

Adoption of the Rules of the General Data Protection Regulation on the Websites of Municipalities

Pascoal Padrão[1], A. J. G. Fernandes[1,2], and Isabel Lopes[1,3,4(✉)]

[1] Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
{toze,isalopes}@ipb.pt

[2] Centro de Investigação de Montanha (CIMO), Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal

[3] UNIAG, Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal

[4] Algoritmi, Universidade do Minho, Largo do Paço, 4704-553 Braga, Portugal

Abstract. With the advent of technologies, the amount of information processed by these means has increased dramatically. In this sense, the protection of personal data has become urgent to guarantee people's freedom of thought and to avoid possible abuses in terms of invasion of privacy and preservation of personal information. Thus, the European Union created a Regulation, in 2016, with the aim of standardizing legislation and practices with regard to data protection, in order to protect its citizens and increase transparency in the processing of their data, the same is called the "General Regulation on Data Protection" (GDPR). After 7 years since its creation and five since its entry into force and since the GDPR also affects websites, we intend with this study to verify if the websites of some Portuguese municipalities (belonging to CIM-TTM, CIM-AT and CIM Douro) include the necessary dynamics to comply with the rules dictated by the regulation.

Keywords: General Regulation on Data Protection · Municipalities · Data Protection Officer · Information systems · Safety

1 Introduction

The technological evolution of the beginning of the century and globalization promoted a transverse revolution in our society and led us to new challenges in terms of personal data protection, imposing a solid and more coherent protection framework in the European Union (EU).

The need for the EU to create a more solid framework in terms of data protection was undoubtedly due to the great technological evolution that led to more and more information being stored digitally, but also to standardize the various existing regulations

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14108, pp. 166–176, 2023.
https://doi.org/10.1007/978-3-031-37117-2_13

and standards in a more robust and unique framework that all EU Member States must abide by through its implementation.

As a result of these findings, the EU created Regulation (EU) 2016/679, with the aim of updating legislation on data protection, aligning it with the new digital age, in addition, it also intended to harmonize legislation in all States EU Members, reinforce the rights of citizens, protecting them from risks and threats in the use of their personal data.

This EU legal imperative in terms of time should have been implemented 5 years ago. Thus, it is imperative to know in this research work, not the state of its implementation in general, but rather, to verify if the Websites include the necessary dynamics mentioned in the regulation.

This regulation applies to all organizations based in the EU. Companies and public entities are required to prove compliance with all requirements arising from the application of this Regulation. Thus, in this study and since Municipalities deal daily with a lot of information from their residents, we find it pertinent to know if the content of their Websites is adjusted to the directives that the GDPR imposes.

The municipalities under study are Portuguese and as the intention is to analyze the Websites of the 308 existing municipalities, the focus of this work will focus on a part of the Portuguese territory located in the north interior, covered by the Municipalities belonging to three Intermunicipal Communities (CIM). In other works, other territories will be covered until the total analysis of the 308 existing Municipalities.

The Intermunicipal Communities are an association of Municipalities, within the Portuguese legal framework, through the creation of a superior local entity, to which the associated Municipalities delegate part of the functions or powers conferred upon them by law, with the aim of providing services to all its members. According to Law No. 75/2013 of September 12, there are currently 23 intermunicipal entities. This study focuses on three:

- Intermunicipal Community of Terras de Trás-os-Montes (CIM-TTM)
- Intermunicipal Community of Alto Tâmega and Barroso (CIM-AT)
- Douro Intermunicipal Community (CIM-Douro)

The structure of this research work begins with this introduction, followed by a brief review of the literature on the general data protection regulation. The methodology used for this research work follows, a methodology that takes us to the point of the results of this study. Finally, the conclusions are briefly presented, as well as the verified limitations and future works are identified.

2 General Regulation on Data Protection

Regulation (EU) 2016/679 (2016), published on April 27, 2016, more commonly known as the General Data Protection Regulation, which puts into effect the new regulations relating to the protection of natural persons, with regard to the processing of personal data and the free movement of such data, thus revoking the previous Directive 95/46/EC, which had as its fundamental objectives to ensure compliance with legislation in all Member States, as well as to allow citizens and business structures to benefit from the

digital economy and e-commerce, reforming the way organizations work with personal data, and above all, protecting the personal data of European citizens, since the GDPR creates new duties for the business and public sector.

The GDPR is a legal framework that provides guidelines for collecting and processing personal information from individuals [1]. GDPR seeks to clarify data protection issues for personal data collected and processed in the EU [2]. Personal data is any information that relates to an individual who can be directly or indirectly identified. Names, email addresses, location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data [3].

In this way, having unified and up-to-date legislation with regard to data protection is essential to safeguard the fundamental right to data protection, as well as to enable the growth of a consolidated digital economy and strengthen the fight against crime and terrorism. The GDPR is generally regarded as the most strict privacy policy released and enforced to date [4, 5].

The GDPR was ratified in 2016 by the European Union and entered into force only in May 2018, directly applicable in all Member States [6, 7].

The same applies to all entities that work with personal data, of natural persons, and the same entities that process personal data must analyse, without exception, the rules provided for therein.

However, it should be noted that the GDPR, despite being a European diploma, is not governed by the correction and penalty of companies that process data worldwide, since the GDPR takes as a paradigm the technology available today for processing personal data and, therefore, aims to reconcile the use of technological solutions in their current and future state of development, and the risks they entail, with the defense of the rights and freedoms of persons whose data are processed [8].

The strictest rules presented by it translate into:

1. there is greater control, by people, over their personal data;
2. there is equal competition from which companies benefit.

The main innovations of the General Data Protection Regulation are [9]:

1. “New rights for citizens.
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 authorisation for certain kinds of processing.
6. New obligations to inform the data subject by means of a system of icons that are harmonised 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 minimisation of data".

Key steps organizations need to take to get their Websites GDPR compliant [10].

1. Improve Your Privacy Policy
2. Create a Cookie Collection Notice
3. Display Notices on All Website Forms
4. Make Sure All Plugins Are GDPR Compliant
5. Use the Double Opt-in
6. Add Unsubscribe Links
7. Delete Personal Data on Request
8. Don't Buy Mailing Lists

The General Data Protection Regulation is thus the most recent and one of the strictest data protection regulations approved by the EU. Fundamentally, it aims to protect the Rights and Freedoms of all individuals included in its terms; ultimately the privacy and security of all our personal data [11].

The introduction of the GDPR enables users to control how their data is accessed and processed, requiring consent from users before any data manipulation is carried out on their (personal) data by smart devices or cloud-hosted services [12].

In addition to the changes already mentioned, the GDPR also affects websites, as these are increasingly a source of data collection.

The GDPR "has changed the way websites collect and process customer data. Its effective implementation in May 2018 brought changes in the construction of procedures for requesting, storing and processing data, as well as in the interaction with consumers regarding information on how, why and where data is stored. Websites must include some dynamics in order to comply with the rules dictated by the GDPR" [13]. These dynamics go through:

- Inform consumers of the basics of data collection;
- Ensuring that consumer rights are being fulfilled;
- Provide updated Privacy and Cookie Policies;
- Allow contact to exercise the Rights of Holders.

In addition, some ways to make a website GDPR compliant are [14]:

- Update Privacy Policy;
- Cookie Consent Policy;
- Secure Data Storage;
- Comply with Data Requests;
- Penetration Testing.

There is no one-size-fits-all approach or solution for websites to be GDPR compliant, because every organization is different, the most important thing is that the GDPR protects the privacy of users and ensures that their information is properly protected.

3 Research Methodology

Document analysis was the method used in this study through the articulation between the literature review on the subject under study with the records collected on the websites of each municipality.

Document analysis becomes revealing throughout the investigation process, as it enables the interpretation of its content and enables the understanding of practices in context [15].

As already mentioned in the summary, and although the analysis of the websites of the 308 Portuguese municipalities would be optimal, this study initiated this study, restricting it to all the municipalities that make up the CIM of Terras de Trás-os-Montes, Alto Tâmega and Barroso and Douro (see Fig. 1).

As observed in Fig. 1 the CIMs under study were three of the CIMs that are part of NUTS III. The CIM of Terras de Trás-os-Montes is made up of 9 Municipalities, the CIM of Alto Tâmega and Barroso is made up of 6 Municipalities and the CIM Douro which is made up of 19 Municipalities. Thus, in this study, 34 websites belonging to the Municipalities that integrate these three CIM's were analyzed.

The analysis of the websites of these 34 municipalities was carried out between August 1, 2022 and September 30, 2022.

In order to respond to the objectives of this study, the analysis of the municipalities' websites began with a search for the terms "General Data Protection Regulation" and "GDPR".

However, the collection of search records on the websites of each municipality by the terms "GDPR" and "General Data Protection Regulation", did not have a great effect,

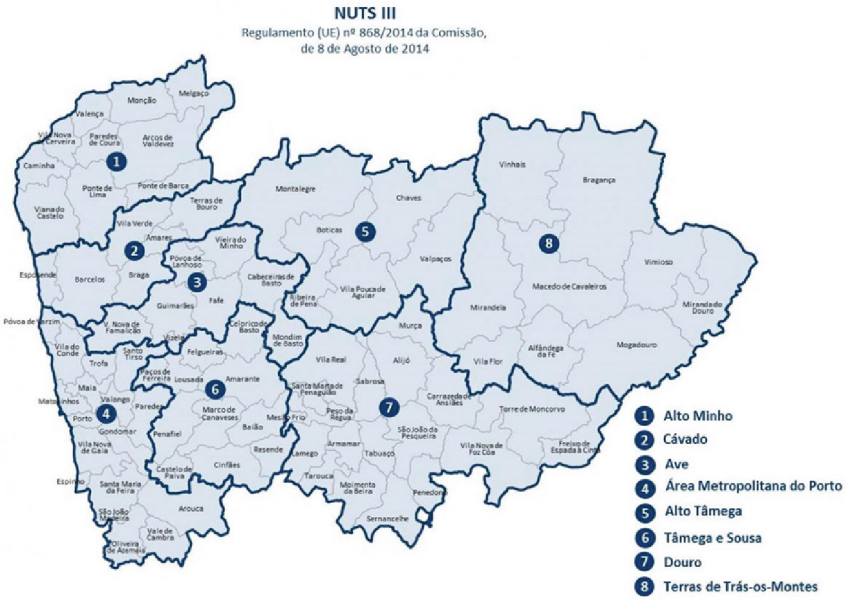

Fig. 1. CIM's study participants (5, 7 and 8)

as we found that, in a large part of them, did not return any results. Since we knew a priori that one of the municipalities had already implemented the GDPR norms and on its website, the aforementioned search did not return any value, a more exhaustive investigation was carried out, whereby we denoted that the term used would be "Privacy and Data Protection Policy".

That said, we reformulated the survey carried out so far and included the two terms in the research, "General Data Protection Regulation" and "Privacy and Data Protection Policy", no longer using the terminology "GDPR" in the research.

4 Results

The first step towards carrying out this investigation was to carry out a survey on each website of the respective municipalities in order to assess whether they contemplated some form of protection of personal data in them.

As such, the following search terms were entered in the search engine of each of the websites: "General Data Protection Regulation" and "Privacy and Data Protection Policy", as previously mentioned, in the item "Adjustments to the Planned Study" in the previous chapter, in a first phase the research focused only on the term "General Data Protection Regulation"; However, we found that most websites use the term "Privacy and Data Protection Policy".

Thus, in a universe of 34 websites researched, carrying out 68 searches in total, that is, carrying out the search for the two terms listed in the methodology, per website, 20 of them presented positive results, which corresponds to 59%, and 14 of them did not

return any given that it included any of the search terms, which corresponds to 41% (see Fig. 2).

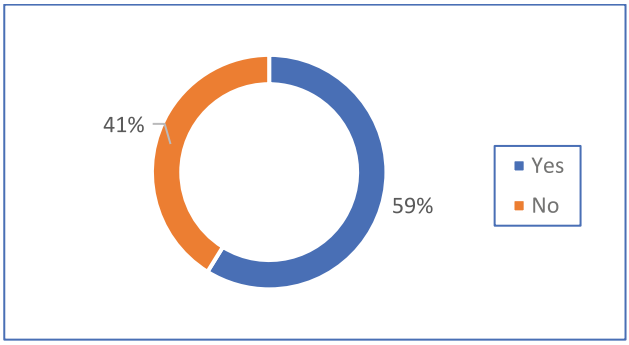

Fig. 2. Website search results

The percentage of 41% of websites that still do not include the necessary dynamics for compliance with the rules dictated by the regulation seems to us to be a somewhat still high figure, given that, after more than five years of the mandatory implementation of the norms contained in the GDPR we are faced with municipalities that still do not comply with these norms.

Since in the methodology we selected three CIM as a sample for this study, it is pertinent at this point to present individually the response of each of the municipalities, as well as the CIM they are part of. As such, in Table 1, we present the result of the search on the website of each municipality, corresponding to the "✗" to a negative result and the "✓" to a positive result, in the return of the search carried out by the two terms carried out.

In Table 1 we have all the Municipalities belonging to the three CIM's, then each of the CIM's is presented graphically. Figure 3, shows the percentage of websites that comply with the rules dictated by the GDPR belonging to the CIM-TTM. A can be seen, most CIM-TTM Municipalities comply with these rules, only 33% do not make any reference to the GDPR.

When we talk about CIM-TTM we are talking about 9 Municipalities that integrate it and as we can in Table 1 the Municipalities that translate on their Website what the data protection regulation dictates are: Alfandega da Fé, Bragança, Macedo de Cavaleiros, Miranda Douro, Mogadouro and Vimioso. On the other hand, those that do not make any reference on their Websites when we carry out searches with the defined keywords are: Mirandela, Vila Flor and Vinhais.

The question that must be asked is whether the Municipalities that do not include the dynamics present in the GDPR on their Websites have implemented the GDPR or not. Because there is a departure, the GDPR will hardly be present on websites if the regulation is not yet a reality in that Municipality.

Regarding the CIM-Douro, the largest of the three CIMs under analysis in this research work, we found that only 53% of the Municipalities comply with the standards on their websites (see Fig. 4). The figure of 47%, corresponding to 9 Municipalities

Table 1. Results by CIM

CIM-TTM	CIM-AT	CIM-Douro
✓ Alfandega da Fé	× Boticas	✓ Alijó
✓ Bragança	✓ Chaves	✓ Armamar
✓ Macedo de Cavaleiros	✓ Montalegre	× Carrazeda de Ansiães
✓ Miranda do Douro	× Ribeira de Pena	× Freixo de Espada à Cinta
× Mirandela	✓ Valpaços	× Lamego
✓ Mogadouro	✓ Vila Pouca de Aguiar	✓ Mesão Frio
× Vila Flor		× Moimenta da Beira
✓ Vimioso		✓ Murça
× Vinhais		× Penedono
		✓ Peso da Régua
		✓ Sabrosa
		✓ Santa Marta de Penaguião
		× São João da Pesqueira
		× Sernancelhe
		× Tabuaço
		× Tarouca
		✓ Torre de Moncorvo
		✓ Vila Nova de Foz Côa
		✓ Vila Real

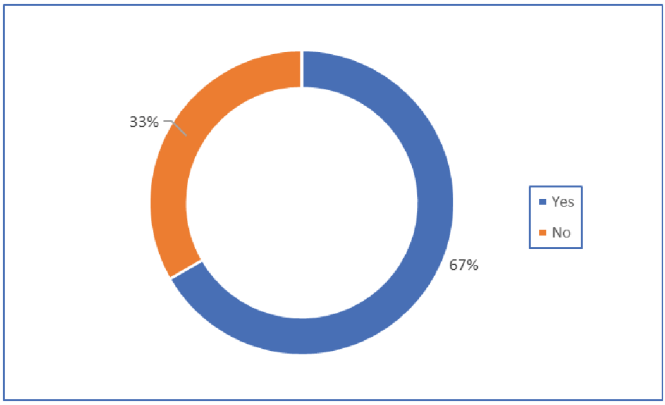

Fig. 3. CIM TTM result

among the 19 that make up the CIM-Douro, is relatively high, considering the time period since the entry into force of the GDPR and this study. Municipalities that do not have their websites in compliance are: Carrazeda de Ansiães, Freixo de Espada à Cinta, Lamego, Moimenta da Beira, Penedono, São João da Pesqueira, Sernancelhe, Tabuaço and Tarouca.

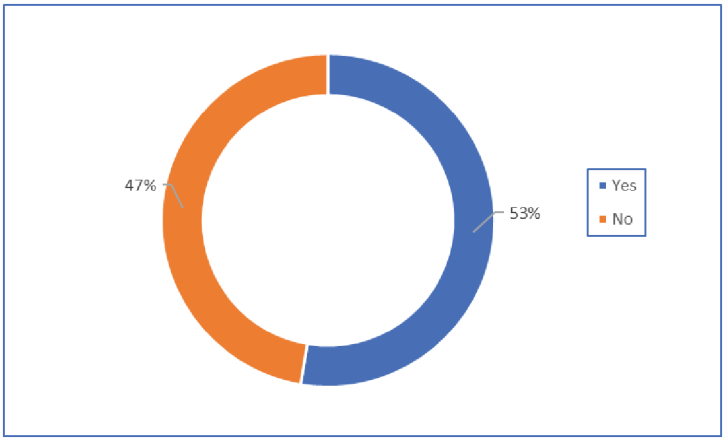

Fig. 4. CIM Douro result

Finally, CIM Alto Tâmega e Barroso, which is the CIM with the fewest Municipalities in this study, has only 6 Municipalities in its composition, 4 of which already comply with the stipulations of the GDPR on their Websites.

As shown in Fig. 5, most municipalities comply with GDPR rules on their websites, only 33% of municipalities make no reference to data protection. Only two Municipalities disagree: Boticas and Ribeira de Pena.

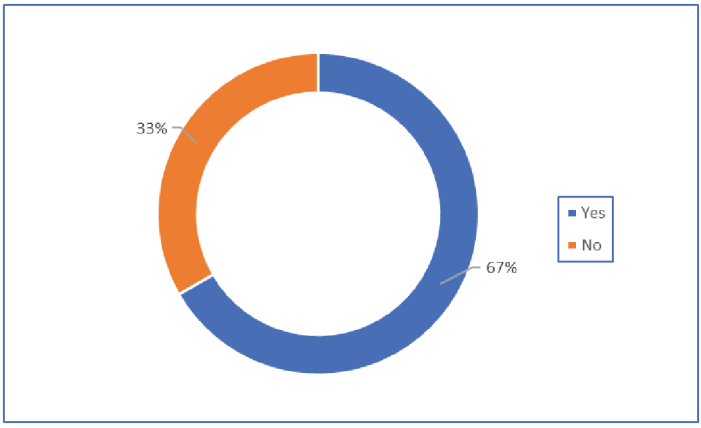

Fig. 5. CIM AT result

As already mentioned, the new General Regulation on Data Protection came into force in 2018. This document represented one of the biggest changes in the way of processing personal data ever made, with an enormous impact on all natural persons and private organizations or public entities that operate with them.

Public organizations, by virtue of their functions, have a high impact. These public organizations include the Municipalities, which due to their proximity to citizens, care in the processing of personal data must be redoubled.

Municipalities have a dual function, in addition to having to implement the GDPR, as they incur heavy fines, as they have websites with a very high consultation by citizens and which can be accessible to anyone, the compliance of these digital platforms with what dictates the GDPR is of no lesser importance.

5 Conclusions

With the development of the Information Society, organizations are getting more and more intertwined data, and the struggle to balance between protecting information resources and the need for sharing information is a daily concern. It implies potential security risks and, on the other hand, the expected benefits from the information sharing process; this balancing is not easy to achieve [16]. The need to share and the need to protect information are at first sight two opposing phenomena.

Ensuring total information security is the aim of many organizations, but the word "totality" when talking about security is very ambitious. But the GDPR will certainly contribute a lot to organizations to better protect the personal data they process.

In this research work regarding the compliance of the Websites of the 34 Municipalities with the GDPR, we realized that most of the websites of the municipalities already respect this dynamic, as 59% of the municipalities have references to the GDPR on their websites.

Although there are still 41% of the Municipalities, that is 14 of the 34 that constitute the universe of this study. This percentage can be considered high if we consider that the regulation entered into force five years ago.

When presenting these results regarding the presence of the GDPR on the websites, there is a question that arises, is whether the Municipalities that do not include the dynamics present in the GDPR on their websites, have or have not implemented the GDPR. Although this survey was not within the scope of the present work, it can be pointed out as a limitation of this study.

As future work, we propose opening this study to more CIM's so that we can better assess whether the Websites of the Municipalities include the necessary dynamics to comply with the rules dictated by the regulations.

Acknowledgements. The authors are grateful to the Foundation for Science and Technology (FCT, Portugal) for financial support through national funds FCT/MCTES (PIDDAC) to CIMO (UIDB/00690/2020 and UIDP/00690/2020) and SusTEC (LA/P/0007/2020).

The authors are grateful to the UNIAG, R&D unit funded by the FCT—Portuguese Foundation for the Development of Science and Technology, Ministry of Science, Technology and Higher Education. "Project Code Reference: UIDB/04752/2020 e UIDP/04752/2020".

References

1. Alshamsan, A.R., Chaudhry, S.A.: A GDPR compliant approach to assign risk levels to privacy policies. Comput. Mater. Continua **74**(3), 4631–4647 (2023)

2. GDPR, Retrieved 25 October 2022. https://gdpr-info.eu/. Accessed 3 Feb 2023
3. Aslan, U., Şen, B.: GDPR compliant audit log management system with blockchain. In: 15th Turkish National Software Engineering Symposium (UYMS), Izmir, Turkey (2021)
4. What is GDPR the EU's new data protection law? (2019). https://gdpr.eu/what-is-gdpr/. Accessed 1 Feb 2023
5. Asif, M., Javed, Y., Hussain, M.: Automated analysis of pakistani websites' compliance with GDPR and Pakistan data protection act. In: International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, pp. 234–239 (2021)
6. EUR-Lex - 31995L0046 - PT. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EL. Accessed 6 Feb 2023
7. Vojkovic, G.: Will the GDPR slow down development of smart cities? In: 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, pp. 1295–1297 (2018)
8. Parecer N.o 20/2018, CNPD (2018). https://www.uc.pt/site/assets/files/475840/20180502_parecer_20_cnpd.pdf. Accessed 8 Feb 2023
9. Primavera. Regulamento Geral de Proteção de Dados, Saiba como adaptar a sua empresa! (2022). https://pt.primaverabss.com/pt/tudo-que-precisa-saber-sobre-o-rgpd/. Accessed 14 Nov 2022
10. Bochis, N.: 8 Steps To Be GDPR Compliant With Your Website. https://www.online-tech-tips.com/web-site-tips/8-steps-to-be-gdpr-compliant-with-your-website/. Accessed 26 Nov 2023
11. Gobeo, A., Fowler, C., Buchanan, W.J.: GDPR and Cyber Security for Business Information Systems, in GDPR and Cyber Security for Business Information Systems, River Publishers (2020)
12. Barati, M., Rana, O., Petri, I., Theodorakopoulos, G.: GDPR compliance verification in Internet of Things. IEEE Access **8**, 119697–119709 (2020)
13. Metakia. https://metakia.com/blog/como-integrar-o-rgpd-no-seu-website/. Accessed 23 Dec 2023
14. Cobalt. https://www.cobalt.io/blog/is-my-website-gdpr-compliant. Accessed 23 Dec 2023
15. Patton, M.Q.: Qualitative Research & Evaluation Methods, 3rd edn. Sage (2002)
16. Anderson, C., Baskerville, R.I., Kaul, M.: Information security control theory: achieving a sustainable reconciliation between sharing and protecting the privacy of information. J. Manag. Inf. Syst. **34**(4), 1082–1112 (2017)