Journal of Information Systems Engineering & Management
2019, 4(2), em0089
ISSN: 2468-4376

Implementation of ISO 27001 Standards as GDPR Compliance Facilitator

Isabel Maria Lopes [1,2,3*], Teresa Guarda [3,4,5], Pedro Oliveira [1]

[1] *Polytechnic Institute of Bragança*, Bragança, PORTUGAL
[2] *UNIAG, Polytechnic Institute of Bragança*, PORTUGAL
[3] *ALGORITMI Centre, Minho University*, Guimarães, PORTUGAL
[4] *Universidad Estatal Península de Santa Elena – UPSE*, La Libertad, ECUADOR
[5] *Universidad de las Fuerzas Armadas – ESPE*, Sangolqui, Quito, ECUADOR

*__Corresponding Author:__ isalopes@ipb.pt

Citation: Lopes, I. M., Guarda, T. and Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *Journal of Information Systems Engineering & Management*, 4(2), em0089. https://doi.org/10.29333/jisem/5888

Published: August 22, 2019

ABSTRACT

Personal Data Protection has been among the most discussed topics lately and a reason for great concern among organizations. The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. The regulation will fundamentally reshape the way in which data is handled across every sector. The organizations had two years to implement it. As referred by many authors, the implementation of the regulation has not been an easy task for companies. The question we aim to answer in this study is how far the implementation of ISO 27001 standards might represent a facilitating factor to organizations for an easier compliance with the regulation. In order to answer this question, several websites (mostly of consulting companies) were analyzed, and the aspects considered as facilitating are listed in this paper.

Keywords: regulation (EU) 2016/679, general data protection regulation, ISO/IEC 27001

INTRODUCTION

In recent years, data protection has become a forefront issue in cyber security. The issues introduced by recurring organizational data breaches, social media and the Internet of Things (IoT) have raised the stakes even further (Mäkinen, 2015, Nurse, Creese, and De Roure, 2017). The EU GDPR, enforced from May 25 2018, is an attempt to address such data protection. The GDPR makes for stronger, unified data protection throughout the EU.

The EU GDPR states that organizations must adopt appropriate policies, procedures and processes to protect the personal data they hold.

The International Organization for Standardization (ISO) /International Electrotechnical Commission (IEC) 27000 series is a set of information security standards that provide best-practice recommendations for information security management (Clements and Milton, 2018).

This international standard for information security, ISO 27001, provides an excellent starting point for achieving the technical and operational requirements necessary to reduce the risk of a breach.

Not all data is protected by the GDPR, since it is only applicable to personal data. This is defined in Article 4 as follows (European Parliament and Council, Regulation (EU) 2016/679, 2016):

"personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an

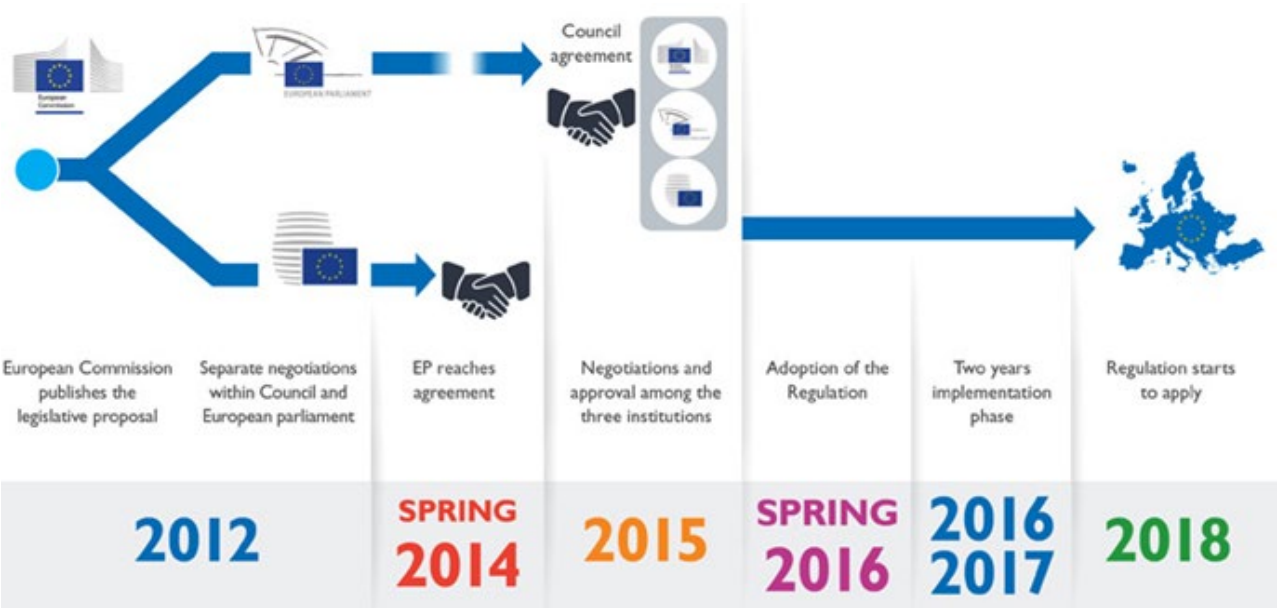

Figure 1. Stages of the GDPR (Goubau, 2018)

identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The structure of the present work consists of an introduction, followed by a desk review on the general data protection regulation and the desk review of ISO 27001, the international standard for information security. Section 4 focuses on the research methodology. Before presenting the results, the discussion is made, focusing on the relationship between ISO 27001 and GDPR. The results of the study are presented in section 6 and section 7 consists of the conclusions drawn from the study. Finally, the limitations of this research work are identified and possible future studies are proposed.

GENERAL DATA PROTECTION REGULATION

The enforcement of the GDPR on natural persons' protection regarding personal data treatment and movement, which repeals the Directive 95/46/CE of October 24 1995, poses innumerable challenges to both public and private entities as well as to all the agents whose activities involve the treatment of personal data.

Although the full application of the new GDPR has been set for May 25 2018, date from which the directive 95/46/CE was effectively repealed, its enforcement on May 25 2016 dictated the need for an adaptation to all the aspects changed or introduced by the regulation. Such adaptation of the present systems and models as well as of best practices regarding personal data treatment and protection by companies is now an imperative stemming from the regulation in order to safeguard its full applicability. In **Figure 1**, we can see all the stages which the GDPR has undergone.

The GDPR mandates a baseline set of standards for companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data.

According to author (Díaz, 2016), the main innovations of the General Data Protection Regulation are:

1. New rights for citizens: the right to be forgotten and the right to a user's data portability from one electronic system to another.
2. The creation of the post of Data Protection Officer (DPO).
3. Obligation to carry out Risk Analyses and Impact Assessments to determine compliance with the regulation.
4. Obligation of the Data Controller and Data Processor to document the processing operations.
5. New notifications to the Supervisory Authority: security breaches and prior authorization for certain kinds of processing.
6. New obligations to inform the data subject by means of a system of icons that are harmonized across all the countries of the EU.
7. An increase in the size of sanctions.
8. Application of the concept 'One-stop-shop' so that data subjects can carry out procedures even though this affects authorities in other member states.
9. Establishment of obligations for new special categories of data.
10. New principles in the obligations over data: transparency and minimization of data.

All organizations, including small to medium-sized companies and large enterprises, must be aware of all the GDPR requirements and be prepared to comply.

ISO/IEC 27001

Information security risks threaten the ability of organizations to reach their operational and strategic goals. Increasing diversification of the information security landscapes makes addressing all risks a challenging task. Information security standards have positioned themselves as generic solutions to tackle a broad range of risks and try to guide security managers in their endeavors (Milicevic and Goeken, 2010).

The ISO 27001 standard represents the international framework for information security management.

The ISO 27001 standard has undergone continuous improvements over the years and stems from a previous set of standards, namely BS7799-2 and the BS7799 (British Standards). In fact, its primary origin is a document published in 1992 by a department of the British government which established a code of practices regarding the management of Information Security.

The adoption of ISO 27001 results in the companies' adoption of an adequate model to establish, implement, operate, monitor, revise and manage an Information Security Management System.

ISO 27001:2013 is part of the management system in an organization based on a business risk approach that purposed to build, implement, operate, observe, maintain and improve information security. The application of ISO/IEC 27001 allows the organization or company to compare the competition and give relevant information about IT security (Bilbao, Bilbao and Pecina, 2011).

ISO 27001 outlines three essential aspects or 'pillars' of effective information security: people, processes and technology. This three-pronged approach helps organizations defend themselves from both highly organized attacks and common internal threats, such as accidental breaches and human error (Irwin, 2018).

The implementation of an information security management system according to ISO/IEC 27001 has the following advantages to organizations:

- It enables the identification and elimination of threats and vulnerabilities;
- It provides security and trust to all stakeholders (clients, partners and others);
- It improves security awareness;
- It increases the capacity to foresee, manage and survive a disaster;
- It deepens the knowledge regarding the organization and its processes, assets and liabilities;
- It provides real knowledge of the risk that the organization faces;
- It ensures business continuity;
- It contributes to a reduction in costs and to the improvement of the processes and services;
- It ensures compliance with the legislation in force;
- It reduces costs associated with 'non security'.

ISO 27001: 2013 provides specifications for information security management systems along with practice (Calder and Watkins, 2008).

ISO 27001: 2013 has 14 security control clauses that contain a total of 35 control objectives and 114 controls (ISO 27001:2013). The 14 security control clauses are as follows:

- Information security policies,
- Organization of information security,
- Human resource security,
- Asset management,
- Access control,
- Cryptography,
- Physical and environmental security,
- Operations security,
- Communications security,
- System acquisition, development, and maintenance,
- Supplier relationships,
- Information security incident management,
- Information security aspects of business continuity management,
- Compliance.

The implementation of ISO 27001 implies a high commitment to information protection, which represents a considerable level of comfort for the organizations that interact with the certified entity.

RESEARCH METHODOLOGY

The use of a research method is paramount since it represents the means to an end. A research methodology does not look for solutions but chooses the way to find them, integrating knowledge through the methods which are applicable to the various scientific or philosophical subjects. Although there are several ways to classify them, research approaches are normally distinguished between quantitative and qualitative (Myers, 1997).

It is acknowledged that the choice of the method must be made according to the nature of the problem being addressed. Therefore, we considered it appropriate to follow a quantitative research method (traditional scientific research), based on the positivist rational thought according to which, through empirical observations, we build theories (expressed in a deductive way) that try to explain what is observed. Among the possible research methods to use, we applied the content analysis.

Content analysis is a method which differs from the other research methods because instead of interviewing or observing people, the researcher deals with pre-existing records and interferes based on those records.

Content analysis is a research technique for the objective, systematic, and quantitative description of manifest content of communications. So that this description can be objective, it requires a precise definition of the analysis categories, in order to enable different researchers to use them and get the same results. So that it is systematic, the whole relevant content must be analyzed in relation to all the meaningful categories. Finally, quantification allows the provision of more precise and objective information concerning the occurrence frequency of content features (Berelson, 1952).

DISCUSSION

The similarities between the ISO 27001 framework and the GDPR requirements mean that organizations which certify to the Standard are already halfway to GDPR compliance.

Its requirements (ISO 27001) are similar in many places to the GDPR, but whereas the Regulation only occasionally suggests specific practices (such as encryption), ISO 27001 clearly lays out what organizations need to do in order to remain secure (Irwin, 2018).

Article 42 of the GDPR details demonstrating compliance with the regulation through; "data protection certification processes". ISO 27001 compliant Information Security Management Systems follow a risk based approach addressing specific security threats faced by organizations considering people, processes and technology (NQA, 2019).

How ISO 27001 can help meet GDPR requirements (Dattani, 2019):

1 – Assurance: The GDPR recommends the use of certification schemes such as ISO 27001 as a way of providing the necessary assurance that the organization is effectively managing its information security risks.

2 - Not just personal data: ISO 27001 follows international best practices and will help companies put processes in place that protect not only customer information but also all the information assets, including information that is stored electronically and in hard copy format.

3 - Controls and security framework: The GDPR stipulates that organizations should select appropriate technical and organizational controls to mitigate the identified risks. The majority of the GDPR data protection arrangements and controls are also recommended by ISO 27001

4 - People, Processes and technology: ISO 27001 encompasses the three essential aspects of information security: people, processes and technology, which means companies can protect their business not only from technology - based risks but also other and more common threats, such as poorly informed staff or ineffective procedures.

5 – Accountability: ISO 27001 requires companies' security regime to be supported by top leadership and incorporated into the organization´s culture and strategy. It also requires the appointment of a senior individual who takes accountability for the ISMS. The GDPR mandates clear accountability for data protection across the organization.

6 - Risk assessments: ISO 27001 compliance means conducting regular risk assessments to identify threats and vulnerabilities that can affect organizations' information assets, and to take steps to protect that data. The GDPR specifically requires a risk assessment to ensure that an organization has identified risks that can impact personal data.

7 - Continual improvement: ISO 27001 requires that the companies' ISMS is constantly monitored, updated and reviewed, meaning that it evolves as their business evolves using a process of continual improvement. This means that the ISMS will adapt to changes - both internal and external - as companies continually identify and reduce risks.

8 - Testing and audits: Being GDPR - compliant means that an organization needs to carry out regular testing and audits to prove that its security regime is working effectively. An ISO 27001 - compliant ISMS needs to be regularly assessed according to the internal audit guidelines provided by the standard.

9 – Certification: The GDPR requires organizations to take the necessary steps to ensure the security controls work as designed. Achieving accredited certification to ISO 27001 delivers an independent, expert assessment of whether organizations have implemented adequate measures to protect their data.

The link between ISO/IEC 27001 and GDPR is (Middleton-Leal, 2019):

ISO/IEC 27001 and GDPR at their core have in common the commitment to properly process and store the sensitive and confidential data. Therefore, the implementation of the ISO/IEC 27001 comprehensive framework steers compliance with the EU GDPR, as many of the EU GDPR requirements are covered by ISO/IEC 27001. However, particular controls have to be adjusted to address the protection of personal data within the Information Security Management System.

If organizations already have an ISO/IEC 27001 framework in place, they will not face duplication of effort, cost and time to comply with the GDPR requirements.

The ISO/IEC 27001 certification supports organizations in creating better business efficiency, safeguards the valuable assets such as personal data, protects staff and organizations' reputation, and simultaneously facilitates the attainment of compliance objectives. Some of the GDPR requirements are not directly covered in ISO/IEC 27001; however, ISO/IEC 27001 provides the means to push companies one step closer to accomplishing conformity to the regulation.

In case that an organization is not ISO/IEC 27001 certified, then the GDPR may be a good catalyst in considering implementing such scheme for higher information protection assurance. Thus, by being ISO/IEC 27001 compliant, companies demonstrate that the data owned and used is managed based on data protection regulations.

Does compliance with ISO 27001 guarantee GDPR compliance (PECB, 2019)?

Certification with ISO 27001 can simplify the process of achieving GDPR compliance. However, there are several differences between these standards. The GDPR is a global standard that provides a strategic vision of how organizations need to ensure data privacy. ISO 27001 is a set of best practices with a narrow focus on information security; it provides practical advice on how to protect information and reduce cyber threats. Unlike the GDPR, it does not directly cover the following issues associated with data privacy, which are outlined in Chapter 3 of the GDPR (Data Subject Rights):

- Consent,
- Data portability,
- The right to be forgotten,
- The right to restriction of processing,
- Right to object,
- International transfers of personal data.

As we can see, the GDPR focuses on data privacy and the protection of personal information; it requires organizations to put more effort into obtaining explicit consent for data collection and ensuring that all data is processed lawfully. However, it lacks technical details on how to maintain an appropriate level of data security or mitigate internal and external threats. In this regard, ISO 27001 comes in handy: It provides practical guidance on how to develop clear, comprehensive policies to minimize security risks that might lead to security incidents.

Although conforming to ISO 27001 does not guarantee GDPR compliance, it is a valuable step. Organizations should consider pursuing ISO 27001 certification to ensure that their security measures are strong enough to protect sensitive data.

RESULTS

According to the GDPR, personal data is critical information that all organizations need to protect (Dattani, 2019; Díaz, 2018; NQA, 2019). Therefore, we analyzed the content of the 15 websites, and after the above discussion, we will summarily present some aspects which we believe deserve to be highlighted when assessing whether the implementation of ISO 27001 might be a facilitating factor for organizations to comply with the GDPR.

After analyzing the websites with regard to the following statement: if the implementation of ISO 27001 identifies personal data as an information security asset, we found that in 9 (60%) sites there is information agreeing with this statement and in the other 6 (40%), there is no mention whatsoever to this respect (see **Figure 2**).

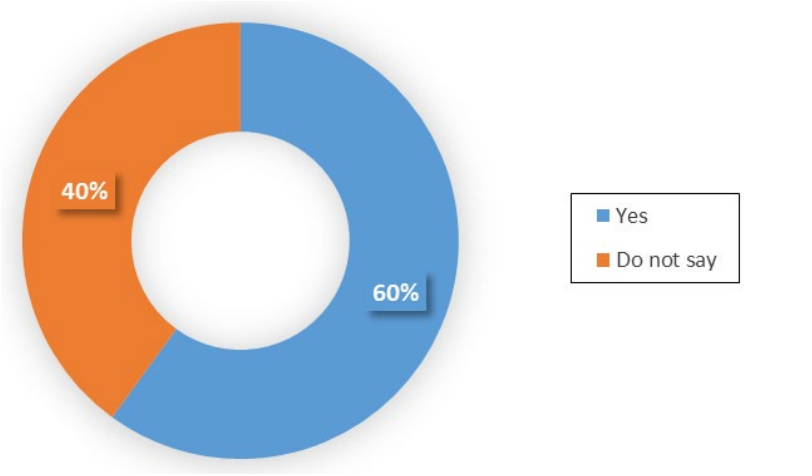

Figure 2. GDPR compliance

Figure 3. How to be in compliance

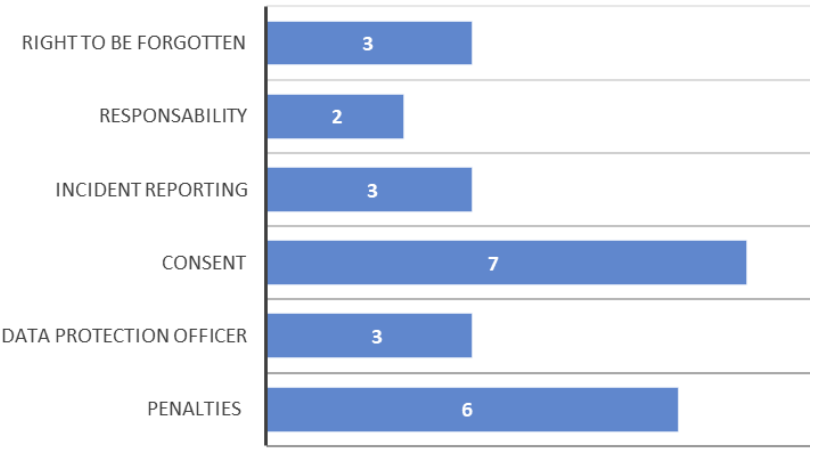

Figure 4. Aspects highly focused in the RGPD

Considering the aspects highlighted in the previous section for being in compliance with the GDPR through the ISO 27001 implementation, we can see in **Figure 3** the ones which were more or less focused in the websites under analysis.

From the **Figure 3**, three aspects stand out as deserving most attention: People, Processes and technology, which takes security beyond the people only, Certification, which proves that the measures were implemented in that organization, and Controls and security framework, which are paramount in any organization.

When analyzing the aspect which are highly detailed in the GDPR but barely focused in ISO 27001, we found the data presented in **Figure 4**.

The aspects which stand out are those concerning consent and penalties. Data controllers have to prove that data subjects have agreed to the processing of their personal data (Articles 7 and 8). The request for consent must

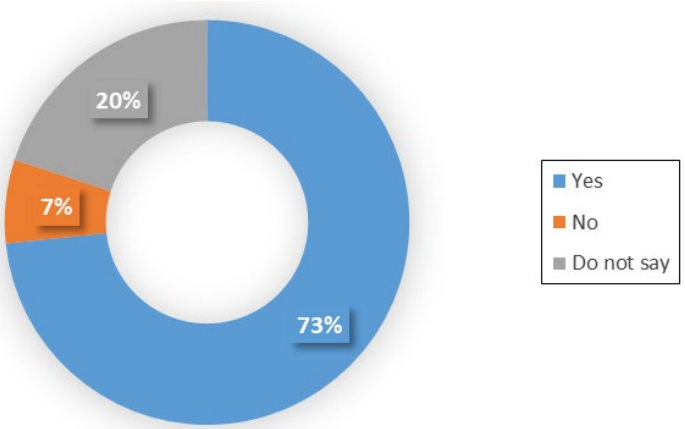

Figure 5. ISO 27001 is an excellent framework for compliance with GDPR

be given in an easily accessible form, with the purpose for data processing attached. Data subjects also have the right to withdraw their consent at any time.

The GDPR establishes a sanction application framework which is quite heavy on companies which do not comply with the new data protection legislation requirements.

Lastly, is The ISO 27001 standard an excellent framework for compliance with the EU GDPR? The results regarding this aspect are presented in **Figure 5**.

As we can see, 11 sites (73%) agree that the ISO 27001 standard is an excellent framework for compliance with the EU GDPR, 3 (20%) do not mention this aspect, and only 1 (7%) of the websites analyzed shows to be in disagreement.

From these findings, we can conclude that it is consensual that although ISO 27001 does not comprise certain important controls, its implementation is considered to be a facilitating factor for organizations to be in compliance with the new personal data regulation.

CONCLUSION

The implementation of the GDPR by organizations should be seen in the context of achieving their business goals. There is a clear need to emphasize its benefits for organizations and the values adding to business. It is absolutely wrong to understand the GDPR as another restriction to the operating environment. The GDPR is a tool for generating a strategic advantage based on trust between the organization, its employees, clients and partners (Tzolov, 2018).

The GDPR encourages the use of certifications such as ISO 27001 in order to show that the organization is actively managing its data security according to international best practices.

Our findings allow concluding that any organization that has already implemented or is in the process of implementing ISO/IEC 27001 is in an excellent position to show compliance with the new GDPR requirements.

The new regulation of data protection introduces a set of rules, which require organizations to implement controls. The implementation of ISO 27001 will help organizations respond to these requirements.

As a possible future work, we suggest assessing organizations by means of a survey on how far the certification of the information security management system by ISO 27001 grants companies' compliance with the GDPR, since the implementation of an information security management system by a company must ensure that all the relevant controls of risk containment associated with confidentiality, integrity and availability are implemented and kept functional (Lopes, Guarda and Oliveita, 2019).

SITES STUDIED

http://vexillum.pt/como-iso-27001-pode-ajudar-alcancar-conformidade-rgpd/
https://www.itgovernance.co.uk/gdpr-and-iso-27001
https://www.nqa.com/en-gb/certification/standards/iso-27001
https://www.itgovernance.co.uk/blog/how-iso-27001-can-help-you-achieve-gdpr-compliance
https://www.nqa.com/certification/standards/iso-27001/gdpr-and-iso-27001
https://www.slideshare.net/IleshDattani/gdpr-and-iso-27001-how-to-be-compliant
https://www.27001.pt/iso27001_5.html
https://koolitus.ee/images/sisu_pildid/ISO_GDPR_link.pdf

https://iso9001mgtsystem.files.wordpress.com/2017/02/how_iso_27001_can_help_eu_gdpr_compliance_en-1.pdf
https://blogs.manageengine.com/it-security/2018/01/15/how-iso-27001-helps-you-comply-with-the-gdpr.html
https://blog.netwrix.com/2018/04/26/gdpr-and-iso-27001-mapping-is-iso-27001-enough-for-gdpr-compliance/
https://www.privacycompliancehub.com/gdpr-resources/does-being-certified-in-iso-27001-really-ensure-that-you-are-gdpr-compliant/
https://www.differentia.consulting/article/iso-27001-and-gdpr/?cli_action=1548614370.003
http://iso27001guide.com/annex-a/compliance/compliance-with-legal-and-contractual-requirements/iso-27001-and-gdpr/
https://ins2outs.com/implement-information-security-management-system/

REFERENCES

Berelson, B. (1952). *Content Analysis in Communications Research*. New York: Free Press.

Bilbao, E., Bilbao, A. and Pecina, K. (2011). *Physical Logical Security Risk Analysis Model*. IEEE, pp. 1-7.

Calder, A. and Watkins, S. (2008). IT Governance.

Clements, T. and Milton, S. (2018). *Maintaining Data Protection and Privacy Beyond GDPR Implementation, ISACA*.

Dattani, L. GDPR and ISO 27001 - how to be compliant. Available at: https://www.slideshare.net/IleshDattani/gdpr-and-iso-27001-how-to-be-compliant (Accessed: 25 January 2019).

Díaz, E. D. (2016). The new European Union General Regulation on Data Protection and the legal consequences for institutions. *Church, Communication and Culture, 1*, 206-239. https://doi.org/10.1080/23753234.2016.1240912

European Parliament and Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Official Journal of the European Union.

Goubau, T. (2018). *How GDPR Will Change Personal Data Control and Personal Data Control an Affect Everyone in Construction*. Available at: https://www.aproplan.com/blog/construction-news/gdpr-changes-personal-data-control-construction (Accessed: 20 July 2018).

Irwin, L. (2018). *How ISO 27001 can help you achive GDPR compliance*, IT Governance.

ISO 27001:2013, International Standard ISO / IEC Information technology — Security techniques — Information security management systems — Requirements, vol. 2013, 2013.

Lopes, I., Guarda, T. and Oliveita, P. (2019). How ISO 27001 can help achieve GDPR compliance. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1-6, IEEE. https://doi.org/10.23919/CISTI.2019.8760937

Mäkinen, J. (2015). Data quality, sensitive data and joint controller ship as examples of grey areas in the existing data protection framework for the Internet of Things. *Information & Communications Technology Law, 24*(3), 262–277. https://doi.org/10.1080/13600834.2015.1091128

Middleton-Leal, M. GDPR and ISO 27001 Mapping: Is ISO 27001 Enough for GDPR Compliance?, netwrix. Available at: https://blog.netwrix.com/2018/04/26/gdpr-and-iso-27001-mapping-is-iso-27001-enough-for-gdpr-compliance/ (Accessed: 27 January 2019).

Milicevic, D. and Goeken, M. (2010). Ontology-Based Evaluation of ISO 27001. In: Cellary W., Estevez E. (eds) Software Services for e-World. I3E 2010. *IFIP Advances in Information and Communication Technology, 341*, Springer. https://doi.org/10.1007/978-3-642-16283-1_13

Myers, M. D. (1997). *Qualitative Research in Information Systems ACM Computing Surveys (CSUR)*, MISQ Discovery.

NQA, GDPR and ISO 27001 - how do they map? Available at: https://www.nqa.com/certification/standards/iso-27001/gdpr-and-iso-27001 (Accessed: 18 January 2019)

Nurse, J. R. C., Creese, S. and De Roure, D. (2017). Security risk assessment in Internet of Things systems. *IEEE IT Professional, 19*(5), 20–26. https://doi.org/10.1109/MITP.2017.3680959

PECB, The link between ISO/IEC 27001 and GDPR. Available at: https://koolitus.ee/images/sisu_pildid/ISO_GDPR_link.pdf (Accessed: 26 January 2019).

Tzolov, T. (2018). One Model for Implementation GDPR Based On ISO Standards. *International Conference on Information Technologies (InfoTech-2018)*, pp. 1-3. https://doi.org/10.1109/InfoTech.2018.8510716