1 Introduction

The ubiquitous presence of information technology in people's daily routine poses challenges regarding the protection of the information they share. Social media, fora, instant messaging, mobile applications and e-commerce activities are some of the most popular technologies that heavily rely on personal data being collected and exchanged, for the provision of respective services. One of the most valuable types of data managed by companies is personal information. Personal data that people share online, exchanged on a broad scale, constitute one of the driving forces of modern enterprises (Spiekermann *et al.*, 2015). Personal data protection legislation attempts to pose restrictions to the uncontrollable use of such data by governments, enterprises, etc. However, different national laws have substantially different characteristics (Palmieri, 2019), allowing organisations to take advantage of such blurred territories of legislation and proceed with the exploitation and processing of such data. Up to May 2018, European Union (EU) Member States applied national privacy laws, following the (Directive 95/46/EC) that the organisations had to comply with. With the General Data Protection Regulation (Regulation (EU) 2016/679) (hereafter, GDPR or Regulation), EU adopted a unified privacy law, aiming to protect and regulate the massive usage of personal data.

Compliance with the GDPR comprises a challenging project for organisations for a series of reasons; the complexity of business activities and the duplication of data (in different information flows or even entire departments within an organisation) are the most important ones. In addition, although organisations are obliged to comply with the GDPR, they lack guidelines that could help them into complying with these requirements. There are technical solutions being developed that can facilitate the compliance with the GDPR, however, none of the current technical solutions can capture the current personal data protection status of an organisation, identify the gaps, assess the criticality of the processing activities and the personal data they use, provide concrete solutions tailored to each organisation to finally fortify its processes and guarantee the protection of individuals' personal data (IAPP, 2018a).

This paper argues that the ISO 27k standard series can form a useful baseline for businesses to build their "towards-compliance" strategy upon, dealing with topics such as risk definition and assessment, continuous evaluation and appropriate documentation. (ISO/IEC 27001:2013 (2013)) (hereafter, ISO 27001) and GDPR aim both to strengthen data security and mitigate the risk of data breaches, and they both require organisations to ensure the confidentiality, integrity and availability of data. Recital 83 of the GDPR states: "*In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption"*. This is also in line with the fact that the market is already mature in the implementation of ISO 27001 ISMS as shown by the constantly increased ISO 27001 certificates issued to organisations; 39,501 ISO 27001 certificates were issued to organisations, worldwide, in 2017[1].

The information-risk-driven approach, which is also followed by the GDPR, consists a fundamental perspective for ISO 27001. ISO 27001 provides detailed best practices while Article 24 of the GDPR specifies that adherence to codes of conduct and approved certifications can be used as an element for demonstrating compliance. There are several similarities as they both aim to cultivate a culture of protecting processes/assets/data and shaping the organisation's philosophy towards this direction. Therefore, this paper argues that for organisations that base their information security frameworks on ISO 27001, compliance with the GDPR requires limited (or at least less than the one required if no such certification exists) effort, as many processes and controls should already be in place, as should be the organisation's attitude towards protecting processes/assets/data. Towards this direction, the authors in (--) have identified synergies by analysing the ISO 27001 standard and the GDPR by extracting the main concepts from both texts, and have proposed best practices for compliance. Next, (--) focuses on the

[1] https://www.iso.org/the-iso-survey.html

security controls level, rather than on security management practices that the (ISO/IEC 27002:2013) (hereafter, ISO 27002) to meet GDPR requirements, by focusing on data protection actions.

Taking into account that there are a lot of ISO 27001 certified organisations, and the market is mature enough to take this certification as a starting point and build on it towards the compliance with the GDPR, the aim of this work is to provide a comprehensive roadmap to organisations that are already ISO27001 certified, by identifying the remaining actions need to be performed by organisations in order to be able to comply with the GDPR. This paper provides a complete analysis of the additional actions needed to be done that will allow an ISO 27001 certified organisation to be compliant with the GDPR.

The rest of the paper is structured as follows. Section 2 presents an overview regarding the acceptance of the GDPR by organisations almost two years after its application. Section 3 analyses the ISMS framework of ISO 27001 and identifies synergies with the GDPR compliance efforts. Section 4 presents the remaining necessary actions that the GDPR describes as necessary for the protection of individuals' personal data protection. Finally, Section 5 concludes the paper by providing overall conclusions and issues for further research.

2 Challenges in personal data protection in the GDPR era

Through the GDPR, EU regulators aim to enforce significant changes on the way that organisations process data subjects' personal information. Even though these changes are expected to promote the privacy of the data subjects, they pose significant challenges for organisations to make considerable shifts on their information technology, culture, business processes, and generally the way they function. Some of these challenges have been documented by organisations, academic papers or by European Commission reports, highlighting the particular aspects of the GDPR that pose these challenges.

Since April 2016 GDPR entered into force, reports were released revealing that organisations are not ready and compliance will be a challenging issue. Gartner (2017) argues that organisations are unprepared and highlights the responsibility of organisations outside the EU. Similarly, the report by Ernst&Young in (Ernst&Young, 2018), states that only 33% of the responding organisations had a plan to address GDPR compliance at the time the survey (October – November 2017) was conducted while 39% of the respondents indicated that they are not at all familiar with the GDPR. This picture does not seem to change much after the GDPR came into force. A recent (Thomson Reuters, 2019) article highlights that evidence show that organisations are still not fully aware of the GDPR's potential impact and are not ready for the GDPR compliance issues. In a survey (IAPP, 2018b) among privacy professionals which was published in 2019, it appears that less than half of respondents said they are fully compliant with the GDPR. Interestingly, nearly 20% of the privacy professionals who participated argue that full GDPR compliance cannot be achieved.

A general challenge pertaining GDPR compliance is the gap in the existence of supporting technologies. Reports identify that although GDPR compliance processes are complex, they are mostly implemented manually, which is not sustainable (McKinsey, 2018). Among the reported challenges (CSA, 2018), it seems that organisations are struggling to satisfy the data subjects' right to erasure ("right to be forgotten") (GDPR/Article 17). This was cited by 53% of the survey respondents as the biggest challenge on achieving compliance with the GDPR. Implementing data protection-by-design and -by-default (GDPR/Article 25) follows with 42% and "records of processing activities" (GDPR/Article 30) with 39%. (IAPP, 2019) has published a Data Protection Officer's (DPO) experience on the GDPR a year after it entered into force and also has highlighted that managing and addressing data subjects' requests was the biggest challenge. Additionally, organisations find challenging the implementation of data breaches reporting (McKinsey, 2018) and only 18% of Ponemon Institute survey (2019) state confidence to communicate reportable data breaches within 72 hours of becoming aware of it.

3 From information security controls to personal data protection controls

ISO 27001 provisions good practices for information security management, risk management and taking security measures, within the context of an Information Security Management System (ISMS) while ISO 27002 provides a list of controls and good practices that can be used as guides when selecting and implementing measures to achieve information security. Juxtaposing ISO 27001 and the GDPR we have identified that, though they adopt different perspectives, both focus on the minimisation of risk realised by data breaches. ISO 27001 focuses on reducing risks to information security by compelling organisations to produce ISMS that are continuously maintained and improved. GDPR aims at the preservation of privacy of individuals, providing them with rights against organisations that process their personal data. GDPR also promotes accountability, by placing clear data protection responsibilities to organisations processing such data. Accountability lies on the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk (GDPR/Article 32).

Both GDPR and ISO 27001 desire the cultivation of the appropriate culture from the leadership till the lower levels of the organisation chart, and the development awareness within the whole organisation as well, regarding the protection of data, exploiting security measures (IAPP, 2018a). The GDPR provisions numerous personal data protection settings and controls, many of which are also recommended in ISO 27001, ISO 27002, and other "ISO27k" standards. Organisations that currently have an ISMS are likely to satisfy many of the GDPR requirements already, needing a few adjustments to be made.

In this section we analyse the ISMS framework included in ISO 27001 and identify synergies with the GDPR compliance efforts. In the following subsections the fourteen control modules of Annex A' of ISO 27001 are presented, focusing on the controls of each objective. At this level, we extend the information security controls to personal data protection controls, analysing and describing the necessary additional actions that an organisation is required to implement towards GDPR compliance. Finally, we provide suggestions to the organisations that are already certified according to the ISO 27001, on necessary actions in order to comply with the requirements of the GDPR.

3.1 Enhancing information security policies with data protection policies

The first control module of ISO 27001 and ISO 27002 includes one control related with the management direction for information security.

Actions towards GDPR compliance: The organisation should be based on the information security policy that has already been developed in order to establish a Data Protection Policy (DPP). The DPP describes the set of rules that define how the organisation protects personal data, so that it complies with the GDPR and protects the privacy of the data subjects. The purpose of the DPP is to provide strategic guidance to the organisation's management and staff for the protection of personal data when processing them. The DPP applies to all operational processes that involve personal data processing. Moreover, it applies to all employees and associates of the organisation who are directly or indirectly involved in the processing of personal data.

This policy should be distinct from the information security policy (Lambrinoudakis, 2018) and should provide information on new processes that regulate organisational aspects pertaining to the way the organisation:

- Manages consent
- Fulfils data subjects' rights
- Makes transfers of personal data to third countries
- Manages collaborating third parties
- Manages transfer or disclosure of personal data
- Responds to incidents that may lead to a personal data breach

- Monitors personal data processing activities and supporting assets, to continuously ensure compliance with the regulation
- Manages personnel awareness and training of specialised personnel (in order to ensure that they have the knowledge and skills to apply the DPP)
- Implements data protection-by-design and -by-default principles regarding systems and applications the organisation develops in-house or through procurement

Similarly to the information security policy, the DPP is not static but should be kept as up to date as possible and adjusted in line with the changes of information systems and the technical and social environment. The DPP should be updated periodically and this process should be documented. In addition, it should also be updated in the event of major changes to the organisation or its IT systems. The senior management of the organisation assigns the responsibility for reviewing the DPP to the DPO.

3.2 Extending organisation of information security with personal data protection structures and roles

This control module refers to i) the internal organisation, and ii) the mobile devices and teleworking. The category concerning Internal Organisation includes five controls. The first refers to information security roles and responsibilities, mentioning that all information security responsibilities should be defined and allocated. The second calls for segregation of duties, where conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets. The third designates maintaining contacts with relevant authorities. The fourth provisions maintaining contacts with special interest groups or other specialist security forums and professional associations. Finally, the fifth control refers to information security in project management, where information security should be addressed in project management, regardless of the type of the project.

Actions towards GDPR compliance: Apart from internal organisation with respect to security, the organisation should implement an organisational framework according to which there are roles with responsibilities for personal data protection. This framework should include the role of the DPO; in cases required. The role of the DPO should be designated by the senior management, assigning this responsibility to a competent person reporting directly to the senior management without receiving any instructions on how to perform his/her tasks. Senior management needs to ensure that the DPO is not dismissed or penalised for performing his/her tasks. The organisational structure should reflect the distinct role of the DPO. Article 39 of the GDPR prescribes the cases in which a DPO should be appointed.

Regarding contact with authorities, the Data Controllers need to cooperate with the supervisory authorities when a data breach occurs (GDPR/Article 33), informing them *without undue delay*, when the personal data breach affects the rights and freedoms of the corresponding natural persons. When the Data Controller realises that the data breach may pose a high risk to their rights and freedoms, they should also inform the data subjects for the violation of their data (GDPR/Article 34).

Regarding contact with special interest groups, in order for a Data Controller to be able to guarantee the protection of the personal data they process, they need to conduct a Data Protection Impact Assessment (DPIA) when particular types of processing is likely to result in a high risk to the rights and freedoms of natural persons (GDPR/Article 35).

Finally, organisations should establish a code of conduct (GDPR/Article 40). Codes of conduct can contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises. They are related to associations and other bodies that represent Data Controllers or Data Processors. To this direction, Data Controllers and Data Processors are encouraged by the GDPR to be certified with a certification mechanism (GDPR/Article 42). Codes of conduct can be drawn up by organisations that represent Data Controllers or Data Processors and approved either by the supervisory authority of a member state or by the European Data Protection Board.

3.3 Expanding human resources security controls to protect personal data handled by employees

The human resources security module consists of three subcategories, i) information security prior to employment; ii) during employment, and iii) termination and change of employment. Information security prior to employment designates screening and applying terms and conditions, while during employment, security controls refer to the management responsibilities, information security awareness, education and training and disciplinary process. Finally, at the termination and change of employment organisations should handle remaining information security responsibilities.

Actions towards GDPR compliance: Further actions should be taken regarding the protection of personal data that an organisation processes by its employees. The organisation should take appropriate measures and controls to protect the personal information (of the personal data of natural persons that the organisation keeps, e.g., personal data of customers, suppliers) that employees process within the scope of their occupation. Specifically, before the employment of their employees, an organisation should take appropriate measures to ensure that the employees are fit to handle personal data, e.g., by informing them about possible legal consequences during the exercising of the work activities (regarding personal data misuse, etc.). During employment, the organisation should review the existing contracts of their employees who have access to personal data, and make sure that they include specific clauses for confidentiality, with legal bindings. Finally, after the employment, the organisation should remove employees' access rights to personal data.

3.4 Enhancing asset management with personal data management

Asset management's module contains three controls: i) responsibility for assets; ii) information classification; and iii) media handling.

Actions towards GDPR compliance: The aim of this clause is to develop and maintain appropriate safeguards for the protection of organisational assets. In this direction, GDPR requires that Data Controllers and Data Processors alike maintain records of their processing activities regarding personal data and special categories of personal data; i.e. sensitive data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership genetic/biometric/health data, sex life, sexual orientation (GDPR/Articles 5, 7, 9, 30). Taking into account that personal data and special categories of personal data also consist a valuable asset, the organisation, acting as a Data Controller, needs to keep records of:

- The categories of data subjects
- The categories of the collected data
- The types of processing activities that have occurred or are likely to take place
- The legal grounds related with the processing (this point is also related with the consent that the organisation should obtain by the data subject)
- Potential recipients of data disclosures
- Potential transfer of data to non-EU countries, accompanied with information regarding the appropriate safeguards these countries have, ensuring an adequate level of protection
- Retention period of the data
- Security measures the organisation applies

When an organisation acts as a Data Processor the records of the processing activities contain contact details of the Data Processor or Data Processors and of each Data Controller on behalf of which the Data Processor is acting, and where applicable, the contact details of the DPO; the categories of processing activities; potential transfer of data to non-EU countries and information regarding technical and organisational security safeguards the organisation applies. The organisation should keep documented records of processing activities.

Additionally, organisations should develop appropriate procedures that allow provision of information to the data subject related to the aforementioned personal data they keep (GDPR/Articles 13-14).

3.5 Implementing data protection-by-design and -by-default in access control

The access control module contains four controls: i) business requirements of access control; ii) user access management; iii) user responsibilities; and iv) system and application access control. These controls are related with guidelines about management of access of the users to information, aiming at the prevention of unauthorised access to services and systems and at making each user accountable for safeguarding organisation's authentication information.

Actions towards GDPR compliance: Taking the above actions as a basis, the organisation should further extend access control systems by implementing a process through which the data subjects can either correct, or request correction (GDPR/Article 16) of the personal data the organisation holds for them or erase, or request the erasure (GDPR/Article 17) of such data. Automated access, rectification, and erasure should be established by the security team. Additionally, with respect to Recital 63[2], the organisation should be able to generate records of the data subjects' requests and the timeliness of the organisation's response. This functionality can also facilitate the measurement of the performance of the organisation to a data subject's request, ensuring that the appropriate information is provided to data subjects upon request in a secure way.

Additionally, the organisation should develop their systems with respect to data protection-by-design and -by-default principles (GDPR/Article 25) in order to protect users' privacy. This means that when designing the access control safeguards the organisation should not take into account only the security requirements (e.g., identification, accountability), but also take into account privacy requirements and principles (e.g., data minimisation).

3.6 Employing cryptography

The control module Cryptography contains one control, i.e. cryptographic controls, which aims at ensuring proper and effective use of the technological measure of cryptography in order to protect the confidentiality, authenticity and/or integrity of information.

Actions towards GDPR compliance: Encryption and pseudonymisation are the two technical measures that the GDPR proposes (GDPR/Article 32). Based on (ENISA, 2013), using encryption, privacy is preserved by keeping personal data confidential, and thus, unauthorised users are not allowed to have access to it. Moreover, for the satisfaction of the data subjects' right to data portability (GDPR/Article 20), the organisation is encouraged to apply encryption to securely communicate the corresponding personal data to other organisations. Based on the criticality of the data and on the risk for an organisation, encryption can be applied to protect equipment, databases, partitions or containers, standalone files, emails, communication channels (CNIL, 2018).

We should note that when anonymisation (which differs from pseudonymisation (Pfitzmann and Hansen, 2010) as it enables the data subject to remain unidentifiable) is applied to a data set, this data set is exempted from GDPR obligations (GDPR/Recital 26). Therefore, anonymisation is a method that can minimise the risk for an organisation when a requirement to store a data subject's identity no longer exists (e.g., keeping data for statistical results). According to (CNIL, 2018), an organisation should determine what has to be anonymised, based on the nature of the data and the risk create for the organisation. Next, organisations can either permanently anonymise the data, or can choose tools (e.g., partial deletion, encryption, hashing, indexing, etc.) that are closer to their requirements.

3.7 Enhancing communications security with personal data protection objectives

This control module contains two controls: network security management and information transfer.

[2] Provision of remote access to a secure system that would provide the data subject with direct access to their personal data

Actions towards GDPR compliance: Taking the above controls as a basis, an organisation can further focus on the design and development of the communication security, protecting thus personal data of any party in its network requesting access to personal data (GDPR/Article 26). This can be extended to the international transfers, where the organisation, before transferring the requested personal data, should have received appropriate safeguards ensuring an adequate level of protection of the corresponding country, the territory, or one or more specified sectors within that third country.

Additionally, appropriate roles should be assigned to the employees who have access to personal data, accompanied with specific responsibilities. This functionality promotes accountability and transparency, while it consists a basis for the accurate response of the organisation, either to any request received by a data subject regarding the processing of their data (GDPR/Articles 13-22), or to the supervisory authority, when a data breach occurs (GDPR/Articles 31, 33). In this way, the organisation is able to locate and retrieve securely the personal data it keeps.

3.8 Acquiring, developing and maintaining systems according to data protection principles

The control module of system acquisition, development and maintenance consists of three controls, i) security requirements of IS, ii) security in development and support process, and iii) test data.

Actions towards GDPR compliance: The requirements of these controls guide the organisation to design and develop information systems and applications following security-by-design principles. According to Article 25 of the GDPR, the organisations should also apply data protection-by-design principles (Cavoukian, 2009). The protection of personal data and users' privacy can be improved and enhanced by designing information systems in a way that reduces the degree of invasion in privacy. One of the measures that the Regulation proposes is data minimisation. In this way, organisations minimise the data they collect to the minimum level demanded for their processing activities. In this area belong a series of methodological frameworks and tools that help analysts, designers and developers to develop ISs that privacy will be a built-in and not an add-on feature. To include privacy as a concept in the software development cycle, it should be transformed into a technical requirement.

In addition, the organisation should estimate/assess the profit in relation to the cost (cost-benefit analysis) of managing a new system related to the lawful processing of data (GDPR/Article 6). This should also be covered in the risk assessment and management process, and taken under consideration when designing or upgrading systems and processes. This assessment may indicate, for example, that some personal data processing residual risk may be accepted, or this risk should be further mitigated by applying one or more security controls.

Also, the organisation should be able to identify and assess the special categories of personal data they process. Information risks could be avoided, where feasible, by assessing the usefulness of the personal and special categories of personal data they keep. Towards risk minimisation, the aggregation of such data is also accepted (GDPR/Articles 9, 11).

In addition, in order to satisfy the right of data subjects to know the outcome of requests related with the correction, completion, erasure, restriction of their personal data (GDPR/Article 19), the organisation should inform the requestor on the above, also providing that this process/application form is easy for insiders and outsiders of the organisation to follow.

3.9 Managing supplier relationships while protecting personal data

The module Supplier Relationships consists of two controls, i) information security in supplier relationships, and ii) supplier service delivery management.

Actions towards GDPR compliance: This control module sets the basis for the establishment of a security framework among an organisation and the external parties it collaborates with, ensuring the protection of the transferred information. GDPR sets specific requirements regarding the management of the relationship of the Data Controller with its Data Processors. If an organisation uses one or more third parties to process personal information ("Data Processors"), it must ensure they too are compliant

with the GDPR (GDPR/Articles 27-28). Towards this direction, Data Controllers should conduct continuous evaluation of their Data Processors and suppliers, and use approved certification mechanisms in order to demonstrate that they ensure an adequate level of protection with respect to data protection-by-design and -by-default principles.

Moreover, organisations need to ensure the proper handling of privacy and other information security aspects of their business partners. This might contain aspects such as jointly investigating and resolving privacy incidents, breaches or access requests, to name a few. These requirements are applied to any relationship the organisation has with external parties, such as ISPs and CSPs, and any other third party that the organisation has exchanged (personal) data with, for example external payroll or marketing companies.

Finally, when data is transferred outside EU, involved organisations should ensure the level of protection of the involved natural persons. Consequently, organisations located outside Europe that interact with European organisations must formally nominate privacy representatives inside Europe if they meet certain conditions (GDPR/Article 27).

3.10 Including data breach notification in incident management

The control module Information Security Incident Management consists of one category which is realised through seven controls. The objective of this category is to ensure a consistent and effective approach to the management of information incidents.

Actions towards GDPR compliance: The organisation that has already established incident management handling procedures, has allocated the relative responsibilities to each employee, and has developed a policy that has been communicated to all involved parties (employees, external parties) containing the actions that have to be taken when a security incident has occurred. For the satisfaction of the Article 33 of the GDPR, the organisation should implement process in order to be able to notify the supervisory authority. Specifically, when a potential data breach occurs, and provided there is a risk for natural persons, the organisation, when acting as a Data Controller, must inform the competent supervisory authority *without delay and, if possible, no later than 72 hours from the time it occurred*, and the data subjects (GDPR/Article 35), if it is required. The organisation, when acting as a Data Processor, should promptly notify the Data Controller for the violations. This notice must be "immediate" to help the Data Controller comply with the time commitments. If the organisation acts as a Data Processor and offers services to more than one Data Controllers, it must report the incident and details about it, to each of them. As the requirement for timely notification to the supervisory authority is too demanding, the organisation should implement procedures for timely notification (i.e. what types of data the organisation should provide (GDPR/Article 33, par.3)) and for communication to data subjects, when necessary.

3.11 Enhancing compliance to satisfy lawfulness of processing

The module Compliance consists of two categories, i) compliance with legal and contractual requirements, and ii) information security reviews, aiming at the avoidance of information security breaches and of any security requirements and at ensuring that the information security is implemented and operated in accordance with the organisational policies and procedures.

Actions towards GDPR compliance: Organisations should extend their actions towards compliance, in order to comply with the GDPR, by following these six privacy principles (GDPR/Article 5):

1. Lawfulness, fairness, and transparency: Regarding lawfulness, the processing should fulfil the described tests in the GDPR. Fairness means that the processed data must match the description. Transparency is achieved by informing the data subject what data processing is to be done.
2. Purpose limitations: Personal data can be acquired only for *specified, explicit and legitimate purposes*}. This data may only be used for a specific purpose of processing of which the subject is made aware and no other, without acquiring further consent.

3. Minimisation of data: Collected data on a data subject should be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*. Only the minimum amount of data is to be kept for the purposes of specific processing.
4. Data accuracy: Data should be *accurate and where necessary kept up to date*. Proper protection and measures against identity theft can be taken through baselining. Holders of data have to build processes for rectification into data management/archiving activities regarding the data subject.
5. Limitations of storage: It is expected by the Data Controller that personal data is *kept in a form which permits identification of data subjects for no longer than necessary*. The data that is no longer required, should be deleted.
6. Confidentiality and integrity of data: It is required from the Data Controllers or Data Processors that data be handled *in a manner [ensuring] appropriate security of the personal data, including protection against unlawful processing or accidental loss, destruction, or damage*.

The organisation must ensure that the above six principles are followed regarding the processing of personal data. However, in order for a processing to be lawful, the organisation should have ensured that at least one of the following applies:

1. The data subject has provided their consent regarding the processing of their personal data.
2. There exists a contract between the Data Controller and the data subject.
3. Processing is necessary for compliance with a legal obligation of the Data Controller.
4. Processing is necessary for the protection of vital interests of natural persons.
5. Processing is necessary for the performance of a task related with public interest
6. Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party.

In order to satisfy the above requirements, the organisation should follow a specific procedure for identifying the types of data processed (personal, special categories, convictions) and be able to prove that the way the data is processed complies with the applicable processing instructions for each type. Moreover, it should document the legal basis for the processing of the data. When consent is the legal basis for the transfer/storage of personal data, special attention should be given in order for consent to be provided by the data subject freely, is specific and clear, and the data subject has been already informed about the processing purposes.

3.12 Modules that support GDPR compliance

The following three modules are also part of the Annex A' of the examined ISO although they have no direct association with GDPR compliance, they can help an organisation develop a culture that will facilitate GDPR compliance. Moreover, these modules are included in our study for the sake of completeness.

3.12.1 Enhancing physical and environmental security for GDPR compliance

This module includes two controls on secure areas and equipment.

Actions towards GDPR compliance: This section applies to the general requirement of the GDPR to the organisations for implementing appropriate technical and organisational measures to ensure the level of security appropriate to the risk (GDPR/Articles 24-25, 28, 32).

3.12.2 Enhancing operations security for GDPR compliance

This module contains seven controls: i) operational procedures and responsibilities, ii) protection from malware, iii) back up, iv) logging and monitoring, v) control of operational software, vi) technical vulnerability management, and vii) information systems audit considerations.

Actions towards GDPR compliance: An organisation is able to demonstrate that they have implemented appropriate technical and organisational measures to safeguard the personal data they keep. Additionally, the organisation should implement procedures related with the management of the satisfaction of the data subjects' rights (GDPR/Articles 12-22) and for the process of the provision of consent of the data subjects (GDPR/Article 7).

3.12.3 Extending business continuity management to support GDPR compliance

This control module contains two controls: i) information security continuity, and ii) redundancies. The objective is the establishment of a business continuity and disaster recovery plan.

Actions towards GDPR compliance: As a general direction for the satisfaction of the GDPR, an organisation should implement appropriate technical and organisational measures to ensure the level of security appropriate to risk (GDPR/Articles 24-25, 28, 32).

3.13 Enhancing the ISMS framework with personal data protection risk management

As mentioned above, one of the fundamental perspectives of ISO 27001 is the information-risk-driven approach, which has not been described as a control per se, but it is part of the ISMS framework. Specifically, according to the clause 6 of ISO 27001, the countermeasures applied by an organisation are not only those described in Annex A', but also those that are the outcome of the security risk assessment.

Accordingly, organisations may need to conduct a DPIA (GDPR/Article 35) to extend the implemented countermeasures for each processing activity. Specifically, an organisation may be required to carry out a DPIA assessment to identify the impact that the processing of personal data, may have, especially in case of a breach. To this end, DPIA is a risk assessment related to the impact that business operations or technologies associated with the processing of personal data, may have. According to Article 35 of the GDPR, DPIA is conducted when particular types of processing is likely to result in a high risk to the rights and freedoms of natural persons.

In order for an organisation to satisfy the requirement for DPIA, the core actions they have to follow are i) to create a list of classified corporate information – including personal data, and ii) to implement an appropriate methodology, and to establish policies and procedures for carrying out an impact assessment. In the literature there are quite a few risk analysis methodologies (Alberts *et al.* 2003; Fredriksen *et al.* 2002; Yazar, 2002), however, Working Party 29 (2017) has released criteria for acceptable DPIA that an organisation can follow, where they also suggest EU generic frameworks as well as sector-specific ones.

3.14 Demonstration of applicability with indicative examples

In the following table we include a fraction of how an organisation can extent ISMS controls and policies to create GDPR compliance policies and controls, respectively. These can be used as a guide of how professionals could start with ISMS policies and controls as a basis to create a GDPR compliance programme.

ISO/GDPR synergies	ISMS policy / control	GDPR policy / control
Enhancing information security policies with data protection policies	Postings by employees from an organisation's email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the organisation, unless posting is in the course of business duties.	Data Protection policy Postings by employees from an organisation's email address to newsgroups should not contain personal data
Extending organisation of information	Secure remote access must be strictly controlled with encryption (i.e. Virtual	Secure remote access must be strictly controlled with encryption

security with personal data protection structures and roles	Private Networks (VPNs)) and strong pass-phrases	when personal data is being transferred
Expanding human resources security controls to protect personal data handled by employees	All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function	All employees who process personal data shall receive appropriate awareness education and training and regular updates in data protection and the current regulation
Enhancing asset management with personal data management	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Personal information, on top of other classification, shall be classified as public, personal or sensitive.
Implementing data protection-by-design and -by-default in access control	Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts	Users must use a separate, unique password for each account they use to process personal data. They may not these passwords for their own personal accounts.
Employing cryptography	All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider	All servers that store and applications that process personal information must have the use encryption and have a certificate by a known, trusted provider
Enhancing communications security with personal data protection objectives	All wireless infrastructure devices that reside at an organisation's site and connect to an organisation's network, must maintain a hardware address (MAC address) that can be registered and tracked.	All wireless infrastructure devices that reside at an organisation's site and provide access to sensitive information must maintain a hardware address (MAC address) that can be registered and tracked.
Acquiring, developing and maintaining systems according to data protection principles	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems	The information privacy related requirements shall be included in the requirements for new information systems or enhancements to existing information systems
Managing supplier relationships while protecting personal data	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain	Agreements with suppliers who are e personal data processors shall include requirements specified in the GDRP to ensure the coverage of the controllers' responsibilities
Including data breach notification in incident management	As soon as a theft, data breach or exposure containing organisation's protected data or sensitive data is identified, the process of removing all access to that resource will begin.	As soon as a theft, data breach or exposure containing organisation's personal or sensitive data is identified, the process of removing all access to that resource will begin and corresponding data authorities should be notified within 72 hours

Enhancing compliance to satisfy lawfulness of processing	The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	The organisation will conduct GDPR internal audits at planned intervals organised and supervised by the DPO. The results will be used to demonstrate compliance.

Table 1: Indicative examples of ISMS polices and controls and respective GDPR extensions

4 Additional GDPR compliance controls

GDPR consists of 11 chapters, analysed in 99 articles. Each chapter corresponds to a thematic area, and contains about 10 articles, that cover all aspects of each theme. In the above section, we captured the common ground between the 14 control modules of ISO27001 and the GDPR. However, there are still some actions described in the GDPR that are not covered by this ISO. This section presents the remaining necessary actions (requirements) that the Regulation describes as necessary for the protection of naturals' persons personal data. When an ISO27001 certified organisation addresses all the additional actions described in this study, this should mean that they are compliant with the GDPR.

4.1 Children consent

The organisation should implement procedure through which will receive the consent when the Data Subject is minor (GDPR/Article 8).

4.2 Criminal convictions and offences

In order for an organisation to process lawfully personal data related with criminal convictions and offences (Article 10), they should i) identify the related legal ground (GDPR/Article 6) that allows them to process such data, and ii) describe in the DPP a procedure through which they will obtain and use personal data related with criminal convictions and offences.

4.3 Authority of the Data Controller/Data Processor

The organisation should implement procedure through which they will check the compliance of the involved to the processing of personal data third parties (i.e. Data Processors, third parties) (GDPR/Article 29) with the terms imposed by the Data Controller. These terms should also be reflected in the contracts between the Data Controller and the involved third parties.

4.4 Prior consultation

Article 36 describes the responsibility of the Data Controller to consult the supervisory authority *prior to processing where a DPIA [...] indicates that the processing would result in a high risk [...].* This action is closely related with the results derived from DPIA regarding the risks associated with the handling of personal data (see Section 4.2). If the identified risks are high and the measures taken are not adequate to protect the data, then the organisation should inform the supervisory authority in order to receive advice regarding the residual risk and sufficient protection of the data.

4.5 Transfer of personal data to third countries

The organisation is allowed to transfer the data to other organisations in third countries or to international organisations complying with the GDPR, to those in jurisdictions deemed "adequate" or to those who are sufficient on the basis of approved company rules (GDPR/Articles 44-49).

If the organisation intends to transfer the processed data in third countries, it must store the data in a database in such a way that it is exportable to common standards (e.g., xml/json/excel table, etc.).

4.6 Data used for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, churches and religious associations

If the organisation processes data that is used for archiving purposes in the public interest, scientific, historical research, or statistical purposes, they should implement procedure for the anonymization/pseudonymization of such data (GDPR/Article 89).

5 Conclusions

The GDPR provisions numerous settings and controls focused on the management and the protection of such data. Many of these controls are also provisioned in ISO 27001, ISO 27002, and other "ISO27k" standards. Thus, organisations that currently have developed an ISMS are likely to satisfy many of the GDPR requirements already, needing a few adjustments to be made. Other organisations might decide to apply an ISMS as a general framework for the management of the personal data of data subjects that they process, in the context of: i) the broader management of the information risks; ii) the security of the data they process, either in hard copy or in a digital version, as well as the relevant compliance; iii) the incident management; and iv) addressing business continuity issues. This work describes the necessary additional actions that an organisation is required to implement since they have already an ISMS in place to reach compliance with the GDPR. That means that if organisations already have an ISO 27001 framework in place, compliance with GDPR requirements will not be necessitated a duplication of the demanded effort. In addition, compliance to the GDPR is mandatory, whereas ISO 27001 certification is not. Organisations can start from ISO 27001 certification and reach GDPR compliance, or vice versa.

This work provides guidelines for practitioners of the domain of information security and protection of privacy, since it presents a roadmap on how to design a "GDPR compliance" project, contributing also to the awareness regarding the protection of personal data of an organisation.

Future work of this study includes the validation of the proposed guidelines towards GDPR compliance by a number of ISO 27001 certified organisations that have also reached GDPR compliance. The analysis of such feedback will further validate (or provide other perspectives to) the findings of this work. Moreover, DPOs could also be involved in this process, providing their experiences regarding the demanded effort to reach GDPR compliance for an already ISO 27001 certified organisation.

References

Alberts, C., Dorofee, A., Stevens, J. and Woody, C., (2003), *Introduction to the OCTAVE Approach*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Cavoukian, A., (2009). "Privacy by design: The 7 foundational principles". *Information and Privacy Commissioner of Ontario, Canada*, *5*.

Cloud Security Alliance (CSA), (2018): "GDPR Preparation and Challenges Survey Report Explores Overall Industry Preparedness in Achieving Compliance", available at: https://cloudsecurityalliance.org/press-releases/2018/04/17/gdpr-preparation-and-challenges-survey-report/ (accessed 08 January 2020).

Commission nationale de l'informatique et des libertés (CNIL), (2018). "Privacy Impact Assessment (PIA) – Knowledge Bases".

--

--

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

Ernst & Young, (2018). "Global forensic data analytics survey", available at: https://eyfinancial-servicesthoughtgallery.ie/global-forensic-data-analytics-survey-2018/, (accessed 08 January 2020).

European Union Agency for Cybersecurity (ENISA), (2013). "Recommended cryptographic measures – securing personal data", available at: https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data (accessed 08 January 2020).

Fredriksen, R., Kristiansen, M., Gran, B.A., Stølen, K., Opperud, T.A. and Dimitrakos, T., (2002). "The CORAS framework for a model-based risk management process". In *International Conference on Computer Safety, Reliability, and Security* (pp. 94-105). Springer, Berlin, Heidelberg.

Gartner, (2017). "Gartner says organizations are unprepared for the 2018 European Data Protection Regulation", available at: https://www.gartner.com/en/newsroom/press-releases/2017-05-03-gartner-says-organizations-are-unprepared-for-the-2018-european-data-protection-regulation (accessed 08 January 2020).

IAAP (2018a). "2018 Privacy Tech Vendor Report", available at https://iapp.org/resources/article/2019-privacy-tech-vendor-report/ (accessed 08 January 2020).

IAPP (2018b). "IAPP-EY Annual Privacy Governance Report 2018", available at: https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/ (accessed 08 January 2020).

IAPP (2019). "GDPR one year later: Looking backward and forward", available at: https://iapp.org/news/a/gdpr-one-year-later-looking-backward-and-forward/ (accessed 08 January 2020).

ISO/IEC 27001:2013 (2013) "Information technology – Security techniques – Information security management systems – Requirements".

ISO/IEC 27002:2013 (2013) "Information technology – Security techniques – Code of practice for information security controls".

Lambrinoudakis, C., (2018). "The General Data Protection Regulation (GDPR) Era: Ten Steps for Compliance of Data Processors and Data Controllers". In *International Conference on Trust and Privacy in Digital Business* (pp. 3-8). Springer, Cham.

McKinsey&Company, (2018). "GDPR compliance after May 2018: A continuing challenge", available at:
https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/GDPR%20compliance%20after%20May%202018%20A%20continuing%20challenge/GDPR-compliance-after-May-2018_A-continuing-challenge.ashx (accessed 08 January 2020).

Palmieri III, N.F., (2019). "Data Protection in an Increasingly Globalized World". *Ind. LJ*, *94*, p.297.

Pfitzmann, A. and Hansen, M., (2010). "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management".

Ponemon Institute, (2019). "A global view of GDPR progress", available at: https://www.mwe.com/law-firm/gdpr/ (accessed 08 January 2020).

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)

Spiekermann, S., Acquisti, A., Böhme, R. and Hui, K.L., (2015). "The challenges of personal data markets and privacy". *Electronic markets*, *25*(2), pp.161-167.

Thomson Reuters (2019). "Study finds organizations are not ready for gdpr compliance issues", available at: https://legal.thomsonreuters.com/en/insights/articles/study-finds-organizations-not-ready-gdpr-compliance-issues (accessed 08 January 2020).

Working Party 29 (2017). "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (accessed 08 January 2020).

Yazar, Z., (2002). “A qualitative risk analysis and management tool–CRAMM”. *SANS InfoSec Reading Room White Paper*, *11*, pp.12-32.