General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance

Vasiliki Diamantopoulou[1(✉)], Aggeliki Tsohou[2], and Maria Karyda[1]

[1] Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece
{vdiamant,mka}@aegean.gr
[2] Department of Informatics, Ionian University, Corfu, Greece
atsohou@ionio.gr

Abstract. The General Data Protection Regulation that is already in effect for about a year now, provisions numerous adjustments and controls that need to be implemented by an organisation in order to be able to demonstrate that all the appropriate technical and organisational measures have been taken to ensure the protection of the personal data. Many of the requirements of the GDPR are also included in the "ISO27k" family of standards. Consequently, organisations that have applied ISO27k to develop an Information Security Management System (ISMS) are likely to have already accommodated many of the GDPR requirements. This work identifies synergies between the new Regulation and the well-established ISO/IEC 27001:2013 and proposes practices for their exploitation. The proposed alignment framework can be a solid basis for compliance, either for organisations that are already certified with ISO/IEC 27001:2013, or for others that pursue compliance with the Regulation and the ISO/IEC 27001:2013 to manage information security.

Keywords: General Data Protection Regulation · ISO/IEC 27001:2013 · Information Security Management System · Compliance

1 Introduction

Personal data is one of the driving forces of modern enterprises and is nowadays exchanged on a broad scale [12]. Consequently, the necessity for protecting individuals' personal data is of utmost importance, especially when taking under consideration the value that personal data has for the digital economies and the interest that its collection attracts, either for public or private organisations. This necessity might have already been imposed by legal and contractual obligations, but since May 2018, is also imposed by the General Data Protection Regulation

S. Gritzalis et al. (Eds.): TrustBus 2019, LNCS 11711, pp. 94–109, 2019.
https://doi.org/10.1007/978-3-030-27813-7_7

(GDPR) [5]. Personal data is considered the driving force of the societies to develop, interact, take decisions. For this reason, the protection of personal data has seen a major upheaval during the last decades, concentrating the attention of politicians, developers, public and private organisations, legislators, authorities, as well as the general public.

European Union provisioned the protection of individuals' privacy by setting the general rules for the processing of personal data with the Directive 95/46/EC [4]. The scope of the Directive was to provide data subjects with a set of rights, to state the obligations of controllers and processors when dealing with personal data and to foresee supervisory authorities and mechanisms for ensuring that the rules are applied. However, the continuous growth and evolution of technology has taken place at such a pace, that the existing legal frameworks had become obsolete, calling for an adaptation of the corresponding legislation. The GDPR that replaces the Directive 95/46/EC builds on the principles and rules of the pre-existing Directive, but it is differentiated in the volume of the enhancement of the rights of the Data Subjects. Moreover, it appoints responsibility to the data controllers and processors for the protection of personal data they keep, by bringing forth the concept of self-regulation and accountability. Finally, it increases the sanctions related to the violations of its provisions.

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. However, even if organisations need to comply with the GDPR, they lack guidelines that could help them into complying with these requirements. There are already products being developed that can be used towards the compliance with the GDPR, however, none of the current technical solutions is able to capture the current security 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 [7].

The GDPR describes the responsibility of data controllers and the data processors to *implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk* (Art. 32), without pinpointing specific methodology or techniques. We argue that the ISO 27k standard series can form a concrete baseline for businesses to build their "towards-compliance" strategy upon, dealing with topics such as risk definitions and assessment, continuous evaluation and appropriate documentation. An important aspect that any entity seeking compliance to current security/privacy standards should be aware of, is the fact that the (existing) ISO/IEC 27001:2013 (hereafter, ISO 27001) and the (newly brought) GDPR do not aggregately add burden (effort/costs) to an organisation. The similarities in both are quite many, and they both aim to cultivate a culture of protecting (processes/assets/data) and shaping the organisation's philosophy in this direction. Therefore, we argue that if an organisation already has an ISO 27001-based framework in place, compliance with the GDPR

requires limited effort, as many processes and controls should already be in place, as well as the organisation's attitude towards protecting (processes/assets/data). The aim of this paper is to identify synergies by analysing the ISO 27001 standard and the GDPR and extracting the main concepts from both texts, and propose best practices for compliance. This work (i) maps the concepts expressed by each of these documents, (ii) identifies the common guidelines that the two documents share, and (iii) provides guidelines to organisations that are already certified according to the ISO 27001, on the actions that they need to take in order to also comply with the requirements of the GDPR. Vice versa, an organisation that satisfies current legal requirements and applies best practices on the field, constitutes also a good candidate for future certification with ISO 27001 with little effort. This should act as a motivation for these organisations to consider gaining such a certification since it leads to considerable benefits, such as more efficient and time saving processing, communication of a positive message to employees and customers, to name a few.

In this way, a transition to a new, consolidated approach to personal data protection and ISMSs, can be achieved.

2 Background: Data Protection in EU

2.1 General Data Protection Regulation (EU) 2016/679

The European Commission (EC) context for personal data protection starts in 1995, with the Directive 1995/46/EC regarding the protection of natural persons against the processing of their personal data and the free movement of such data. Moreover, the Directive 2001/58/EC [1] is related with the Processing of Personal Data and Protection of Privacy in Electronic Communications. Finally, the Directive 2006/24/EC [3] is about 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 [2].

The development of new types of Information Systems (IS) (e.g., interoperable IS which require the transfer of data from one system to another, possibly from one country to another, the uploading activity of personal data, etc.), as well as their rapid growth development, demand the establishment of new ways of management of the data these IS process. Since January of 2012, EC has proposed a reform of data protection rules and principles in order to increase the level of control of users' data, and thus, reduce the cost for businesses. Proposes a reform of data protection rules in order to increase the control over (personal) user data and reduce costs for businesses. Two years later, on March 2014, EC approves the proposal for the new Regulation (first draft), while on April 2015 it approves the General Data Protection Regulation 679/2016. One month later, on May 2016, the Regulation comes into effect, with a 2-year transition period. With brought us to the infamous 25th May 2018 when the Regulation is being applied, as a directly applicable law in all the member - states of European Union.

Conclusively, the GDPR is new regulation, which brings new obligations, new rights to the world formed by Information and Communication Technologies and the globalisation of information flows and services. The GDPR's orientation is to support the security of personal data so that it can then support citizens' rights. It lays down the requirements for the protection of individuals with regard to the processing of personal data and the free movement of such data. It is mandatory for public and private organisations that manage personal data of European citizens. The aim is for citizens in the European Union to gain (more) control of their personal data.

2.2 Major Breakthroughs of GDPR

The GDPR is an attempt to change stakeholders' mentality about the uncontrolled processing of their personal data. Additionally, the use of ISs to talk to each other, to exchange data between IS owners and use them for unknown processing purposes is a major problem for democracy in an information society. Consequently, the implementation of the GDPR is not tertiary, it is of major importance for the citizens' own life; this orientation was given by the European Parliament. Major breakthroughs of the GDPR are summarised in the following list:

- **Definition of Personal Data**.
  Additionally to the definition of personal data presented in the Directive 95/46/EC, which mentions that it is any information relating to an identified or identifiable natural person, the GDPR has added *location data*, *an online identifier*, as well as factors specific to the *genetic identity* of a natural person, besides physical, physiological, mental, economic, cultural or social identity, already included in Directive 95/46/EC.
- **Definition of Special Categories of Personal Data**. In special categories of personal data, GDPR includes the processing of *genetic data* and *biometric data for the purpose of uniquely identifying a natural person*, apart from personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation, already included in Directive 95/46/EC.
- **Data Controller's responsibilities:** The GDPR describes precisely the term of the data controller, its roles and responsibilities. Compared with the Directive 95/46/EC, the data controller shall now *implement appropriate technical and organisational measures* to ensure and to be able to demonstrate that processing is performed 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*.
- **Jurisdiction:** This point presents another dimension in the territorial scope of the application of the Regulation, since it applies, now, to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, *regardless of whether the*

processing takes place in the Union or not. This requirement relates with processing regarding *the offering of goods or services, or the monitoring of their behaviour as far as their behaviour takes place within the Union.*

- **Consent Management:** The way that data subject's consent is given to anyone who wants to process their data changes, by meaning that the consent should be *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.* In this way, the data subjects are given the opportunity/ability to gain control over the management of their data, and the controllers can manage the provided consent as a proof for their legal processing.
- **Breach notification:** In the Directive 95/46/EC, there wasn't any reference regarding the notification of the supervisory authorities when a data breach occurs. The GDPR describes this process as an obligation assigned to the data controller, highlighting the short time period that they should react, by informing the supervisory authorities *without undue delay and, where feasible, not later than 72 h after having become aware of it.* Reference is also made to the notification of data subjects, if there is a risk for their rights and freedoms.

In the context of the new legislation, with which many non EU based organisations need to comply, when they process EU citizens data, data protection entails new and increased security requirements. However, this new regulation is not to be taken as a new set of laws, guidelines and obligations; there already exists an internationally known and well-established framework that can stand as a baseline for conforming to information security requirements in general; with necessary extensions this could also assist in accommodating data protection requirements.

3 ISO/IEC 27001:2013

ISO 27001 [8] is part of ISO27k standards which provide recommendations on good practices for information security management, risk management and taking security measures, within the context of an Information Security Management System (ISMS). ISO27k standards provide details (e.g., ISO/IEC 27005 about the information security risk management and ISO/IEC 27018 for the protection of personally identifiable information in public clouds), while other ISO and non-ISO standards and resources provide much more information and, in some cases, propose alternative or complementary approaches and controls. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organisation's overall business risks. The objective of the standard is to thoroughly describe an ISMS, to provide definitions on the fundamental terms of information security, and for terms that are referenced in the family of ISO 27k. This standard is addressed to all types of organisations and businesses of any business sector, size, and activities.

The standard consists of two main sections, the main body of the document and the Annex A'. The main body of the document consists of ten sections/clauses. Clauses 4–10 describe the ISMS, while Annex A' presents the

security modules, control objectives and controls that an ISMS shall cover at minimum. The structure of security controls includes 14 modules that expand in 35 security objectives and 114 security controls to achieve the objectives. An organisation must deal with all the security controls in the Annex, except the non-applicable ones. In this case, the exceptions are recorded in a Statement of Applicability. Each certificate states the Statement of Applicability: That is, which of the controls of Annex A' includes and which it excludes.

4 From an ISMS to GDRP Compliance

The GDPR provisions numerous personal data protection settings and controls, many of which are also recommended in ISO/IEC 27001:2013, ISO/IEC 27002: 2013, 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. 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.

In this section we analyse the ISMS framework of ISO 27001 and identify synergies with the GDPR compliance efforts. In the next section we analyse the fourteen control modules of Annex A' of ISO 27001 and we then describe the necessary additional actions that an organisation is required to implement, in relation to the aforementioned controls, towards GPDR compliance. Finally, we provide suggestions to the organisations that are already certified according to the ISO 27001, on the following actions they have to conduct to also comply with the requirements of the GDPR.

4.1 Analysis: Extending the ISMS Towards GDPR Compliance

The compliance of an organisation with the GDPR can be seen as a project that follows the fundamental steps of the Deming Plan-Do-Check-Act (PDCA) cycle [11]. PDCA is an iterative four-step management method used in business for the control and continual improvement of processes and products. Although ISO 27001 in version 2013 extends in more steps, in fact, in a general perspective it is based in the PDCA cycle, as all management standards. In the project of GDPR compliance, each of these steps includes the following actions that should be conducted:

- **Plan:** In this first step we set the objectives of the project, and we identify the corresponding employees that will be involved in the process. Practically, in this step we have the initiation of the project, which is supported by the whole organisation and has the commitment of the management. Additionally, we define the organisational structure for managing data protection (i.e.

nominating a DPO, distinguishing roles related with the security of IS and data protection). Also, this step contains the identification of personal data the organisation keeps, and the classification of them. This process will facilitate the risk assessment (GDPR, Recital 76) with respect to personal data as well as the conduction of a Data Protection Impact Assessment (DPIA), if it is necessary.

- **Do:** This step allows the plan set up in the previous step to be carried out. It includes the design of the necessary controls and procedures as well as their implementation. The documentation of key processes and security controls is also included in this step. Documentation facilitates the management of the aforementioned processes and controls, and it varies depending the type, the size and the complexity of the organisation, their IS any other technologies available, as well as the requirements of the stakeholders and the relevant third parties (customers, suppliers). Furthermore, this step contains the establishment of a communication plan, as well as the set up of awareness and training sessions for the employees of the organisation.
- **Check:** This step consists of two concrete actions. The first action contains the monitoring, measurement, analysis and evaluation of the process. In order to be sure that the suggested controls, set up in the second step, are implemented efficiently, the organisation shall determine the controls that need to be measured and monitored, focusing on the activities that are linked to the organisation's critical processes. The second action refers to the internal audit that the organisation shall conduct. The objectives of the audit should be focused on the evaluation of the actions related with the GDPR requirements been implemented in the organisation.
- **Act:** The final step of the process aims at maintaining the results of the project and identification of corrective action processes as well as the continuous improvement of the established framework. The corrective actions procedure is realised through the following steps: (i) identification of the nonconformity and analysis of its impacts on the organisation; (ii) analysis of the situation, i.e. analysis of the root causes, assessment of the available options, selection of the most appropriate solution(s); (iii) corrective actions, by implementing the chosen solutions and recording the actions taken; (iv) continuous improvement, by evaluating and reviewing the actions taken.

The certification of an organisation to the ISO 27001 facilitates its compliance with the GDPR since the requirements of the latter can be compared with an already established control framework, as the one of the ISMS.

5 A Consolidated Compliance Framework: Extending Control Objectives and Controls to Achieve GDPR Compliance

ISO 27001 facilitates compliance with the GDPR because its requirements may be compared with an operational and already established control framework,

such as the ISMS. Hereafter, we present the necessary controls and processes that should be implemented in order for the organisations to be compliant with the GDPR. The proposed list of those items is not exhaustive, since additional controls or processes might be required, depending on the nature and particularities of each organisation.

The following guidelines are based on the analysis of the 14 modules of the ISO 27001, where the implementation/satisfaction of them describes the ISMS. Each paragraph describes the obligations that ISO imposes to organisations, and compared to them, we propose the additional actions that the organisation has to conduct towards GDPR compliance.

5.1 Enhancing Information Security Policies with Data Protection Policies

The first control module includes one control related with the management direction for information security. The objective is the provision of management direction and support for information security in accordance with business requirements, and relevant laws and regulations.

Complying with GDPR: Since the organisation has already developed an information security policy, the requirement towards GDPR compliance for the data controller is the development and establishment of a data protection policy. This policy should meet in particular the principles of data protection by design and data protection by default [6,10]. More specifically, this policy should be distinct from the information security policy [9], providing information on:

- The lawfulness of processing (which requires legal analysis).
- The time frame that the processing/storage of personal data will take place.
- The existence of any automated decision-making process, including profiling, with information on possible consequences.
- Data collected from other sources.
- The Data Protection Officer's data.
- The procedures employed in order to satisfy all data subjects' rights.

The Data Protection Policy applies to all personal data processed by the organisation, to all operational processes that involve the processing of personal data, and to all members of the organisation who are directly or indirectly involved in the processing of personal data. It is not a static document but should be kept as up to date as possible and adjusted in line with the changes of IS and the technical and social environment. It is also updated in the event of major changes to the organisation or its IT systems.

5.2 Extending Organisation of Information Security

This control module includes two controls, (i) the internal organisation, and (ii) the mobile devices and teleworking. This control module aims at the establishment of a framework for the administration on the implementation and operation

of security within the organisation, and the protection of security related with the information accessed, processed and/or stored at teleworking sites, and the use of portable devices.

Complying with GDPR: The requirements towards GDPR compliance include, firstly, specific management of personal data that the organisation keeps. More specifically, the personal data should be (Art. 5):

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- 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.
- Processed in a manner that ensures appropriate security of the personal data.

Next, the data controllers need to cooperate with the supervisory authorities when a data breach occurs (Art. 33), informing them without undue delay, when the personal data breach is likely to result in a risk to the rights and freedoms of 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.

Additionally, the data controller needs to conduct a DPIA when particular types of processing is likely to result in a high risk to the rights and freedoms of natural persons (Art. 35). The data controller carries out DPIA in case of (i) systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, (ii) processing on a large scale of special categories of data, (iii) systematic monitoring of a publicly accessible area on a large scale.

Furthermore, a data protection officer should be appointed, since (i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity, (ii) the data controller's main activities require regular and systematic monitoring of the data subjects on a large scale, the data controller's main activities are large scale processing of specific categories of personal data.

Finally, an organisation can proceed to the establishment of codes of conducts (Art. 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 (Art. 42). Such mechanisms may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors. They enable the mandatory monitoring of compliance either by the supervisory authority, or by

an accredited organisation (demonstrating independence and expertise). 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.

5.3 Expanding Controls on Human Resources Security to Employees' Privacy Protection

This control module consists of three of controls: (i) information security prior to employment; (ii) during employment, and (iii) termination and change of employment. The corresponding objectives of these controls are to ensure that the employees and contractors understand their responsibilities and are suitable for the roles which they are appointed; that they are aware of and fulfil their information security responsibilities; to protect the organisation's interests as part of the process of changing or terminating employment.

Complying with GDPR: Additionally to the above that mainly deal with the security of the organisation related with their employees, GDPR sets a series of actions related with the protection of data of an organisation's employees. Starting with the management of the personal data that the organisation keeps, they have to apply special restrictions to personal data concerning criminal convictions and offences (Art. 10). Moreover, data controllers have to maintain relevant documentation related with data protection, i.e. records of processing activities (Art. 30), by maintaining a list of classified corporate information - including personal data, and documentation of applied technical and organisational measures the organisation applies.

5.4 Enhancing Asset Management with Personal Data Management

This control module contains three controls: (i) responsibility for assets; (ii) information classification; and (iii) media handling. The objective for the first control is the identification of the organisational assets, and the definition of appropriate protection responsibilities. Regarding the information classification, the organisation need to ensure that information receives appropriate level of protection in accordance with its importance, and finally for the media handling control, the organisation is responsible for preventing unauthorised disclosure, modification, removal or destruction of information stored on media.

Complying with GDPR: It is clear that this control provides guidelines for the protection of any valuable for the organisation asset. Taking into account that personal data and special categories of personal data also consist a valuable asset, the organisation needs to know all location where this data is kept (Art. 5, 7, 9, 30), and under which lawful process this data has been obtained (this point is also related with the consent that the organisation should obtain by the data subject). Additionally, the data controller/processor should be in position to provide information to the data subject related to the aforementioned personal data they keep (Art. 13, 14) by developing appropriate procedures for the satisfaction of this right.

5.5 Establishing Access Control Designed Following Data Protection by Design and by Default Principles

Access control contains four controls: (i) business requirements of access control; (ii) user access management; (iii) user responsibilities; and (iv) system and application access control. All these controls are related with the access management of the users to information, preventing unauthorised access to systems and services and promoting accountability for safeguarding organisation's authentication information.

Complying with GDPR: The organisation should develop their systems with respect to data protection by design and by default principles (Art. 25) in order to protect users' privacy. Additionally, the organisation should implement process through which the data subjects can either correct, or request correction (Art. 16) of the personal data the organisation holds for them, or erase, or request the erasure (Art. 17) of such data.

5.6 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.

Complying with GDPR: Encryption and anonymisation are the two technical measures that the GDPR proposes (Art. 32). Moreover, for the satisfaction of the right to data portability (Art. 20), the organisation is encouraged to apply encryption to securely communicate the corresponding personal data to other organisations.

5.7 Enhancing Communications Security with Personal Data Protection Objectives

This control module contains two controls: network security management and information transfer. The objective is to ensure the protection of information in networks and its supporting information processing facilities and to maintain the security of information transferred within an organisation and with any external entity.

Complying with GDPR: Emphasis should be given to the design and development of the communication security where more than one organisations are involved and access to personal data is required (Art. 26). Appropriate roles should be given to the corresponding employees who have access to such data, accompanied with specific responsibilities. Additionally, the organisation should be able to locate and retrieve securely the personal data it keeps, satisfying thus the right of access by the data subject (Art. 15).

5.8 Acquiring, Developing and Maintaining Systems Following Data Protection Principles

This control module contains three controls: (i) security requirements of IS, (ii) security in development and support process, and (iii) test data. The requirements of this section are referred to the development process of IS. It is worth mentioning that this is the first time that we meet requirements related to the development of a system in ISO 27001. Organisations should be able to choose their working environment (framework, language, operating system, to name a few parameters) in relation to the criticality of the product they wish to develop.

Complying with GDPR: 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 (Art. 6). This should also be covered in the risk assessment and management, in general, 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 keep. In order to avoid information risks, where feasible, the organisation needs to assess if they really need to keep personal and special categories of personal data or the aggregation of such data is also accepted (Art. 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 (Art. 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.

5.9 Managing Supplier Relationships While Protecting Personal Data

This control module contains two controls: (i) information security in supplier relationships, and (ii) supplier service delivery management. The objective is to manage the relationship of the organisation with its suppliers, or any other third party that has access to the organisation's assets, and to set up and agreed level of information security and service delivery.

Complying with GDPR: Organisations located outside Europe that interact with European organisations must formally nominate privacy representatives inside Europe if they meet certain conditions. If an organisation uses one or more third parties to process personal info ("processors"), it must ensure they too are compliant with GDPR (Art. 27, 28). Moreover, organisations need to ensure the 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.

5.10 Extending Incident Management with Notification in Case of Data Breach

This control module contains one control, i.e. management of information security incidents and improvements. The objective of this control is to ensure a consistent and effective approach to the management of information incidents.

Complying with GDPR: The organisation should implement process in order to be able to notify without undue delay the supervisory authority (Art. 33) and the data subjects (Art. 35) if it is required.

5.11 Enhancing Compliance to Satisfy Lawfulness of Processing

This control module contains two controls: (i) compliance with legal and contractual requirements, and (ii) information security reviews. This last control aims at the avoidance of any kind of breaches related to information security and of any security requirements and to ensure that the information security is implemented and operated in accordance with the organisational policies and procedures.

Complying with GDPR: Additionally, the organisation should develop processes to satisfy the lawfulness of processing (Art. 5), for the consent of the data subjects (Art. 7, 8), for the satisfaction of the rights of data subjects (Art. 12–22), for ensuring the appropriate safeguards in case of a transfer of personal data to third countries or international organisation (Art. 44).

5.12 Modules that Support GDPR Compliance

This section presents modules that have no direct application to the GDPR, but can help an organisation develop a culture that will assist towards reaching GDPR compliance; they are also included here for the sake of completeness.

Enhancing Physical and Environmental Security for GDPR Compliance: This control module contains two controls: the secure areas and the equipment. The identification of secure areas can prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities, while the safeguarding of the equipment of the organisation prevents loss, damage, theft or compromise of assets and interruption of organisation's operation.

Complying with GDPR: 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 (Art. 24, 25, 28, 32).

Enhancing Operations Security for GDPR Compliance: This control 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. The objective of this section is to ensure correct and secure operations of information processing facilities, protection against malware and data loss, to record events and generate evidence, to ensure the integrity of operational systems, to prevent exploitation of technical vulnerabilities and to minimise the impact of audit activities on operational systems.

Complying with GDPR: Similarly to the previous section of "physical and environmental security", an organisation is able to demonstrate that they have implemented they 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 (Art. 12–22) and for the process of the provision of consent of the data subjects (Art. 7).

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. The continuity of operations is indented to restore the operation of the organisation's systems within a reasonable time. In addition, staff training is required in the continuity plan, while its efficiency must be tested and managed properly.

Complying with GDPR: 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 (Art. 24, 25, 28, 32).

6 Conclusions

The application of ISO 27001 supports organisations in creating better business efficiency, safeguards valuable assets such as personal data or hardware, protects staff and organisations' reputation, and simultaneously facilitates the attainment of compliance objectives. Several GDPR requirements are not covered in ISO 27001, however ISO 27001 provides the means to push organisations one step closer to accomplish conformity to the Regulation, minimising the required effort.

Even for organisations that are not ISO 27001 certified, complying with the GDPR is a good catalyst for considering implementing such a scheme for higher information protection assurance. Already, by being ISO 27001 compliant, organisations demonstrate (and is the case) that the data owned and used is managed based on data protection regulations. Consequently, if organisations already have an ISO 27001 framework in place, compliance with GDPR requirements will not

be necessitated a duplication of 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.

The results of this work provide guidelines for practitioners, such as information security and privacy experts since it presents a roadmap on how to design a "towards GDPR compliance" project, contributing also to their awareness regarding the protection of personal data of their 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, data protection officers 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

1. Commission directive 2001/58/EC of 27 July 2001 amending for the second time directive 91/155/EEC defining and laying down the detailed arrangements for the system of specific information relating to dangerous preparations in implementation of article 14 of European parliament and council directive 1999/45/EC and relating to dangerous substances in implementation of article 27 of council directive 67/548/EEC (safety data sheets)
2. Directive 2002/58/EC of the European parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications)
3. 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
4. European commission: Directive 95/46/EC of the European parliament and of the council. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046. Accessed 14 May 2017
5. European parliament: 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)
6. Cavoukian, A., et al.: Privacy by design: the 7 foundational principles. Inf. Privacy Commissioner Ontario, Canada **5** (2009)
7. IAAP: Privacy tech vendor report. Technical report (2018)
8. ISO/IEC: ISO 27001:2013 information technology - security techniques - information security management systems - requirements. Technical report (2013)
9. Lambrinoudakis, C.: The general data protection regulation (GDPR) era: ten steps for compliance of data processors and data controllers. In: Furnell, S., Mouratidis, H., Pernul, G. (eds.) TrustBus 2018. LNCS, vol. 11033, pp. 3–8. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98385-1_1

10. Langheinrich, M.: Privacy by design—principles of privacy-aware ubiquitous systems. In: Abowd, G.D., Brumitt, B., Shafer, S. (eds.) UbiComp 2001. LNCS, vol. 2201, pp. 273–291. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45427-6_23
11. Moen, R., Norman, C.: Evolution of the PDCA cycle (2006)
12. Spiekermann, S., Acquisti, A., Böhme, R., Hui, K.L.: The challenges of personal data markets and privacy. Electron. Markets **25**(2), 161–167 (2015)