.

[176] A standard is a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context, being based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits (ISO, n.d.-h)

[177] Amended by the 2018 version.

As for the design/implementation of data protection requirements on ICT systems, namely on SaaS structures:

1. Does the combination of ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019 standards have the same function, considering the design and implementation of data protection requirements to ICT systems, as interpreted by the functional method, as the GDPR regarding data protection?
2. If the first question has got a positive answer, then would a combination of the ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019, standards be an accurate technical approach regarding public SaaS solutions to be compliant with the GDPR?
3. If the second question also has got a positive answer, would a combination of the ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019 standards be an accurate technical approach regarding public SaaS solutions to be compliant with the Portuguese data protection law, that regulates the implementation on the national context of GDPR?

It is important to keep in mind that if the first research question has a negative answer, then the elements that make the standards differ from the GDPR will be analysed, in order to provide further guidance to adjust the standards to the Regulation.

7.2. Comparing and Results

To do comparative law the description of laws has to be followed by the identification of similarities and differences. To do so, categories and concepts can be useful tools to focus the comparison (Siems, 2018). GDPR and the standards will be subject to comparison, in order to understand which requirements and controls are compatible between them, to provide criteria to establish a certification to SaaS structures on the Portuguese context. It will be made a broad analysis and, when needed, referred specifications proper to the Portuguese data protection law and its dispositions.

Elements of GDPR and the standards will be analyzed, namely the objectives, scope, definitions, actors and, in accordance with the certification criteria, the following elements will also be taken into consideration: the lawfulness of processing (which is included in one of the GDPR's principles); the principles of data processing; the data subjects' rights; the obligation to notify data breaches; the obligation of data protection by design and by default; whether a data protection impact assessment has been conducted, if applicable; and the technical and organizational measures.

The analysis will start with the first research question, having as categories of comparison the elements previously referred. If the answer to the research question has a positive answer, then the focus will be on the second research question; otherwise, the second and third research questions will not be considered, and the study will continue, exploring the differences between the standards and the Regulation.

7.2.1. Does the combination of ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019 standards have the same function, considering the design and implementation of data protection requirements to ICT systems, as interpreted by the functional method, as the GDPR regarding data protection?

7.2.1.1.Introduction

Considering that when drafting certification criteria the following compliance aspects in support of the assessment of the processing operation shall be taken into account, where applicable:

> the lawfulness of processing pursuant to Article 6; the principles of data processing pursuant to Article 5; the data subjects' rights pursuant to Articles 12-23; the obligation to notify data breaches pursuant to Article 33; the obligation of data protection by design and by default, pursuant to Article 25; whether a data protection impact assessment, pursuant to Article 35(7)(d) has been conducted, if applicable; and the technical and organisational measures put in place pursuant to Article 32 (European Data Protection Board, 2019a, p. 15),

the main elements of GDPR will be subject to comparison with the core elements of the standards that can have a similar functional relation.

From this study, there will be excluded from scope: requirements and conditions to processing activities related to sensitive data (Articles 9 and 10 from GDPR), transfers of personal data to third countries and binding corporate rules.

7.2.1.2.Objectives

The main objective of GDPR is to ensure: the protection of natural persons about the processing of personal data and rules relating to the free movement of personal data and the protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. Moreover, it is also indicated that the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data (GDPR, 2016).

As for the ISO/IEC 29100 Privacy, it provides a high-level framework for the protection of PII within ICT systems. defining privacy safeguarding requirements while "specifying a common privacy terminology; defining the actors and their roles in processing PII; describing privacy safeguarding requirements; and referencing known privacy principles" (ISO/IEC, 2011, p. vi).

The ISO/IEC 29101:2018:"1) provides a consistent, high-level approach to the implementation of privacy controls for the processing of PII in ICT systems; 2) provides guidance for planning, designing and building ICT system architectures that safeguard the privacy of PII principals by controlling the processing, access and transfer of PII; and 3) shows how PETs can be used as privacy controls" (ISO/IEC, 2018c, p. v)

The ISO/IEC 29134:2017 gives guidelines for a process on privacy impact assessments, and a structure and content of a PIA report (ISO/IEC, 2017b).

The ISO/IEC 29151:2017 has as objective to enable organizations to put in place a set of controls as part of their overall PII protection programme. They can be used in a framework for maintaining and improving compliance with privacy-related laws and regulations, managing privacy risks and meeting the expectations of PII principals, regulators or clients, in accordance with the privacy principles described in ISO/IEC 29100. It is a specification that offers guidance for PII controllers on a broad range of information security and PII protection controls that are commonly applied in many different organizations that deal with protection of PII (ISO/IEC, 2017c).

The ISO/IEC 27701 "specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization" (ISO/IEC, 2019b, Chapter 1).

The ISO/IEC 27018:2019 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect PII in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment, specifying guidelines based on ISO/IEC 27002 and taking into consideration the regulatory requirements for the protection of PII (ISO/IEC, 2019a).

Comparing the main objective from the GDPR with those of the ISO/IEC 29100 family of standards, it is possible to conclude that they have the same function, even if formally described as different. While the GDPR uses the concept of data protection and the ISO/IEC 29100 family uses the concept of privacy, in fact that term used on the standards is functionally equivalent as the one on GDPR, since privacy in this sense, refers to the protection of personally identifiable information of an individual. Nevertheless, they have different scopes and that will be analyzed on the next subchapter.

Moreover, considering the standards ISO/IEC 27701 and ISO/IEC 27018, it is possible to conclude that both aim to enhance the protection of privacy, even if on different domains: the first, under the organizational context; the second, under the cloud computing environment. Therefore, once again, the objectives are aligned, even if the scope and the practical considerations and contexts are not.

7.2.1.3.Scope

As for the scope of GDPR and the standards, the first is limited both on a material and territorial level [178], while the others are only on the material one. the Portuguese Data Protection Law only defines its territorial scope, making no reference to the material one (2019, Article 2). None of the standards defines its territorial scope. It is the organization that has the role to define the scope of application on that matter. In general, GDPR applies only to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (GDPR, 2016).

The ISO/IEC 29100 and ISO/IEC 29101 are applicable all entities involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII (ISO/IEC, 2011, 2018c).

The ISO/IEC 29134:2017 is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations and it is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII (ISO/IEC, 2017b).

The ISO/IEC 29151 is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), in the context of an organization's information security risk environment(s) (ISO/IEC, 2017c).

[178] See GDPR: Portrayal of the New Regulation: Material scope and Territorial scope.

The ISO/IEC 27701 specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing (ISO/IEC, 2019b).

As for the ISO/IEC 27018, it is applicable to all types and sizes of organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations (ISO/IEC, 2019a).

It is possible to conclude that the GDPR has the broadest material scope, being applicable both to controllers and processors. As for the ISO/IEC 29000 family, its scope is mainly the application of privacy to ICT systems, with all the definitions, actors, requirements, controls and guidelines, considering a risk approach. As for the ISO/IEC 27701, it is applicable to all PII controllers and processors.

Two exceptions must be pointed out: ISO/IEC 29151 applies to all types and sizes of organizations acting as PII controllers in the context of an organization's information security risk environment(s) [181]; and ISO/IEC 27018 is applicable to all types and sizes of organizations, which provide information processing services as PII processors via cloud computing (ISO/IEC, 2019a).

However, GDPR has limitation on its territorial application; as for the standards, that criteria should be defined by the organizations that want to implement it.

There are some points of contact between GDPR and the ISO/IEC 29100 family of standards considering their scopes. In order to achieve a maximum correspondence between the common grounds, all three standards should be taken into consideration.

7.2.1.4.Definitions

Considering definitions, the GDPR's will be regarded as the main ones, which will be compared to the terms on standards.

Comparing personal data, as defined on GDPR, and PII, as defined on ISO/IEC 29100, it is possible to conclude that both have the same function, since both refer to a piece of information or data that can directly or indirectly identify a natural person. Nevertheless, it is important to clarify that GDPR does not apply to deceased persons (GDPR, 2016), being this exclusion not indicated on standards. Nevertheless, it is also important to point out that the Portuguese data protection law protects the personal data of deceased people when they are integrated on the special categories of personal as defined on Article 9 of GDPR or they are related to the intimacy of private life, image or data related with communications (2019).

Considering data subject, as defined on GDPR, as opposed to PII principal, as defined on ISO/IEC 29100, both concepts have the same function: to identify the natural person that personal data or PII is related to. Moreover, the data subject/PII principal may be identified or identifiable with that piece of information, considering both the GDPR and the standard.

As for processing (GDPR) and processing of PII (ISO/IEC 29100), they also have the same function, including both an operation or set of operations which are performed on personal data or upon PII. Both definitions provided examples of what those operations may include. The only difference is that on GDPR it is referred that the processing may be operated or not by automated means; on ISO/IEC 29100 there is no such a reference.

The restriction of processing, as defined on GDPR, hasn't a direct match on standards. However, its practical implementation will be needed in order to comply with the GDPR's and standards' principles. Even though is not provided a definition, the control "PII de-identification and deletion at the end of processing." indicated on ISO/IEC 27701, stating that the organization should have mechanisms to eras or de-identify the PII when no further processing is anticipated [181] is related with the GDPR's definition.

Profiling is also another term defined on GDPR. As for the standards, only the ISO/IEC 27701 refers to the term, considering the right of the PII principal to withdraw or modify its consent to that processing activity (ISO/IEC, 2019b).

Considering the term "pseudonymisation", it is also possible to conclude that they both have the same function on GDPR and standards, since they refer a special type of processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. In order to do so, an alias may be used.

As for filing system (GDPR) there isn't a straight match with the ICT systems that store and PII (ISO/IEC 29100). Nevertheless, they both have the same function: to store and process personal data/PII.

Considering controller (GDPR) and PII controller (ISO/IEC 29100), the definitions have the same function: to characterize am entity that alone or jointly with others, determines the purposes and means of the processing of personal data/PII.

As regard to processor (GDPR) and PII processor (ISO/IEC 29100), they have the same function, which is to characterize an entity that processes personal data/PII on behalf of and in accordance with the instructions of a controller/PII controller.

GDPR also defines recipient, as an entity to which the personal data are disclosed, whether a third party or not. This definition is stricter that one that could be related on ISO/IEC 29100, which is privacy stakeholder. A privacy stakeholder is a much broader definition, in the sense that is an entity that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to PII processing. Thus, they do not present the same function, even if they have some point of contact.

A third party (GDPR) has the same designation on standards and both have the same function: to characterize and entity which, under the direct authority of the controller/PII controller or processor/PII processor, is authorized to process personal data.

Considering the consent of the data subject (GDPR) and consent (ISO/IEC 29100), both have the same function: to refer to a freely given, specific, informed indication of the data subject's/PII principal's wishes by which he or she, by a statement or by a clear affirmative action (an agreement).

GDPR also defines a personal data breach, which being formally different from the privacy breach as defined on ISO/IEC 29100 or the data breach referred on ISO/IEC 27018:2017, it has the same function: to describe a situation where the security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Sensitive data or data of a highly personal nature, which includes special categories of personal data as defined in Article 9, as well as personal data as defined in Article 10, and beyond these provisions of the GDPR, since other categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals, being considered as sensitive because they are linked to household and private activities, or because they impact the exercise of a fundamental right or because their violation clearly involves serious impacts in the data subject's daily life (as defined by WP29) has a clear relation with sensitive PII, which is category of PII, either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal, and may include the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that might be defined as sensitive.

Genetic data, biometric data and data concerning health, even if defined on GDPR, they don't have a direct match on the previously indicated standards. However, they are defined on ISO/IEC 19944 and they are on the category of sensitive data.

The other definitions provided on GDPR won't be analyzed, since their practical implementation is out of scope of this study.

7.2.1.5.Actors

Data Subject

GDPR considers a data subject the natural person who can be identified of identifiable by any information (GDPR, 2016). According to ISO/IEC 29100, PII principals, who may also be designated as natural persons or data subjects, provide their PII for processing to PII controllers and PII processors. Also, it is not necessary that the natural person is directly identified by name in order to be considered a PII principal; If the natural person to whom the PII relates can be identified indirectly, he or she is considered to be the PII principal for that PII set. (ISO/IEC, 2011).

Thus, it is possible to conclude that data subjects and PII principals have the same function: they are the actors that can be identified or identifiable by data that is processed by data controllers or processors.

The Controller

As defined on Article 4, (7), controller "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" (GDPR, 2016).

In ISO/IEC 29100, a PII controller determines the purpose and the means of the processing of PII (ISO/IEC, 2018c).

Therefore, it is possible to conclude that the controller and the PII controller have the same function: those are the actors that determine the purposes and means of data processing.

Joint Controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers, which means that they shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject (GDPR, 2016, Article 26). However, in the context of joint control the participation of the parties to the joint determination may take different forms and does not need to be equally shared (Article 29 Data Protection Working Party, 2010).

As for the ISO/IEC, a joint PII controller is PII controller that determine the purposes and means of the processing of PII jointly with one or more other PII controllers (ISO/IEC, 2019b, p. 1).

Functionally, the two concepts are equivalent.

The Processor

According with the Article 4, (8), processor "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (GDPR, 2016). Two basic conditions for qualifying as processor are: 1) being a separate legal entity with respect to the controller; and 2) processing personal data on his behalf. This processing activity may be limited to a very specific task or context or may be more general and extended (Article 29 Data Protection Working Party, 2010).

As for ISO/IEC 29100, a PII processor carries out the processing of PII on behalf of a PII controller, acts on behalf of, or in accordance with the instructions of the PII controller, observes the stipulated privacy requirements and implements the corresponding privacy controls. Furthermore, in some jurisdictions, the PII processor is bound by a legal contract to the PII controller (ISO/IEC, 2011).

Therefore, it is possible to conclude that the processor and the PII processor have the same function: both refer to an independent entity that processes data according to the instructions or on behalf of a controller.

Data Protection Officer

DPOs act as intermediaries between relevant stakeholders and facilitate compliance through the implementation of accountability tools (Article 29 Data Protection Working Party, 2017c).

DPOs are not personally responsible in case of non-compliance with the GDPR: it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions. Therefore, data protection compliance is a responsibility of the controller or the processor (Article 29 Data Protection Working Party, 2017c).

The ISO/IEC equivalent would be the chief privacy officer (CPO), which is a "senior management individual who is accountable for the protection of personally identifiable information (PII) in an organization" (ISO/IEC, 2017c, p. 1). With the introduction of further information by the ISO/IEC 27701, it seems clear that both are functionally equivalent, since there is a responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII. Moreover, the same document indicates that in some jurisdictions such a person is called a data protection officer, defining when such a position is required, along with their position and role (ISO/IEC, 2019b, Chapter 6.3.1.1).

The two actors have the same functions: to ensure that the organization is compliant with GDPR/privacy standards and implement accountability tools to ensure that.

7.2.1.6.Principles

There are 7 main principles relating to processing of personal data that must be followed considering the GDPR's dispositions. As before, those will be the basis of comparison with the principles provided on standards.

Principle of lawfulness, fairness and transparency

The first one is the principle of lawfulness, fairness and transparency, which states that personal data shall be "processed lawfully, fairly and in a transparent manner in relation to the data subject" (GDPR, 2016 Article 5(1)(a)). This principle has got as main function to protect the data subjects from unlawful processing activities and enforce three main areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights (Article 29 Data Protection Working Party, 2018d). It is important to point out that even if GDPR states that in order to processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned, other lawful basis may also be applicable, laid down by law, either in GDPR or in other Union or Member State law[179] (GDPR, 2016), which would include, as far as described on GDPR:

> a) the data subject's consent; b) performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) compliance with a legal obligation to which the controller is subject; d) protection the vital interests of the data subject or of another natural person; e) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or

[179] See Recital 40 of GDPR.

> fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (GDPR, 2016, Article 6(1)).

This principle has a relation with three principles described on ISO/IEC 29100: the principle of consent and choice and specification, the openness, transparency and notice principle and the individual participation and access principle.

The principle of consent and choice aims to protect the PII principal, considering that organizations should provide the means necessary for PII principals to exercise meaningful, informed, unambiguous and freely given consent except where the PII principal cannot freely refuse consent or where applicable law specifically allows the processing of PII without the principal's consent (ISO/IEC, 2017c), since other lawful grounds apply (ISO/IEC, 2019b). Therefore, it indicates that the consent may be a lawful basis and indicates the needed provisions so it can be considered as valid. Moreover, it also indicates that are other lawful ground may be applicable, even if it doesn't provide further information on this point. However, ISO/IEC 27701 clarifies this issue, indicating that some jurisdictions require the organization to be able to demonstrate that the lawfulness of processing was duly established before the processing (ISO/IEC, 2019b). The legal basis for the processing of PII can include: consent from PII principals; performance of a contract; compliance with a legal obligation; protection of the vital interests of PII principals; performance of a task carried out in the public interest; legitimate interests of the PII controller (ISO/IEC, 2019b).

As for the openness, transparency and notice principle, it aims to ensure that PII principals are informed about the PII controller's policies, procedures and practices with respect to the processing of PII (ISO/IEC, 2011).

Finally, regarding the individual participation and access principle, it aims to empower the PII principal, giving PII principals the ability to access, review, verify and demand the accuracy and completeness of their PII and enable PII principals to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost (ISO/IEC, 2011).

Therefore, it is possible to conclude if the three principles of the ISO/IEC 29100 are followed, the principle of lawfulness, fairness and transparency is guaranteed.

Principle of purpose limitation

The principle of purpose limitation states that personal data shall be

> 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 (GDPR, 2016, Article 5(1)(b)).

In particular, "the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data" (GDPR, 2016, Recital 39).

The ISO/IEC 29100 has got an equivalent, named purpose legitimacy and specification principle, which determines that the purpose(s) complies with applicable law and relies on a permissible legal basis and the purpose(s) has to be communicated to the PII principal before the time the information is collected or used for the first time for a new purpose (ISO/IEC, 2011).

Also, in order to restrict the processing activities, the ISO/IEC has got another principle, namely use, retention and disclosure limitation principle, that imposes other conditions: the use, retention and disclosure (including transfer) of PII should be limited to that which is necessary in order to fulfil specific, explicit and legitimate purposes and the use of PII should be limited to the purposes specified by the PII controller prior to collection, unless a different purpose is explicitly required by applicable law (ISO/IEC, 2011).

Then, it is possible to conclude that complying with the two referred principles of ISO/IEC, the principle of purpose limitation as envisioned on GDPR will be protected.

Principle of data minimization

The principle of data minimization indicates that personal data should "be adequate, relevant and limited to what is necessary for the purposes for which they are processed" (GDPR, 2016, Article 5(1)(c)).

The ISO/IEC 29100 has got two principles related with the GDPR's principle of data minimization: the collection limitation principle and the data minimization principle. The first imposes a limitation on the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s); the second is meant to minimize the PII which is processed and the number of privacy stakeholders and people to whom PII is disclosed or who are allowed to process it and to ensure the adoption of a "need-to-know" principle (i.e., one should be allowed to process only the PII which is necessary for the conduct of his/her official duties in the framework of the legitimate purpose of the PII processing (ISO/IEC, 2011, 2018b).

The principle as defined on GDPR seems to have the same function as the other two indicated on ISO/IEC 29100, which is to follow a minimalistic approach on data processing: the data collected and afterwards processed must be reduced at a minimum, that goes along with the purposes for which it was collected.

Principle of accuracy

The principle of accuracy indicates that personal data shall be 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 (GDPR, 2016, Article 5(1)(d); Recital 39).

The ISO/IEC 29100 has one principle related with the one described on GDPR: the accuracy and quality principle. This principle indicates that should be ensured that the PII processed is accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use; ensured the reliability of PII collected from a source other than from the PII principal before it is processed; verified, through appropriate means, the validity and correctness of the claims made by the PII principal prior to making any changes to the PII (in order to ensure that the changes are properly authorized), where it is appropriate to do so; established PII collection procedures to help ensure accuracy and quality; and established control mechanisms to periodically check the accuracy and quality of collected and stored PII (ISO/IEC, 2011).

Thus, where the GDPR's principle states that personal data shall be accurate, the ISO/IEC 29100's principle states exactly the same; as for the kept up to date, they also formally match; and also the two principles clearly indicate that proper measures must be taken in order to rectify or erase (if not needed anymore) inaccurate data.

It is possible to conclude that both principles have the same function, which is to ensure that data is accurate and proper measures to guarantee this are taken.

Principle of storage limitation

The principle of storage limitation indicates that personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" (GDPR, 2016, Article 5(1)(e)). This requires ensuring that the period for which the personal data are stored is limited to a strict minimum and in order to ensure that the personal data are not kept longer than necessary; time limits should be established by the controller for erasure or for a periodic review[180] (GDPR, 2016).

The ISO/IEC 29100 has one related principle, even if it does not formally match: the use, retention and disclosure limitation principle. Part of this principle (the one that concerns storage limitation), indicates

[180] See Recital 39 of GDPR.

that: the retention of PII should be limited to that which is necessary in order to fulfil specific, explicit and legitimate purposes and the PII should be retained only as long as necessary to fulfil the stated purposes, and thereafter securely destroying or anonymizing it; any PII should be locked when and for as long as the stated purposes have expired, but where retention is required by applicable laws (ISO/IEC, 2011).

Analyzing the storage limitation principle, it indicates that personal data shall be kept to a strict minimum and the retention period must be defined in accordance with the purpose for which the data was collected. The main purpose of this principle is to ensure that personal data is not kept indefinitely by the controller, without attending to the purposes for which they were processes in the first place. The same goal is present on the ISO/IEC principle. Furthermore, both principles indicate that after that period, data must be anonymized or destroyed: on GDPR it is implied "personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary"; on the standard it is clearly established. Therefore, it is possible to conclude that both principles have the same function.

Principle of integrity and confidentiality

The principle of integrity and confidentiality states that personal data shall be processed in a manner that ensures appropriate security and confidentiality of the personal data, using appropriate technical or organisational measures[181] (GDPR, 2016).

The ISO/IEC 29100 has got one related principle; the information security principle. The information security principle aims to protect PII with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and protect it against risks such as unauthorized access, destruction, use, modification, disclosure or loss throughout the whole of its life cycle (ISO/IEC, 2011).

Therefore, it is possible to conclude that both are functionally equivalent, since they aim to protect personal data ensuring security and confidentiality, pointing out the need to take measures to do so.

Principle of accountability

Finally, we have the principle of accountability, which indicates that the controller shall be responsible for, and be able to demonstrate compliance with all of the above described principles[182] (GDPR, 2016).

The ISO/IEC 29100 has two principles related with the GDPR's principle of accountability: the accountability principle and the privacy compliance principle. The first aims to enhancing duty of care

[181] See Article 5(1)(f) and Recital 39 of GDPR.

[182] See Article 5(2) of GDPR.

and the adoption of concrete and practical measures for the protection of PII; the second principle requires to verify and demonstrate that the processing meets data protection and privacy safeguarding requirements by periodically conducting audits; adopt appropriate internal controls and independent supervision mechanisms in place that assure compliance with relevant privacy law and with their security, data protection and privacy policies and procedures; and develop and maintain privacy risk assessments (ISO/IEC, 2011).

Thus, even though the ISO/IEC makes a distinction between accountability and privacy compliance, by addressing those two principles, the GDPR's accountability principle is protected.

7.2.1.7.Data subject's rights

As stated before, the GDPR sets out the rights data subjects have regarding their personal data (ITGP Privacy Team, 2017). On the other hand, ISO/IEC presents the other side of the same coin: PII obligations to PII principals that have to be fulfilled by controllers. It makes sense, since while following a standard, only the organization that is being audited can be evaluated; hardly the auditor has access to the PII principal.

Those are the right to transparent information, communication and modalities for the exercise of the rights of the data subject, right to information and access to personal data, right to access, right to rectification, right to erasure, right to restriction of processing, right to data portability, the right to object to specific types of data processing, the right to appropriate decision making and the right to lodge a complaint with a Supervisor Authority against the controller/processor if the data subject considers that the processing of personal data relating to him or her infringes the GDPR.

The first right points out that the controller shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child" (GDPR, 2016 Article 12(1)). This right in particular is protected by the ISO/IEC choice principle, related with the consent, which means that the PII controller needs to provide PII principals with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice and to give consent in relation to the processing of their PII at the time of collection, first use or as soon as practicable thereafter. It is important to clarify that the ISO/IEC 29100 family is focused mainly on consent, even though the ISO/IEC 29151 and ISO/IEC 27701 refer other lawful basis. Also, the ISO/IEC 29100 has another principle that protects this particular data subject right: the openness, transparency and notice principle, which include to provide PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to the processing of PII; include in notices the fact that PII is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the PII might be disclosed, and the identity of the PII controller including information on how to contact the PII controller; and give notice to the PII principals when major changes in the PII handling procedures occur (ISO/IEC, 2011). Therefore, when these two principles of ISO/IEC 29100 are followed, the transparency right is guaranteed.

The data subject also has the right to information and access to personal data, which goes beyond providing the data subject with general information on data processing activities, giving the possibility to the data subject to demand more in-depth information on processing (Voigt & Bussche, 2017). Also, it requires that the data controller proactively informs the data subject about the identity and the contact details of the controller, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing[183] (GDPR, 2016; Voigt & Bussche, 2017). This right is under the scope of the individual participation and access principle, which when complemented with the ISO/IEC 27701 A.7.3.2 control "the organization should determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision." (ISO/IEC, 2019b, Chapter A.7.3.2) offers enough protection.

There is also the right to access: the data subject has the right to obtain confirmation from the controller as to whether or not its personal data is being processed and if such processing takes place, then the data subject shall have access to its personal data processed and the purposes of processing, the categories of personal data concerned, the recipients to whom the data has been or will be disclosed, the storage period or the criteria to determine that period, the existence of the data subject's rights to deletion, rectification, restriction of processing or the right to object, the right to lodge a complaint with the Supervisory Authority[184] (GDPR, 2016; Voigt & Bussche, 2017). Furthermore, the data subject is also given the right to have a copy of the personal data undergoing processing, free of charge (GDPR, 2016, Article 15(3); Voigt & Bussche, 2017). This right is under the scope of the individual participation and access principle, which when complemented with the ISO/IEC 27701 A.7.3.8 control "providing copy of PII processed - the organization should be able to provide a copy of the PII that is processed when requested by the PII principal (ISO/IEC, 2019b, Chapter A.7.3.8)" offers enough guarantees of compliance with GDPR.

[183] See Articles 13 and 14 of GDPR.

[184] See Article 15 and Recital 63 of GDPR.

The right to rectification, which states that the data subject shall have the right to obtain from the controller the rectification of inaccurate personal data concerning him or her and the right to have incomplete personal data completed[185] (GDPR, 2016), is related with the ISO/IEC 29100 principle of accuracy, as described before, that indicates that should be ensured that the PII processed is accurate and complete, among others. Thus, if the principle is being properly followed, the data subject's right is ensured.

The right to erasure which indicates that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay under certain circumstances: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based; the data subject objects to the processing pursuant to profiling or direct marketing purposes; the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; the personal data have been collected based on a child's consent in relation to the offer of information security services[186] (GDPR, 2016). This right is linked with several principles. In order to analyse it properly, each of the circumstances will be individualized. All of them are related with the use, retention and disclosure principle, but they may be combined with other elements: the first one, "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed", is guaranteed if the use, retention and disclosure limitation principle; the second, "; the data subject withdraws consent on which the processing is based", is ensured when the principle of consent and choice is being implemented; the third, "the data subject objects to the processing pursuant to profiling or direct marketing purposes", if the individual participation and access principle is applied and complemented with the ISO/IEC 27701 A.7.3.4 and A.7.3.5 controls; the fourth, "the personal data have been unlawfully processed", with the ISO/IEC 27701 A.7.2.2 (identify lawful basis), the fifth "the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject" with the purpose legitimacy and specification principle; and the seventh, "the personal data have been collected based on a child's consent in relation to the offer of information security services", with the principle of consent and choice.

The right to restriction of processing, is applicable when one of the following circumstances is verified:

[185] See Article 16 of GDPR.

[186] See Article 17 and Recital 65 of GDPR.

> (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 including profiling pending the verification whether the legitimate grounds of the controller override those of the data subject (GDPR, 2016, Article 18).

This right is closely related with the control of ISO/IEC 27701 A.7.3.4, which indicates that there can be restrictions on the processing of PII, which can include restricting the PII controller from deleting the PII in some cases, and the purpose legitimacy and specification principle, as well as individual participation and access principle on ISO/IEC 29100.

The right to data portability, which states that the data subject shall have the right to receive the personal data concerning him or her, whenever personal data that the data subject has provided to a controller are processed based on the data subject's consent or based on their necessity for the performance of a contract between the data subject and the controller and the processing is carried out by automated means (GDPR, 2016; Voigt & Bussche, 2017), is related with the ISO/IEC 27701 A.3.8 control (providing copy of PII processed) as well as the individual participation and access ISO/IEC 29100's principle.

Furthermore, the data subject has the right to object to specific types of data processing, including direct marketing, processing based on legitimate interests or in the wider public interest and processing for research or statistical purposes. This is ensured by the ISO/IEC 27701 A.7.3.5 control, that states that "Some jurisdictions provide PII principals with a right to object to the processing of their PII. Organizations subject to the legislation and/or regulation of such jurisdictions should ensure that they implement appropriate measures to enable PII principals to exercize this right.".

The data subject has the right to appropriate decision making (ITGP Privacy Team, 2017). Therefore, he/she 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" (GDPR, 2016, Article 22). Individuals must be able to trigger intervention, express their point of view, obtain an explanation for a decision and contest the resulting decision (ITGP Privacy Team, 2017). The ISO/IEC 27701 has one specific control related to this right: A.7.3.10 "The organization should identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of

PII. Some jurisdictions define specific obligations to PII principals when a decision based solely on automated processing of PII significantly affects them, such as notifying the existence of automated decision making, allowing for the PII principals to object to such decision making, and/or obtaining human intervention. In some jurisdictions, some processing of PII cannot be fully automated. Organizations operating in these jurisdictions should take compliance with these obligations into account."

Finally, the data subject has several rights, considering remedies, liability and penalties.

The data subject has the right to "lodge a complaint with a Supervisor Authority against the controller/processor if the data subject considers that the processing of personal data relating to him or her infringes this Regulation" (GDPR, 2016, Article 77). Moreover, each natural or legal person "shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them" (GDPR, 2016, Article 78). These rights go along with the provisions on the ISO/IEC 27701, control A.7.3.2, the control A.10.3 from ISO/IEC 29151 "organizations should implement appropriate measures to efficiently handle complaints received from PII principals".

7.2.1.8.Data breaches' notification

As soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons[187] (GDPR, 2016)

The ISO/IEC 27701 indicates that when a breach of PII has occurred, response procedures should include relevant notifications and records. Some jurisdictions define cases when the breach should be notified to the supervisory authority, and when it should be notified to PII principals (ISO/IEC, 2019b). On the other hand, the ISO/IEC 29151 states that when PII is compromised, the rights and interests of the PII principal cannot be protected without immediate measures and jurisdictions may impose specific requirements related to the reporting or notification of security incidents involving PII. Also, when a security incident related to PII occurs, the details of the incident, including the organizations' proposed response, should be notified as soon as possible to relevant authorities, which may include data protection authorities, law enforcement agencies and individuals affected by the incident (ISO/IEC, 2017c).

[187] See Recital 85 and Article 33 of GDPR.

Therefore, it is possible to conclude that if the standards are properly followed, the notification to the supervisor authority (and to the data subject) should be made in accordance with the applicable jurisdiction.

7.2.1.9.Data protection by design and by default

GDPR indicates that 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 processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects – data protection by design[188] (GDPR, 2016).

Also, 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 - data protection by default. 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. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility[189] (GDPR, 2016).

The standard ISO/IEC 27701 devotes a full subchapter to privacy by design and privacy by default, which includes to limit collection and processing of PII, ensure that PII is accurate, complete and up-to-date, define and document data minimization objectives, delete or de-identify PII, the disposal of temporary files, define retention, document policies, procedures and/or mechanisms for the disposal of PII and define PII transmission controls (ISO/IEC, 2019b).

Thus, even if GDPR gives a broader definition of privacy by design and privacy by default, the standard offers a detailed approach to both, having an equivalent function.

7.2.1.10. DPIA vs. PIA

[188] See Article 25 and Recital 78 of GDPR.

[189] See Article 25 and Recital 78 of GDPR.

A DPIA describes the processing of personal data, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data, by assessing them and determining the measures to address them (Article 29 Data Protection Working Party, 2017b). In this sense, there is a similar function between a DPIA and a PIA: the is an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes PII and for taking actions as necessary in order to treat privacy risk (ISO/IEC, 2017b). However, the scope is wider on a DPIA, since the PIA according to the ISO/IEC 29134 is restricted to the ICT domain.

If according to the GDPR the controller is responsible for the carrying-out of a DPIA to evaluate the origin, nature, particularity and severity of a risk, seeking the advice of the DPO (GDPR, 2016), the standard preconizes that responsibility with the person in charge of PII protection or, on his/her absence, with the project manager developing the new technology, service or other initiative that may impact privacy. Nevertheless, the accountability for ensuring the PIA is undertaken and the quality of the result should lie with the top management of the PII controller (ISO/IEC, 2017b).

On both cases, there is the accountability paradigm, being the DPIA and the PIA a tool devoted to assess risks and take measures to ensure compliance and protect data of data subjects'/PII principals, taking into consideration their views, enhancing transparency.

Overall, the content of a DPIA and of a PIA is the same.

Thus, it is possible to conclude that they have the same function.

7.2.1.11. Organizational and technical measures

Under the GDPR; the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk inherent in the processing[190] (GDPR, 2016). The measures shall include, inter alia as appropriate:

> a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 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; d) a process for regularly testing, assessing and evaluating the effectiveness

[190] See Article 32 and Recital 83 of GDPR.

> of technical and organisational measures for ensuring the security of the processing (GDPR, 2016, Article 32).

Under the standards, organization must protect PII with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and protect it against risks such as unauthorized access, destruction, use, modification, disclosure or loss throughout the whole of its life cycle and base these controls on applicable legal requirements, security standards, the results of systematic security risk assessments and the results of a cost/benefit analysis; implement controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that might be affected, and the context in which it is held; subject the controls to periodic review and reassessment in an ongoing security risk management process (ISO/IEC, 2011). Therefore, it is possible to conclude that functionally, the organizational and technical measures are equivalent between the GDPR and the standards: they intend to ensure a level of security adequate to the processing, taking the risk assessment into consideration.

7.2.1.12. Final considerations

Comparing the main objective from the GDPR with those of the ISO/IEC 29100 family of standards, it is possible to conclude that they have the same function, even if formally described as different. While the GDPR uses the concept of data protection and the ISO/IEC 29100 family uses the concept of privacy, in fact that term used on the standards is functionally equivalent as the one on GDPR, since privacy in this sense, refers to the protection of personally identifiable information of an individual. Moreover, considering the standards ISO/IEC 27701 and ISO/IEC 27018, it is possible to conclude that both aim to enhance the protection of privacy, even if on different domains.

It is possible to conclude that the GDPR has the broadest material scope, being applicable both to controllers and processors. As for the ISO/IEC 29000 family, its scope is focused on the application of privacy to ICT systems. As for the ISO/IEC 27701, it is applicable to all PII controllers and processors. The ISO/IEC 29151 applies to all types and sizes of organizations acting as PII controllers in the context of an organization's information security risk environment(s) and ISO/IEC 27018 is applicable to all types and sizes of organizations, which provide information processing services as PII processors via cloud computing.

However, GDPR has limitation on its territorial application; as for the standards, that criteria should be defined by the organizations that want to implement it.

There are points of contact between GDPR and the ISO/IEC 29100 family of standards considering their scopes. In order to achieve a maximum correspondence between the common grounds, all standards should be taken into consideration.

Overall, the main definitions provided on GDPR and standards have the same function and an association between them can be made.

Moreover, considering the actors, it is possible to conclude that data subjects and PII principals have the same function: they are the actors that can be identified or identifiable by data that is processed by data controllers or processors. The controller and the PII controller also have the same function: those are the actors that determine the purposes and means of data processing. As joint controllers and joint PII controllers, they are functionally equivalent. Similarly, the processor and the PII processor have the same function: both refer to an independent entity that processes data according to the instructions or on behalf of a controller. The two figures that may have some differences considering their functions are the DPO and the CPO. Nevertheless, both ensure that the organization is compliant with GDPR/privacy standards and implement accountability tools to ensure that.

While analyzing the GDPR's principles, it is possible to conclude that they are related with the principles described on standards.

The principle of lawfulness, fairness and transparency has a relation with three principles described on ISO/IEC 29100: the principle of consent and choice and specification, the openness, transparency and notice principle and the individual participation and access principle. If those three principles of the ISO/IEC 29100 are followed, the principle of lawfulness, fairness and transparency is guaranteed.

The principle of purpose limitation is related the purpose legitimacy and specification principle, and the use, retention and disclosure limitation principle. If there is compliance with the two referred principles of ISO/IEC, the principle of purpose limitation as envisioned on GDPR will be protected.

The principle of data minimization is related with the collection limitation principle and the data minimization principle from ISO/IEC 29100 family. The principle as defined on GDPR seems to have the same function as the other two indicated on ISO/IEC 29100, which is to follow a minimalistic approach on data processing: the data collected and afterwards processed must be reduced at a minimum, that goes along with the purposes for which it was collected.

The principle of accuracy from GDPR has an equivalent on the accuracy and quality principle from the standards. Both have the same function, which is to ensure that data is accurate and proper measures to guarantee that are taken.

The principle of storage limitation has one related principle, even if not formally equivalent: the use, retention and disclosure limitation principle. The main purpose of both principles is to ensure that personal data is not kept indefinitely by the controller, without attending to the purposes for which they were processes in the first place. Furthermore, they indicate that after that period, data must be anonymized or destroyed: on GDPR it is implied "personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary"; on the standard it is clearly established. Therefore, it is possible to conclude that both principles have the same function.

The principle of integrity and confidentiality has got one related principle; the information security principle. Both are functionally equivalent, since they aim to protect personal data ensuring security and confidentiality, pointing out the need to take measures to do so.

Finally, there is the principle of accountability, which has two related principles from the standards: the accountability principle and the privacy compliance principle. Even though the ISO/IEC makes a distinction between accountability and privacy compliance, by addressing those two principles, the GDPR's accountability principle is protected.

GDPR sets out the rights data subjects have regarding their personal data; the standards, however, indicate several PII obligations to PII principals that have to be fulfilled by controllers.

Considering the GDPR, there are the right to transparent information, communication and modalities for the exercise of the rights of the data subject, right to information and access to personal data, right to access, right to rectification, right to erasure, right to restriction of processing, right to data portability, the right to object to specific types of data processing, the right to appropriate decision making and the right to lodge a complaint with a Supervisor Authority against the controller/processor if the data subject considers that the processing of personal data relating to him or her infringes the GDPR.

The first right from GDPR is protected by the ISO/IEC choice principle, related with the consent. Also, the ISO/IEC 29100 has another principle that protects this particular data subject right: the openness, transparency and notice principle. When these two principles of ISO/IEC 29100 are followed, the transparency right is guaranteed.

The data subject also has the right to information and access to personal data, which is under the scope of the individual participation and access principle, and when complemented with the ISO/IEC 27701 A.7.3.2 control "the organization should determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision." (ISO/IEC, 2019b, Chapter A.7.3.2) offers enough protection.

The right to access is under the scope of the individual participation and access principle, which when complemented with the ISO/IEC 27701 A.7.3.8 control "providing copy of PII processed - the organization should be able to provide a copy of the PII that is processed when requested by the PII principal (ISO/IEC, 2019b, Chapter A.7.3.8)" offers enough guarantees of compliance with GDPR.

The right to rectification is related with the ISO/IEC 29100 principle of accuracy, as described before. Thus, if the principle is being properly followed, the data subject's right is ensured.

The right to erasure is linked with several principles from the standards: the use, retention and disclosure principle, the principle of consent and choice, the individual participation and access principle, the purpose legitimacy and specification principle and the controls from the ISO/IEC 27701 A.7.3.4, A.7.3.5, A.7.2.2.

The right to restriction of processing is closely related with the control of ISO/IEC 27701 A.7.3.4, which indicates that there can be restrictions on the processing of PII and the purpose legitimacy and specification principle, as well as individual participation and access principle on ISO/IEC 29100.

The right to data portability is related with the ISO/IEC 27701 A.3.8 control, as well as the individual participation and access ISO/IEC 29100's principle.

The right to object to specific types of data processing, including direct marketing, processing based on legitimate interests or in the wider public interest and processing for research or statistical purposes, is ensured by the ISO/IEC 27701 A.7.3.5 control.

The right to appropriate decision making is related with one specific control from ISO/IEC 27701: A.7.3.10.

The right to lodge a complaint with a Supervisor Authority against the controller/processor if the data subject considers that the processing of personal data relating to him or her infringes the GDPR and the right to an effective judicial remedy against a legally binding decision of a supervisory authority are protected by the provisions on the ISO/IEC 27701, control A.7.3.2, and the control A.10.3 from ISO/IEC 29151.

Considering the requirements inherent to the notification to the Supervisor Authority of a personal data breach, it is possible to conclude that if the standards are properly followed, the notification to the supervisor authority (and to the data subject) should be made in accordance with the applicable jurisdiction.

GDPR provides guidance on the implementation of the privacy by design and privacy by default principles. In accordance, the standard ISO/IEC 27701 devotes a full subchapter to privacy by design and privacy by default. Even if GDPR gives a broader definition of privacy by design and privacy by default, the standard offers a detailed approach to both, having an equivalent function.

A DPIA and a PIA have an equivalent function of describing the processing data, assessing the inherent risks, include treatment measures, enhancing the transparency and being a tool to promote accountability.

Finally, considering organizational and technical measures, under the GDPR; both the controller and the processor shall them, in order to to ensure a level of security appropriate to the risk inherent in the processing, and they include: a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 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; d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. Under the standards, organization must protect PII with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and protect it against risks throughout the whole of its life; implement controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that might be affected, and the context in which it is held; subject the controls to periodic review and reassessment in an ongoing security risk management process. Therefore, it is possible to conclude that functionally, the organizational and technical measures are equivalent between the GDPR and the standards: they intend to ensure a level of security adequate to the processing, taking the risk assessment into consideration.

Taking into consideration all of the above, it is possible to conclude that the combination of ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019 standards has the same function, considering the design and implementation of data protection requirements to ICT systems, as interpreted by the functional method, as the GDPR, regarding data protection.

Therefore, this study will continue to the second research question.

7.2.2. Would a combination of the ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019, standards be an accurate technical approach regarding public SaaS solutions to be compliant with the GDPR?

To properly answer to the second research question, the first needed to have a positive answer, which it did. Even though the standards do not follow the same terminology as the GDPR, they are functionally equivalent.

Taking that into consideration, and following the conditions described on Chapter 6, it is possible to conclude that that specific combination is an actual consistent and accurate technical approach regarding public SaaS solutions to be compliant with the GDPR.

Analyzing the phases of the PII processing life-cycle, considering the data protection requirements as they were described (never forgetting that each organization has to evaluate, adapt and define its own requirements), as well as the privacy/data protection controls (that followed all the GDPR's conditions and, once again, they may be adjusted to the organization's context) and the privacy architecture framework, it can be stated that this approach is consistent and provides a structure that organizations that develop and offer SaaS solutions should follow.

Therefore, this is a possible solution to be compliant with the GDPR without further guidance, useful to draw-up a Code of Conduct to SaaS processors or, as stated before, it could be useful when drafting certification criteria by certification, by the competent supervisory authority or by the Board, since it considers the all the compliance aspects stipulated by the EDPB.

Furthermore, these criteria are uniform and verifiable, auditable, relevant with respect to the targeted audience (in this particular case, the processors that develop and offer SaaS solutions), take into account and are be inter-operable with other standards (such as ISO standards and national level standards[191]); and is flexible and scalable for application to different types and sizes of organisations including micro, small and medium sized enterprises in accordance with Article 42(1) and the risk-based approach in accordance with Recital 77.

7.2.3. Would a combination of the ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019 standards be an accurate technical approach regarding public SaaS solutions to be compliant with the Portuguese data protection law, that regulates the implementation on the national context of GDPR?

Finally, and considering the first and second positive research answers, it is possible to conclude that the model developed, taking into consideration the standards, as well as the GDPR and the Portuguese data

[191] The Resolution of the Council of Ministers acts as legislation to public authorities but also as guidance to the enterprise sector of the Portuguese State.

protection requirements, is an accurate technical approach regarding public SaaS solutions. Actually, a specific Portuguese legal document (Resolution of the Council of Ministers 41/2018) provided further requirements[192], but also further guidance on how to technically implement some controls that are important to enhance data protection. Those considerations are included on the subchapter 6.3 and are part of the developed model on this study.

However, as previously stated by CNPD, careful consideration must be taken while analysing the Portuguese context: the Portuguese Data Protection Law, regarding its territorial scope, is incompatible with GDPR (CNPD, 2019). Nevertheless, the CNPD has got competence (and therefore the Portuguese Data Protection Law hasn't limitations considering the incompatibility of supervisor authorities) where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), since in such cases Article 56 does not apply (GDPR, 2016, Article 55).

Thus, this is a possible solution to be compliant with the GDPR and the Portuguese context, without further guidance, useful to draw-up a Code of Conduct to SaaS processors or, it could be useful when drafting certification criteria by certification bodies referred to in Article 43 or by the CNPD.

[192] As stated before, the Resolution of the Council of Ministers acts as legislation to public authorities but also as guidance to the enterprise sector of the Portuguese State.

8. CONCLUSION

Globalization and global governance have become central themes and more legislating actors appear (Günther, 2008; Wessel & Wouters, 2008).

With the development of the international legal order, the creation of legal norms outside the national legal systems has grown. This is particularly evident for EU Member States, since European Law is increasingly affecting their citizens and businesses (Wouters et al., 2008). The strict dividing lines between European and national law became blurred and precarious and domestic legal systems are increasingly influenced of international regulation (Bache, 2005; Wessel & Wouters, 2008; Wouters et al., 2008).

With the multi-level governance, European integration has diminished the prerogatives of the state (Hooghe & Marks, 2003; Trnski, 2005). There is a top down impact of the EU on its member states, with European decisions' impacting member states' politics and policies EU (Bache, 2005; Trnski, 2005).

In Portugal, there is a weak multilevel governance, despite incremental shifts toward greater subnational and nonstate participation and the creation of new regional structures. However, there still is a high level of institutional centralization (Bache, 2008, 2009; Chrabąszcz & Zawicki, 2016).

If privacy has largely been a matter of law and policy, security has largely been a matter of technology and policy (IAPP-OneTrust, 2018), even if it was protected as a fundamental right as the other one, considering the UDHR (United Nations, 1948), CFREU (Charter of Fundamental Rights of the European Union, 2012), and considering the Portuguese context, the CPR (Constitution of the Portuguese Republic, 2005).

The privacy and data protection rights are closely related, even if there is a growing tendency to individualize them. From the Hague Peace Conference of 1899, the Convention 108, to the UDHR the protection of those rights has been enhanced. Within the European context, the CFREU and afterwards the Directive 95/46/EC were necessary but insufficient steps to ensure data protection. The entry into force of the Lisbon Treaty in December 2009 had an enormous impact on the development of EU data protection law, closing the loopholes regarding data protection in the EU. Finally, the GDPR came into force, in order to reduce legal fragmentation, provide greater legal certainty, improve the protection of individuals, and contribute to the free flow of personal data within the Union (European Commission, 2012a; Poullet, 2018; Reding, 2012).

The Portuguese legislator wasn't ready to adjust the internal law to the GDPR's requirements, which is can be proved by the deliberation made by CNPD, but, on the other hand, provided useful guidance on technical requirements.

Since legislation tends to be technologically neutral (and it aims to), further guidance needs to be provided to the ones that develop and implement technology, in order to be compliant with the, sometimes, blurred requirements of data protection law.

Cloud computing can be considered a new paradigm in computing that is rapidly changing the landscape of information technology and consequently, various business models have evolved to integrate this technology into software applications, programming platforms, data storage, computing infrastructures and hardware as a service (Armbrust et al., 2010; Dukaric & Juric, 2013; Jansen & Grance, 2011; Shawish & Salama, 2014; Talia, 2011; WeDo Technologies, 2011; Youseff et al., 2008).

Considering its characteristics, and more precisely the SaaS service, this dissertation aimed to explore if the already designed standards by ISO/IEC (namely ISO/IEC 29100:2011, ISO/IEC 29101:2018, ISO/IEC 29134:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2019 and ISO/IEC 27701:2019) could be functionally equivalent to GDPR and if they were able to ensure a technical and accurate solution to be compliant with the Regulation (and if possible, with the dispositions that affect the Portuguese context), from the SaaS provider processor's perspective. It is important to point out that some elements were considered out of scope, namely: requirements and conditions to processing activities related to sensitive data (Articles 9 and 10 from GDPR), transfers of personal data to third countries and binding corporate rules.

The solution described mainly on chapter 6 offers a structure that organizations should follow in order to be compliant with the GDPR without further guidance. Moreover, it is also useful to draw-up a Code of Conduct to SaaS processors or it could be used when drafting certification criteria by certification bodies, by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority.

This dissertation is focused on the SaaS provider perspective, more precisely when it acts as a processor. Further studies should focus on the perspective of the CSC, as well as the data subject, and also take into consideration the elements that were considered out of scope from this study.

Moreover, it is important to keep in mind that the structure that was considered to develop and implement a GDPR compliant SaaS solution is designed on an abstract level. All organizations must consider their own specific characteristics, nature, scope and context to select and apply the chosen controls. For instance, the ISO/IEC 27002 has more controls than the ones that were selected for this study purposes, but can be useful to some organizations.

Finally, other standards may be considered on future studies (such as NIST) and the already created codes of conduct finally approved and taken into account.

LEGISLATION

Assembleia da República. *Lei n.◦ 67/98, de 26 de outubro*. (1998).

Assembleia da República. *Lei n.◦ 46/2018, de 13 de agosto* (2018).

Assembleia da República. *Lei n.◦ 58/2019, de 8 de agosto*. (2019).

Charter of Fundamental Rights of the European Union. (2012).

CNPD. Regulamento n.◦ 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados. , Diário da República § (2018).

CNPD. *Deliberação/2019/494*. (2019).

Conselho da Europa. *Convenção Europeia dos Direitos do Homem*. (1950).

Conselho de Ministros. *Resolução do Conselho de Ministros n.◦ 41/2018*. (2018).

Constitution of the Portuguese Republic. (2005).

Council of Europe. Convention for the protection of Individuals with regard to Automatic Processing of Personal Data. , European Treaty Series § (1981).

Council of Europe. (2018). Chart of signatures and ratifications of Treaty 005: Convention for the Protection of Human Rights and Fundamental Freedoms. Retrieved June 9, 2018, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures

Decreto-Lei n.º 7/2004, de 7 de janeiro. (2004).

Decreto-Lei n.◦ 48/95, de 15 de março. (1995).

Decreto-Lei n.º 220/95, de 31 de agosto. (1995)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995).

European Convention on Human Rights. (1950).

European Court of Human Rights. *Case of K.U. v. Finland*. (2004).

European Court of Human Rights. *Case of Von Hannover v. Germany*. (2004).

ECJ. *Digital Rights Ireland Ltd (C-293/12) and Kärntner Landesregierung (C-594/12)*. (2014).

ECJ. *Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. (2014).

EJC. *Lindqvist (Case C-101/01)*. (2003).

EJC. *Maximillian Schrems v Data Protection Commissioner*. (2015).

European Parliament and the Council of the European Union. Directive (EU) 2016/1148 of the European

Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. , Official Journal of the European Union § (2016).

European Parliament and the Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) § (2016).

Ministério dos Negócios Estrangeiros. *Aviso de 02/01/1979*. (1979).

Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community. (2007).

United Nations. *Universal Declaration of Human Rights*. (1948).

BIBLIOGRAPHY

Ahmed, M., & Hossain, M. A. (2014). Cloud Computing and Security Issues in the Cloud. *International Journal of Network Security & Its Applications (IJNSA)*, *6*(1), 25–36.

Al-Anzi, F. S., Yadav, S. K., & Soni, J. (2014). Cloud computing: Security model comprising governance, risk management and compliance. *2014 International Conference on Data Mining and Intelligent Computing, ICDMIC 2014*, 1–6. https://doi.org/10.1109/ICDMIC.2014.6954232

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Zaharia, M. (2009). Above the clouds: A Berkeley view of cloud computing. *University of California, Berkeley, Tech. Rep. UCB*, 7–13. https://doi.org/10.1145/1721654.1721672

Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., … Rabkin, A. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4). https://doi.org/10.1145/1721654.1721672

Article 29 Data Protection Working Party. (2009). *The Future of Privacy*. Retrieved from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

Article 29 Data Protection Working Party. (2010). *Opinion 1/2010 on the concepts of "controller" and "processor."* Retrieved from http://ec.europa.eu/justice/data-protection/index_en.htm

Article 29 Data Protection Working Party. (2012). *Opinion 05/2012 on Cloud Computing*. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Article 29 Data Protection Working Party. (2013). *Opinion 03/2013 on purpose limitation*. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Data Protection Working Party. (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. Retrieved from https://ec.europa.eu/newsroom/article29/news.cfm?item%7B_%7Dtype=1360

Article 29 Data Protection Working Party. (2017a). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. Retrieved from https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

Article 29 Data Protection Working Party. (2017b). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of*

Regulation 2016/679 (rev. 01). Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Article 29 Data Protection Working Party. (2017c). *Guidelines on Data Protection Officers ('DPOs')*. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

Article 29 Data Protection Working Party. (2017d). *Guidelines on the right to data portability* (rev. 01). Retrieved from http://ec.europa.eu/justice/data-protection/index_en.htm

Article 29 Data Protection Working Party. (2018a). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 - Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018*. https://doi.org/10.2139/ssrn.2972855

Article 29 Data Protection Working Party. (2018b). *Guidelines on Consent under Regulation 2016/679* (rev. 01). https://doi.org/10.2139/ssrn.2972855

Article 29 Data Protection Working Party. (2018c). *Guidelines on Personal data breach notification under Regulation 2016/679* (rev. 01). Retrieved from https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827

Article 29 Data Protection Working Party. (2018d). *Guidelines on transparency under Regulation 2016/679* (rev. 01). Retrieved from https://ec.europa.eu/newsroom/article29/news.cfm?item%7B_%7Dtype=1360

Article 29 Data Protection Working Party. (2018e). *Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*. Retrieved from http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045

Assembleia da República. *Lei n.º 67/98, de 26 de outubro*. , (1998).

Assembleia da República. *Lei n.º 46/2018, de 13 de agosto*. , (2018).

Assembleia da República. *Lei n.º 58/2019, de 8 de agosto*. , (2019).

Bache, I. (2005). Europeanization and Britain: Towards multi-level governance? *EUSA 9th Biennial Conference*. Retrieved from http://aei.pitt.edu/3158/2/Bache.doc

Bache, I. (2008). *Europeanization and Multilevel Governance: Cohesion Policy in the European Union and Britain*. Rowman & Littlefield.

Bache, I. (2009). *Europeanization and multi-level governance: Empirical findings and conceptual challenges*. Retrieved from https://www.researchgate.net/profile/Ian_Bache/publication/5014743_Europeanization_and_multi-level_governance_Empirical_findings_and_conceptual_challenges/links/02e7e53ac73d1ad5290

00000/Europeanization-and-multi-level-governance-Empirical-findings-and-con

Bartolini, C., Santos, C., & Ullrich, C. (2018). Property and the cloud. *Computer Law and Security Review*, *34*(2), 358–390. https://doi.org/10.1016/j.clsr.2017.10.005

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144. https://doi.org/10.1111/ips.12048

Berman, P. S. (2007). Global legal pluralism. *Southern California Law Review*, *80*(6), 1155–1238.

Blokdijk, G., & Menken, I. (2009). *Cloud Computing - The Complete Cornerstone Guide to Cloud Computing Best Practices*. The Art of Service.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. *International Journal of Law and Information Technology*, *19*(3), 187–223. https://doi.org/10.1093/ijlit/ear005

Brand, O. (2007). Conceptual comparisons: Towards a coherent methodology of comparative legal studies. *Brooklyn Journal of International Law*, *32*(2), 405–466. Retrieved from http://brooklynworks.brooklaw.edu/bjilhttp://brooklynworks.brooklaw.edu/bjil/vol32/iss2/3

Calboli, I. (2017). A call for strengthening the role of Comparative Legal Analysis in the United States. *Saint Johns Law Review*, *90*(3), 609–638. https://doi.org/10.1097/ANS.0000000000000109

Casagran, C. B. (2016). The reinforcement of fundamental rights in the Lisbon Treaty. In S. Dosenrode (Ed.), *The European Union after Lisbon: Polity, Politics, Policy*. New York: Routledge.

Casalicchio, E., & Palmirani, M. (2015). A cloud service broker with legal-rule compliance checking and quality assurance capabilities. *Procedia Computer Science*, *68*, 136–150. https://doi.org/10.1016/j.procs.2015.09.230

Castro, C. S. e. (2005). *Direito da Informática, Privacidade e Dados Pessoais*. Coimbra: Almedina.

Castro, C. S. e. (2016). 40 anos de “Utilização da Informática”: O artigo 35.º da Constituição da República Portuguesa. *E-Pública: Revista Eletrónica de Direito Público*, *3*(3), 84–99.

Charter of Fundamental Rights of the European Union. , (2012).

Chrabąszcz, R., & Zawicki, M. (2016). The evolution of multi-level governance: The perspective on EU anti-crisis policy in Southern-European Eurozone states. *Zarządzanie Publiczne*, *4*(38), 17–31. https://doi.org/10.15678/ZP.2016.38.4.02

Cloud Security Alliance. *Cloud Security Alliance Code of Conduct for GDPR Compliance*. , (2018).

CNPD. Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados. , Diário da República § (2018).

CNPD. *Deliberação/2019/494*. , (2019).

Commission of the European Communities. (1990). COM(90) 314 final - SYN 287 and 288. Retrieved August 27, 2018, from http://aei.pitt.edu/3768/1/3768.pdf

Conselho da Europa. *Convenção Europeia dos Direitos do Homem*. , (1950).

Conselho de Ministros. *Resolução do Conselho de Ministros n.º 41/2018*. , (2018).

Constitution of the Portuguese Republic. , (2005).

Council of Europe. Convention for the protection of Individuals with regard to Automatic Processing of Personal Data. , European Treaty Series § (1981).

Council of Europe. (1981b). Explanatory Report of Convention for the protection of individuals with regard to automatic processing of personal data. In *European Treaty Series*. Retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Council of Europe. (2018). Chart of signatures and ratifications of Treaty 005: Convention for the Protection of Human Rights and Fundamental Freedoms. Retrieved June 9, 2018, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures

Crompton, S., & Jensen, J. (2019). Towards a secure and GDPR-compliant fog-to-cloud platform. *Proceedings - 11th IEEE/ACM International Conference on Utility and Cloud Computing Companion, UCC Companion 2018*, 296–301. https://doi.org/10.1109/UCC-Companion.2018.00071

Decreto-Lei n.º 48/95, de 15 de Março. , (1995).

Di Martino, B., Cretella, G., & Esposito, A. (2015). Towards a legislation-aware cloud computing framework. *Procedia Computer Science*, *68*, 127–135. https://doi.org/10.1016/j.procs.2015.09.229

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. , (1995).

DLA Piper UK LLP. (2015). *Comparative Study on cloud computing contracts*.

Dobinson, I., & John, F. (2017). Legal research as qualitative research. In M. McConville (Ed.), *Research Methods for Law*. Edinburgh: Edinburgh University Press.

Dukaric, R., & Juric, M. B. (2013). Towards a unified taxonomy and architecture of cloud frameworks. *Future Generation Computer Systems*, *29*(5), 1196–1210. https://doi.org/10.1016/j.future.2012.09.006

Duncan, B., & Zhao, Y. (2018). Risk management for cloud compliance with the EU general data protection regulation. *Proceedings - 2018 International Conference on High Performance*

Computing and Simulation, HPCS 2018, 664–671. https://doi.org/10.1109/HPCS.2018.00109

Eberle, E. J. (2009). The method and role of Comparative Law. *Washington University Global Studies Law Review*, *8*(3).

ECJ. *Digital Rights Ireland Ltd (C-293/12) and Kärntner Landesregierung (C-594/12).* , (2014).

ECJ. *Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.* , (2014).

EJC. *Lindqvist (Case C-101/01).* , (2003).

EJC. *Maximillian Schrems v Data Protection Commissioner.* , (2015).

ENISA. (2017a). *Handbook on Security of Personal Data Processing*. https://doi.org/10.2824/569768

ENISA. (2017b). *Security aspects of virtualization*. https://doi.org/10.2824/955316

ENISA. (2018a). *Recommendations on shaping technology according to GDPR provisions: An overview on data pseudonymisation*. https://doi.org/10.2824/74954

ENISA. (2018b). *Recommendations on shaping technology according to GDPR provisions: Exploring the notion of data protection by default*. https://doi.org/10.2824/518496

ENISA. (2018c). *Reinforcing trust and security in the area of electronic communications and online services: Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing*. https://doi.org/10.2824/015812

ENISA Ad Hoc Working Group on Privacy & Technology. (2008). *Technology-induced challenges in Privacy & Data Protection in Europe*.

EU Cloud CoC. (2019). *EU Data Protection Code of Conduct for Cloud Service Providers*. Retrieved from https://eucoc.cloud/fileadmin/cloud-coc/files/former-versions/European_Cloud_Code_of_Conduct_1-7.pdf

EUGDPR.org. (n.d.). GDPR Key Changes: An overview of the main changes under GDPR and how they differ from the previous directive. Retrieved August 30, 2018, from https://www.eugdpr.org/key-changes.html

European Commission. (2001). *Enhancing Democracy: A White Paper on Governance in the European Union*. Retrieved from https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_1_white_papers/com2001_white_paper_european_governance.pdf

European Commission. (2010). *Communication from the Commission to the European Parliament, the Council, the Economic and social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union*.

European Commission. (2012a). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding privacy in a connected world: A European Data Protection Framework for the 21st Century*. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF

European Commission. (2012b). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012DC0529

European Commission. (2018). *Communication from the Commission to the European Parliament and the Council: Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018*. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf

European Commission. (2019). *The European Commission Cloud Strategy: Cloud as an enabler for the European Commission Digital Strategy* (1.0.1). https://doi.org/10.4324/9780429496189

European Convention on Human Rights. , (1950).

European Court of Human Rights. *Case of K.U. v. Finland*. , (2004).

European Court of Human Rights. *Case of Von Hannover v. Germany*. , (2004).

European Data Protection Board. (2018a). *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*. Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

European Data Protection Board. (2018b). *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)-Version for public consultation*. (November), 23. Retrieved from https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf

European Data Protection Board. (2018c). *Opinion 18/2018 on the draft list of the competent supervisory authority of Portugal regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*. Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/valdybos-nuomone-64-str/opinion-182018-draft-list-competent-supervisory_pt

European Data Protection Board. (2019a). *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679* (3rd ed.). Retrieved from https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-12018-certification-and-identifying_pt

European Data Protection Board. (2019b). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*. Retrieved from https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf

European Parliament and the Council of the European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. , Official Journal of the European Union § (2016).

Expert Group Report. (2010). *The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010*. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1168

Fundación Tecnalia Research & Innovation. (2018). *Certification Schemes for Cloud Computing*. https://doi.org/10.2759/64404

GDPR. , (2016).

Gray, A. (2013). Conflict of laws and the cloud. *Computer Law and Security Review*, *29*(1), 58–65. https://doi.org/10.1016/j.clsr.2012.11.004

Griffiths, J. (1986). What is legal pluralism. *Journal of Legal Pluralism and Unofficial Law*, *24*(1).

Grossman, R. L. (2008). A quick introduction to clouds. *Relation*, *10*(1.101), 9822.

Grossman, R. L. (2009). The case for cloud computing. *IT Professional*, *11*(2), 23–27.

Günther, K. (2008). Legal pluralism or uniform concept of law?: Globalisation as a problem of legal theory. *No Foundations: Journal of Extreme Legal Positivism*, (5), 5–21.

Hage, J. (2014). Comparative law as Method and the Method of Comparative Law. *Maastricht European Private Law Institute Working Paper, (2014/11)*. https://doi.org/10.2139/ssrn.2441090

Hannum, H. (1995). The status of the Universal Declaration of Human Rights in national and international law. *GA. J. INT'L & COMP. L.*, *25*(287). Retrieved from http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1396&context=gjicl

Harris, D. J., O'Boyle, M., Bates, E., & Buckley, C. (2014). *Law of the European Convention on Human Rights* (3rd ed.). Oxford: Oxford University Press.

Höfer, C. N., & Karagiannis, G. (2010). Taxonomy of cloud computing services. *2010 IEEE Globecom Workshops*, 1345–1350. https://doi.org/10.1109/GLOCOMW.2010.5700157

Höfer, C. N., & Karagiannis, G. (2011). Cloud computing services: Taxonomy and comparison. *Journal of Internet Services and Applications*, *2*, 81–94. https://doi.org/10.1007/s13174-011-0027-x

Hon, W. K., & Millard, C. (2018). Banking in the cloud: Part 3 – contractual issues. *Computer Law and Security Review*, *34*(3), 595–614. https://doi.org/10.1016/j.clsr.2017.11.007

Hon, W. K., Millard, C., & Walden, I. (2012). Who is responsible for "personal data" in cloud computing? — The cloud of unknowing, Part 2. *International Data Privacy Law*, *2*(1), 3–18. https://doi.org/10.1093/idpl/ipr018

Hooghe, L., & Marks, G. (2003). Multi-level governance Unraveling the Central State, But How? Types of Multi-Level Governance. *American Political Science Review*, *97*(2), 233–243.

Hooghe, L., Marks, G., & Marks, G. W. (2003). Unraveling the central state, but how? Types of multi-level governance. *American Political Science Review*, *97*(2), 233–243.

Hustinx, P. (2014). EU data protection law: The review of directive 95/46/EC and the proposed general data protection regulation. Retrieved August 27, 2018, from https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf

IAPP-OneTrust. (2018). *IAPP-OneTrust Research: Bridging ISO 27001 to GDPR*. Retrieved from https://iapp.org/media/pdf/resource_center/IAPP-OneTrust-Bridging-ISO-GDPR-final.pdf

Information Commissioner of Slovenia. (2012). *Personal data protection and cloud computing*. Retrieved from https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf

ISO/IEC. (2011). *ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework* (1st ed.). 1st ed.

ISO/IEC. (2013a). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements* (2nd ed., p. 38). 2nd ed., p. 38.

ISO/IEC. (2013b). *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls* (2nd ed., p. 90). 2nd ed., p. 90. Retrieved from www.iso.org

ISO/IEC. (2014a). *ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary* (1st ed.). 1st ed.

ISO/IEC. (2014b). *ISO/IEC 17789:2014 Information technology — Cloud computing — Reference* *architecture* (1st ed.). 1st ed.

ISO/IEC. (2015). *Using and referencing ISO and IEC standards to support public policy*. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/pub100358.pdf%0Ahttp://www.iec.ch/about/%0Ahttp://www.iec.ch/about/?ref=menu

ISO/IEC. (2017a). *ISO/IEC 19941:2017 Information technology — Security* (1st ed.). 1st ed. https://doi.org/ISO/IEC 11889-1:2009(E)

ISO/IEC. (2017b). *ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment* (1st ed.). 1st ed.

ISO/IEC. (2017c). *ISO/IEC 29151:2017 Information technology — Security techniques — Code of practice for personally identifiable information* (1st ed.). 1st ed.

ISO/IEC. (2018a). *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary* (5th ed., p. 38). 5th ed., p. 38. Retrieved from http://k504.khai.edu/attachments/article/819/ISO_27000_2014.pdf

ISO/IEC. (2018b). *ISO/IEC 29100:2018 Information technology — Security techniques — Privacy framework* (Amendment). Amendment. Retrieved from https://www.iso.org/obp/ui/#!iso:std:44378:en

ISO/IEC. (2018c). *ISO/IEC 29101:2018 Information technology — Security techniques — Privacy architecture framework* (2nd ed.). 2nd ed. Retrieved from https://www.iso.org/obp/ui/#!iso:std:44378:en

ISO/IEC. (2018d). ISO/IEC Directives, Part 2: Principles and rules for the structure and drafting of ISO and IEC documents. Retrieved August 25, 2019, from https://www.iso.org/sites/directives/current/part2/index.xhtml

ISO/IEC. (2019a). *ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* (2nd ed.). 2nd ed. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-2:v1:en

ISO/IEC. (2019b). *ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines* (1st ed.). 1st ed.

ISO/IEC JTC 1/SC 27/WG 5, & Information. (2017). *Text for SC 27/WG 5 Standing Document 2 (WG 5 SD2) – Privacy references list*.

ISO/IEC JTC 1/SC 27. (2018). *SC 27 Standing Document 6 (SD6): Glossary of IT Security Terminology*.

Retrieved from https://www.din.de/en/meta/jtc1sc27/downloads

ISO. (n.d.-a). ABOUT US. Retrieved August 28, 2019, from https://www.iso.org/about-us.html

ISO. (n.d.-b). BENEFITS OF STANDARDS. Retrieved August 25, 2019, from https://www.iso.org/benefits-of-standards.html

ISO. (n.d.-c). CASCO: Conformity Assessment tools to support public policy: Welcome. Retrieved August 25, 2019, from https://www.iso.org/sites/cascoregulators/index.html

ISO. (n.d.-d). CASCO: Conformity Assessment tools to support public policy: What is Conformity Assessment? Retrieved August 25, 2019, from https://www.iso.org/sites/cascoregulators/01_0_conformity-assessment-basic-concepts.html

ISO. (n.d.-e). IPQ: PORTUGAL. Retrieved August 26, 2019, from https://www.iso.org/member/2054.html

ISO. (n.d.-f). ISO AND POLICY MAKERS. Retrieved August 25, 2019, from https://www.iso.org/iso-and-policy-makers.html

ISO. (n.d.-g). National Examples. Retrieved August 25, 2019, from https://www.iso.org/sites/policy/national_examples.html

ISO. (n.d.-h). Resources: Definitions. Retrieved August 25, 2019, from https://www.iso.org/sites/policy/resources.html

ITGP Privacy Team. (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. Ely: IT Governance Ltd.

Jaatun, M. G., Pearson, S., Gittler, F., Leenes, R., & Niezen, M. (2016). Enhancing accountability in the cloud. *International Journal of Information Management*. https://doi.org/10.1016/j.ijinfomgt.2016.03.004

Jadeja, Y., & Modi, K. (2012). Cloud computing - concepts, architecture and challenges. *International Conference on Computing, Electronics and Electrical Technologies*. https://doi.org/10.1109/ICCEET.2012.6203873

Jansen, W. (2011). Cloud hooks: Security and privacy issues in cloud computing. *Proceedings of the 44th Hawaii International Conference on System Sciences*, 1–10.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. In *NIST Special Publication 800-144 Guidelines*.

Jula, A., Sundararajan, E., & Othman, Z. (2014). Cloud computing service composition: A systematic literature review. *Expert Systems with Applications*, *41*(8), 3809–3824. https://doi.org/10.1016/j.eswa.2013.12.017

Karhu, J. (2004). How to make comparable things: Legal engineering at the service of Comparative Law. In M. Van Hoecke (Ed.), *Epistemology and Methodology of Comparative Law*. Hart Publishing.

Kemp, R. (2018). Legal aspects of cloud security. *Computer Law and Security Review*, *34*(4), 928–932. https://doi.org/10.1016/j.clsr.2018.06.001

Knorr, E., & Gruman, G. (2010). What cloud computing really means. *Courts Today*, *8*(4), 34–36. Retrieved from http://search.proquest.com.library.capella.edu/docview/755055015/fulltextPDF?accountid=27965

Koops, B. (2014). On legal boundaries, technologies, and collapsing dimensions of privacy. *Politica e Società*, *3*(2), 247–264.

Kshetri, N. (2012). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 1–15. https://doi.org/http://dx.doi.org/10.1016/j.telpol.2012.04.011

Kuner, C. (2012). The European Commission's proposed data protection regulation: A copernican revolution in European data protection law. *Privacy & Security Law Report*, 1–15.

Lachaud, E. (2018). The General Data Protection Regulation and the rise of certification as a regulatory instrument. *Computer Law and Security Review*, *34*(2), 244–256. https://doi.org/10.1016/j.clsr.2017.09.002

Ladeur, K.-H. (2004). Methodology and European law – Can methodology change so as to cope with the multiplicity of the law? In M. Van Hoecke (Ed.), *Epistemology and Methodology of Comparative Law*. Hart Publishing.

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2). https://doi.org/10.1177/2053951714541861

Marks, G. (1993). Structural policy and multilevel governance in the EC. In A. Cafruny & G. Rosenthal (Eds.), *The State of the European Community: The Maastricht Debate and Beyond* (pp. 391–411). Boulder, Colorado: Lynne Rienner.

Marques, G., & Martins, L. (2000). *Direito da informática*. Coimbra: Almedina.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing: Recommendations of the National

Institute of Standards and Technology. *National Institute of Standards and Technology, Information Technology Laboratory*, *145*, 7. https://doi.org/10.1136/emj.2010.096966

Michaels, R. (2019). The functional method of Comparative Law. In M. Reimann & R. Zimmermann (Eds.), *The Oxford Handbook of Comparative Law*. Oxford University Press.

Ministério dos Negócios Estrangeiros. *Aviso de 02/01/1979.* , (1979).

Moghaddam, F. F., Ahmadi, M., Sarvari, S., Eslami, M., & Golkar, A. (2015). Cloud computing challenges and opportunities: A survey. *2015 International Conference on Telematics and Future Generation Networks, TAFGEN 2015*, pp. 34–38. https://doi.org/10.1109/TAFGEN.2015.7289571

Moore, S. F. (1973). Law and social change: The semi-autonomous social field as an appropriate subject of study. *Law & Society Review*, *7*(4), 719–746.

Moreira, V., & Canotilho, J. J. G. (2007). *Constituição da República Portuguesa Anotada (Vol. 1)*.

Morsink, J. (1999). *The Universal Declaration of Human Rights: Origins, Drafting, and Intent*. Philadelphia: University of Pennsylvania Press.

Murtaza, S., & Al Masud, R. (2012). An extended and granular classification of cloud's taxonomy and services. *International Journal of Soft Computing and Engineering*, *2*(2), 278–286.

Nickel, J. W. (1987). *Making Sense of Human Rights: Philosophical Reflections on the Universal Declaration of Human Rights*. Berkeley: University of California Press.

Normand, R., & Zaidi, S. (2008). *Human Rights at the UN: The Political History of Universal Justice*. Bloomington: Indiana University Press.

Oderkerk, M. (2018). The need for a methodological framework for comparative legal research – sense and nonsense of "methodological pluralism" in Comparative Law. *Rabels Zeitschrift Für Ausländisches Und Internationales Privatrecht*, *79*(3), 589. https://doi.org/10.1628/003372515x14339403063927

ONU. (2017). Drafting of the Universal Declaration of Human Rights: A Historical Record of the Drafting Process. Retrieved June 6, 2018, from http://research.un.org/en/undhr/introduction

Pallis, G. (2010). Cloud computing: The new frontier of internet computing. *IEEE Internet Computing*, *14*(5), 70–73.

Pearson, S. (2009). Taking account of privacy when designing cloud computing services. *ICSE-Cloud 2009, Vancouver. IEEE, Los Alamitos (2009); HP Labs Technical Report, HPL-2009-54 (2009)*.

Pearson, S., & Charlesworth, A. (2009). Accountability as a way forward for privacy protection in the cloud. *IEEE International Conference on Cloud Computing*, 131–144. Springer.

Pearson, S., Shen, Y., & Mowbray, M. (2009). A privacy manager for cloud computing. *IEEE International*

Conference on Cloud Computing, 90–106.

Perlroth, N., Larson, J., & Shane, S. (2013). NSA able to foil basic safeguards of privacy on web. *The New York Times*, *5*, 1–8. Retrieved from http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

Pinheiro, A. S., Coelho, C. P., Duarte, T., Gonçalves, C. J., & Gonçalves, C. P. (2018). *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina.

Platsas, A. E. (2008). The functional and the dysfunctional in the comparative method of law: Some critical remarks. *Electronic Journal of Comparative Law*, *12*(3), 1–16.

Porcedda, M. G. (2018). Patching the patchwork: Appraising the EU regulatory framework on cyber security breaches. *Computer Law and Security Review*, *34*(5), 1077–1098. https://doi.org/10.1016/j.clsr.2018.04.009

Poullet, Y. (2018). Is the General Data Protection Regulation the solution? *Computer Law and Security Review*, *34*(4), 773–778. https://doi.org/10.1016/j.clsr.2018.05.021

Qian, L., Luo, Z., Du, Y., & Guo, L. (2009). Cloud computing: An overview. *IEEE International Conference on Cloud Computing*, 626–631. Berlin, Heidelberg: Springer.

Reding, V. (2011). Tomorrow's privacy: The upcoming data protection reform for the European Union. *International Data Privacy Law*, *1*(1), 3–5.

Reding, V. (2012). The European data protection framework for the twenty-first century. *International Data Privacy Law*, *2*(3), 119–129. https://doi.org/10.1093/idpl/ips015

Reimann, Mathias. (2002). The progress and failure of comparative law in the second half of the twentieth century. *The American Journal of Comparative Law*, *50*(4), 671–700.

Reitz, J. C. (1998). How to do Comparative Law. *American Journal of Comparative Law*, *46*(4), 617–636. https://doi.org/10.2307/840981

Rittinghouse, J. W., & Ransome, J. F. (2010). *Cloud Computing Implementation, Management, and Security*. Boca Raton: CRC Press.

Rudgard, S. (2018). Origins and historical context of Data Protection Law. In E. Ustaran (Ed.), *European Data Protection: Law and Practice*. Portsmouth: IAPP.

Rudolf, B. (2006). Council of Europe: Von Hannover v. Germany. *International Journal of Constitutional Law*, *4*(3), 533–539. https://doi.org/10.1093/icon/mol024

Russo, B., Valle, L., Bonzagni, G., Locatello, D., Pancaldi, M., & Tosi, D. (2018). Cloud computing and the new EU General Data Protection Regulation. *IEEE Cloud Computing*, *5*(6), 58–68. https://doi.org/10.1109/MCC.2018.064181121

Samuel, G. (2004). Epistemology and Comparative Law. In M. Van Hoecke (Ed.), *Epistemology and Methodology of Comparative Law*. Oxford: Hart Publishing.

Samuel, G. (2013). Comparative law and its methodology. In D. Watkins & M. Burton (Eds.), *Research methods in law*. London: Routledge.

Schubert, L., & Jeffery, K. (2012). *Advances in clouds: Research in future cloud computing*. https://doi.org/http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-finalreport-experts.pdf

Schwarz, P. (2014). Information privacy in the cloud. *University of Pennsylvania Law Review*, *161*. Retrieved from http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2907&context=facpubs

Shawish, A., & Salama, M. (2014). Cloud computing: Paradigms and technologies. In F. Xhafa & N. Bessis (Eds.), *Inter-cooperative collective intelligence: Techniques and applications* (pp. 39–68). https://doi.org/10.1007/978-3-642-35016-0

Siems, M. M. (2018). *Comparative Law* (2nd ed.). Cambridge University Press.

Silva, A. C. M. S. (2016). *Análise jurídica da gestão da informação sensível nos serviços cloud*. Universidade do Minho.

Sindhu, S., & Sindhu, D. (2017). Cloud computing models and security challenges. *International Journal of Engineering Science and Computing*, *7*(4), 10934–10941. Retrieved from http://ijesc.org/upload/ea18d45990170c751b2b2531393b25e1.Cloud Computing Models and Security Challenges.pdf

Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010). Security and privacy challenges in cloud. *IEEE Security and Privacy*, *8*(6). https://doi.org/10.1109/MSP.2010.186

Talbot, D. (2010). Security in the ether. *Technology Review*, *113*(1), 36–42.

Talia, D. (2011). Cloud computing and software agents: Towards cloud intelligent services. *WOA*, *11*, 2–6. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.229.71&rep=rep1&type=pdf

Tamanaha, B. Z. (2008). Understanding legal pluralism: Past to present, local to global. *Sydney L. Rev.*, *30*. https://doi.org/10.4324/9781315091891-17

The Cloud Privacy Check (CPC). (2017). *Cloud & data protection 06/2017*.

The Guardian. (2013a). NSA collecting phone records of millions of Verizon customers daily. Retrieved August 27, 2018, from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

The Guardian. (2013b). NSA whistleblower Edward Snowden: “I don’t want to live in a society that does these sort of things" – video. Retrieved August 27, 2018, from https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

Toshkov, D. (2016). Compliance and enforcement of EU law: Who wins, who loses, and who settles. *Ninth Annual Conference on the Political Economy of International Organizations*, 1–26. Salt Lake City, Utah.

Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community. , (2007).

Trnski, M. (2005). Multi-level governance in the EU. In *Regional Co-operation as Central European Perspective* (pp. 23–32). Pécs: Európa Centrum PBC.

United Nations. *Universal Declaration of Human Rights.* , (1948).

van Dijk, P., & Hoof, G. J. H. (1998). *Theory and Practice of the European Convention on Human Rights*. The Hague: Kluwer Law International.

Van Hoecke, M. (2015). Methodology of comparative legal research. *Law and Method*, 1–35. https://doi.org/10.5553/rem/.000010

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, *39*(1).

Vasconcelos, M. da G. das N. (2012). *Comunicações electrónicas e direitos fundamentais no âmbito do Direito da União Europeia*.

Verble, J. (2014). The NSA and Edward Snowden: Surveillance in the 21st century. *ACM SIGCAS Computers and Society - Special Issue on Whistleblowing*, *44*(3), 14–20. https://doi.org/10.1145/2684097.2684101

Vidovic, M. Š. (2016). EU data protection reform: Challenges for cloud computing. *Croatian Yearbook of European Law and Policy*, *12*(1), 171–206. https://doi.org/10.1525/sp.2007.54.1.23.

Vogenauer, S. (2006). Sources of law and legal method in comparative law. In R. Zimmermann & M. Reimann (Eds.), *The Oxford Handbook of Comparative Law*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=944547

Voigt, P., & Bussche, A. von dem. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer.

von Benda-Beckmann, K. (2002). Globalisation and legal pluralism. *International Law FORUM Du Droit International*, *4*(1), 19–25.

Voorsluys, W., Broberg, J., & Buyya, R. (2011). Introduction to Cloud Computing. In R. Buyya, J. Broberg,

& A. Goscinski (Eds.), *Cloud Computing: Principles and Paradigms*. New Jersey: John Wiley & Sons, Inc.

Vries, S. A. de. (2017). The Charter of Fundamental Rights and The EU's "creeping" competences: Does the Charter have a centrifugal effect for fundamental rights in the EU? In S. Douglas-Scott & N. Hatzis (Eds.), *Research Handbook on EU Law and Human Rights* (pp. 58–98). Cheltenham: Edward Elgar.

WeDo Technologies. (2011). *The cloud: Hype or new horizon?* Retrieved from http://www.wedotechnologies.com/0_content/wedo_technologies/white_papers/telecom/WeDo_Technologies_The_Cloud_-_Hype_or_new_horizon.pdf

Wessel, R. A., & Wouters, J. (2007). The phenomenon of multilevel regulation: Interactions between global, EU and national regulatory spheres. *International Organizations Law Review*, *4*, 257–289. https://doi.org/10.1163/157237308X278232

Wessel, R. A., & Wouters, J. (2008). The phenomenon of multilevel regulation: Interactions between global, EU and national regulatory spheres: Towards a research agenda. In A. Føllesdal, R. A. Wessel, & J. Wouters (Eds.), *Multilevel Regulation and the EU: The Interplay Between Global, European, and National Normative Processes* (pp. 9–48). Leiden: BRILL.

Whytock, C. A. (2009). Legal origins, functionalism, and the future of comparative law. *BYU L. Rev.*, 1879–1906.

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

Wouters, J., Wessel, R. A., & Follesdal, A. (2008). Multilevel regulation and the EU: A brief introduction. In A. Føllesdal, R. A. Wessel, & J. Wouters (Eds.), *Multilevel Regulation and the EU: The Interplay between Global, European and National Normative Processes* (pp. 1–6). https://doi.org/10.1163/ej.9789004164383.i-426.6

Youseff, L., Butrico, M., & Silva, D. (2008). Toward a unified ontology of cloud computing. In *In Grid Computing Environments Workshop, 2008. GCE'08* (pp. 1–10). IEEE.

Zetterquist, O. (2011). The Charter of Fundamental Rights and the European Res Publica. In G. Di Federico (Ed.), *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument*. Bologna: Springer.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7–18. https://doi.org/10.1007/s13174-010-0007-6

Zhao, B. (2014). The Internationalisation of Information Privacy: Towards a Common Protection. *Groningen Journal of International Law*, *2*(2), 1–13.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

Zumbansen, P. C. (2012). Defining the space of transnational Law: Legal theory, global governance & legal pluralism. *Transnational Law and Contemporary Problems*, *21*(2), 305–336. https://doi.org/10.2139/ssrn.1934044

Zweigert, K. (1972). Methodological problems in comparative law. *Israel Law Review*, *7*(4), 465–474.