A Gestão da Privacidade nas Organizações

O papel do standard ISO/IEC 27701 na garantia de conformidade com o Regulamento Geral de Proteção de Dados

Privacy Management in Organisations

The role of ISO/IEC 27701 standard in ensuring compliance with the General Data Protection Regulation

Catarina Conde Nogueira

Extended Abstract

Mestrado em Segurança de Informação e Direito no Ciberespaço

Orientador: Capitão de Fragata EN-MEC Gonçalo Baptista de Sousa
Co-orientador: Prof. Doutor Carlos Manuel Costa Lourenço Caleiro

Júri

Presidente: Prof. Doutor Paulo Alexandre Carreira Mateus
Vogais: Capitão de Fragata EN-MEC Gonçalo Baptista de Sousa
Prof. Doutor Anacleto Cortez Correia

9 de dezembro de 2022

Abstract

The digital era in which we live enhances a continuous increase in the volume of personal data processed, resulting in a higher risk for organisations and in a threat to the Privacy of data subjects in general.

Ensure a secure personal data processing is still a challenge for organisations that must act in accordance with legal and regulatory requirements in this matter, especially the General Data Protection Regulation (GDPR), which introduced a set of requirements to store, process and collect personal data aiming to claim the fundamental right of data protection.

In order to adapt to the requirements of this Regulation, and avoid the defined penalties, organisations had to invest in implementing practices in line with its demands and have been faced with the need to interpret a legal document that does not specify, in practice, which solutions should be implemented.

The ISO/IEC 27701:2019 standard provides guidance for the establishment of a Privacy Management System, aligned with ISO/IEC 27001:2013 for Information Security management, whose data protection requirements are much in line with those established in the GDPR.

To understand the role of ISO/IEC 27701:2019 in ensuring compliance with GDPR's requirements, a comparative analysis was carried out between the requirements of both documents, which was proven in a real case study in the company Celfocus, S.A, whose Privacy Management System has recently obtained certification in the standard in study.

Keywords: Privacy Management System; ISO/IEC 27701:2019; Information Security; Data Protection; GDPR.

Goals

The objective of this work is related mainly to the presentation of a comparative analysis between the requirements of the General Data Protection Regulation (GDPR) and the controls of ISO/IEC 27701:2019 standard, in order to understand, on the one hand, the benefit that the alignment in this standard brings to Privacy management in organisations and, on the other hand, to understand its role in ensuring compliance with the regulatory requirements set out in the GDPR, transposed into Portuguese law through Law no. 58 of 2019.

First, it is presented the analysis of the points of convergence and divergence of the approaches of both standard and the Regulation, which is followed by a real case developed in the company Celfocus, S.A., whose Privacy Management System (PMS) obtained, in July 2022, the certification in the standard under study - ISO/IEC 27701:2019 - in order to investigate the role of the application of the controls established in the standard in ensuring compliance with the GDPR.

Introduction

Globalisation, together with fast technological developments, has enabled the free flow of personal data and its use on unprecedented levels, which created new challenges for the protection of personal data, requiring organisations to establish a robust data protection framework based on the requirements of the GDPR[1]. In order to achieve compliance with the requirements of this Regulation and avoid the defined penalties, organisations must invest in the implementation of good personal data protection practices[2].

The ISO/IEC 27701:2019 standard, an extension to ISO/IEC 27001 and ISO/IEC 27002, regarding privacy management, provides the key tools for organisations to be compliant with global privacy requirements, namely the internationally recognised GDPR. This standard provides the necessary guidance for the establishment, implementation, maintenance and continuous improvement of the Privacy Information Management System, as well as the implementation of the related controls to ensure personal data protection and its data subjects, regardless of the organisation's role in relation to the processing of such personal data[3]. Being an extension to ISO/IEC 27001:2013, the requirements presented for the Privacy Management System (PMS) are complementary to the requirements for the Information Security Management System (ISMS), since this standard was designed to allow the addition of specific requirements related to personal

[1] Crocetti, *et al*, 2021; Almeida Teixeira, 2019: 1-2.
[2] Lameiras, 2022; Lachaud, 2020: 11.
[3] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 1.

data processing, providing the opportunity for interested organisations to integrate their Information Security and Privacy Management Systems[4].

Regarding the structure of ISO/IEC 27701, the privacy requirements are added in clauses 5 (PIMS-specific requirements related to ISO/IEC 27001), 6 (PIMS-specific guidance related to ISO/IEC 27002), 7 (Additional ISO/IEC 27002 guidance for PII controllers) and 8 (Additional ISO/IEC 27002 guidance for PII processors), as well as in annexes A (PIMS-specific reference control objectives and controls (PII Controllers)) and B (PIMS-specific reference control objectives and controls (PII Processors)), all considered in the comparative analysis carried out[5].

The ISO 27001 and ISO 27701 certifications offer many operational advantages to companies, which are looking for a viable solution to streamline information security and personal data protection, establishing a trustworthy relationship between the organisation and its stakeholders, namely customers, partners and government authorities[6]. Since ISO/IEC 27701 is an extension to ISO/IEC 27001, it is only possible to achieve this privacy management certification if the ISMS is also certified in ISO 27001.

However, the ISO/IEC 27701 standard was not specifically developed in accordance with the GDPR, being inclusive to the application of other data protection laws, being up to organisations to duly adapt their management system to its requirements. Given that, the comparative analysis between the requirements of both documents is essential, to ensure that the alignment of the data protection practices with the standard's requirements also serves the purpose of ensuring compliance with the GDPR, which is mandatory to the organisations established in the European Union (EU) that process personal data, and also to other organisations that process European citizens' personal data[7].

Comparative Analysis

Knowing that ISO/IEC 27701 was not specifically developed to meet the GDPR, the PMS of the organisations needs to be adapted to its requirements. To understand what level of adaptation is needed, a comparative analysis between the standard's requirements and the GDPR's requirements was carried out, identifying the points of convergence and divergence, in order to assess in what extent this ISO can ensure compliance with GDPR in organisations.

Convergence points

The ISO/IEC 27701 covers articles 5 to 49 of the GDPR, with the exception of article 43 (Certification bodies), while the remaining articles, from 50 to 99, are not directly addressed to

[4] Anwar e Gill, 2020: 3; Knuuti *et al*., 2020: 17.
[5] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
[6] Lopes et. al, 2019: 3-4.
[7] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 32-33.

organisations but rather to the supervisory authorities, the European Data Protection Board and the Member States, as these are requirements that go beyond the organisations' responsibilities as Controllers and/or Processors, this being the main reason why they are not included in the ISO. It is possible to state that the standard and the GDPR have a broad convergence, namely in determining the role and responsibilities of the organisation as Controller, joint-Controller or Processor; in defining technical and organisational measures that guarantee the security of personal data processing (although the standard is more detailed); in applying the concept of continuous improvement; in assessing privacy risks; in providing the necessary resources for the proper performance and operation of the organisation with regard to data protection requirements; in requiring adequate training for people who have access to personal data; in defining internal and external communication needs, such as for the notification of personal data breaches, internally to the dedicated teams or externally to the competent supervisory authority; in ensuring data protection awareness throughout the organisation; in recording all personal data processing activities carried out, including the identification of assets where personal data is stored; in requiring compliance with applicable laws and regulations (including the GDPR); in defining a contact point for issues related to the processing of personal data, both for data subjects and competent authorities, whose role is compatible with Data Protection Officer (DPO) role defined in the GDPR; in ensuring that only those who actually need access to personal data have access to it; in using cryptographic controls for the protection of certain categories of personal data; in the ability to guarantee the permanent confidentiality, integrity, availability and resilience of the systems where personal data is processed; in establishing a contract between the Controller and the Processor that sets out the data protection requirements, as well as the need for employees who access personal data to commit to confidentiality; in following the principles of privacy by design and by default in the systems related to the processing of personal data; and in the rules for notifying privacy breaches to the responsible authorities and for its treatment.

It should also be noted that the requirements in clauses 7 and 8, for Controllers and Processors respectively, are very much in line with Articles 5 (Principles relating to processing of personal data) and 6 (Lawfulness of processing) of the GDPR, in setting out requirements for obtaining consent and for ensuring a lawful processing of personal data, as well as imposing conditions for the collection of the data.

In addition, there are also similar requirements with those in Articles 24 (Responsibility of the controller) and 28 (Processor) of the GDPR, namely in the need to apply appropriate measures that ensure the protection of personal data in the organisation and in the need to have a contract binding the Processor to the Controller, which explicitly states that the Processor only processes personal data in accordance with the Controller's documented instructions. There is also guidance in the ISO equivalent to the instructions for the preparation of the record of personal data processing activities provided in Article 30 (Records of processing activities) of the GDPR. Regarding the conduct of privacy impact assessments there is also an alignment with Article 35 (Data protection impact assessment) of the GDPR, as similar instructions are given to conduct this assessment.

In what concerns the rights of the data subjects, which are established under GDPR's Articles 15, 16, 17, 18, 20, 21 and 22 (Right of access, rectification, erasure, restriction of processing, data portability, object and non-subjection to automated individual decisions, including profiling, respectively), these are pretty much in line with sub-clauses 7.3 and 8.3 (Obligations to PII principals) of the ISO.

There is also a solid alignment with GDPR's Article 25 (Data protection by design and by default), being of utmost importance for organisations to ensure that processes and systems are designed to limit the collection and processing of personal data to what is strictly necessary, as dictated by the privacy by design and by default principle advocated in the GDPR, by following the ISO guidelines for its establishment.

The personal data transfer topic addressed in GDPR's Chapter V (Transfers of personal data to third countries or international organisations) is also present in the ISO sub-clauses 7.5 and 8.5 (PII sharing, transfer, and disclosure). The major goal of ensuring that personal data transfer to third countries doesn't compromise the protection of such data and its data subject, is common to both documents.

With the analysis of ISO/IEC 27701:2019 it is easy to understand the existing analogy with the personal data processing principles governing the GDPR. In a more general point of view, both ISO/IEC 27701:2019 and the GDPR aim to strengthen data privacy, with the GDPR focusing more on defining the basic principles for collecting and processing personal data, while the ISO seeks to assist organisations in implementing the necessary procedures to ensure compliance with applicable law and their commitment to ensuring the confidentiality and integrity of personal data. Besides this, both have a risk-based approach regarding the security of data processing, being required to assess the related risks to identify any threats that may compromise security and to act towards its minimization. The standard and the GDPR hold organisations accountable for potential personal data breaches and require promptness in notifying the competent authorities and both state the importance of keeping an up-to-date record of all personal data processing activities.

Divergence points

The divergences between the GDPR and the ISO are essentially on a conceptual level – the GDPR's approach is grounded in the protection of the data subjects' fundamental right to personal data protection plus the free movement of such data within the European Economic Area (EEA), in which information security is only one component to ensure an adequate protection, as in the ISO the main focus stands on the application of information security controls to achieve data protection.

The nature of these documents is also different. The GDPR is a mandatory Regulation for organisations that process personal data of European citizens, and the ISO is a standard of voluntary application by organisations. This reinforces some substantial differences, namely related to the material and territorial scopes, where the GDPR applies to the processing of

personal data in a non-automated, partially or fully automated way, regarding the processing of personal data of data subjects residing in the EU, regardless of whether the Controller or Processor is established in the EU territory, i.e., regardless of whether the processing takes place within or outside the EU. In the ISO, the scope is not restricted to EU territory and data subjects residing in the EU but applies to all organisations that are Controllers and/or Processors, interested in improving their information security and privacy practices.

Another difference has to do with the fact that ISO/IEC 27701 requires the implementation of a management system aligned with other ISO standards, namely ISO 27001 and ISO 27002, while the RGPD makes no such requirement, establishing a legal regime with its own principles and requirements, which are not intended to be directly auditable. It should also be noted that only ISO proposes requirements for the protection of organisations' intellectual property, which is outside the scope of the GDPR.

About certification, the GDPR foresees the establishment of data protection certification procedures, for organisations to prove the compliance of their processing operations with the Regulation. The planned certification is voluntary and issued by certification bodies with an adequate level of competence in data protection matters, by the competent supervisory authority or the European Data Protection Board, being valid for a maximum period of three years and possibly renewed under the same conditions. However, this certification procedure has never been implemented since the entry into force of the GDPR, and there is no official accredited certification even today, although the EDPB has defined the certification criteria and the CNPD has already published, in *Diário da República*, the additional accreditation requirements that it is up to the supervisory authorities to establish. When comparing with the ISO certification scheme, which was designed to certify management systems, it is possible to conclude that they are not equivalent. On the one hand, due to the fact that ISO standards are private and protected by copyright, so they couldn’t be approved by public entities, nor the requirements for certification made public and easily accessible, as required by the GDPR. On the other hand, because the ISO audit process for the organisations’ certification must be carried out by certified auditors and made official by the competent accreditation bodies, which is also not in line with what is established in Article 42 (Certification) of the GDPR. However, being ISO/IEC 27701 a widely applicable standard and an internationally recognized framework, there are several authors who argue that the certification of the PMS in this standard could serve as a basis for a potential certification mechanism for the GDPR.

Knowing that non-compliance with the GDPR may cause damage to the legal sphere of the data subjects, the Regulation provides the right for the data subject to lodge a complaint with the supervisory authority if he considers that his personal data has been unduly processed, as well as the right to take legal action against the supervisory authority, the Controller or the Processor, with the right to receive compensation for the damages suffered. In addition, the application of fines by the supervisory authority is also provided for, whenever there is a breach of the GDPR, depending on the nature, severity and duration of the breach, among other factors, with the maximum amount being twenty million euros or four percent of the organisation's annual

worldwide turnover, whichever is higher. The ISO standard doesn't foresee any penalties for organisations, only the identification of non-compliant situations during audits, which, depending on the seriousness, have stipulated deadlines for correction, and certification may be suspended while the situations are not mitigated. It should also be noted that the ISO provides the possibility of organisations to identify controls that are not applicable, according to the context in which they operate, as long as this exclusion is duly justified in their Statement of Applicability, which is not provided in the GDPR, where Controllers and Processors are responsible for complying with all data protection principles concerning them.

After this analysis, it is possible to conclude that the convergence and complementarity of these two documents are greater than the divergences found, so the organisations can benefit from the alignment with the applicable laws and a greater maturity with regard to data protection requirements, with the adoption of a PMS in accordance with ISO 27701. This comparative analysis shows that ISO 27701 can assist in the compliance with the applicable data protection laws, with the proper interpretation of the standard, to eliminate the points of divergence mentioned, facilitating the operationalisation of the necessary measures that ensure a secure personal data processing.

Case Study

This case-study was carried out in the company Celfocus, S.A with the goal of analysing to what extent the alignment of its Privacy Management System with ISO/IEC 27701:2019 provided an improvement in compliance with the requirements of the GDPR. This study was based on the comparative analysis between the requirements of the GDPR and those of ISO 27701, which were then compared with the practices implemented in the organisation and the respective documented information.

This case-study was relevant to the company, especially since it took place at the ideal time when Celfocus' Information Security and Privacy Management Systems were being prepared for the certification in ISO/IEC 27001:2013 and ISO/IEC 27701:2019, respectively, that occurred in July 2022. This made it possible to assess the impact of the application of the ISO 27701 controls in improving compliance with the GDPR, precisely during the preparation process for this certification.

At Celfocus there is no single Information Security and Privacy management system (the so-called PIMS in ISO 27701), however, the PMS and ISMS are perfectly aligned and oriented towards a common objective - to ensure compliance with contractual and regulatory requirements, with emphasis on the GDPR; to ensure the confidentiality, integrity and availability of information, including personal data; and to establish a standard of quality consistent with the size and importance of the organisation - which means that many of the Privacy practices are backed by Information Security processes, procedures and methodologies.

The alignment of the PMS with ISO/IEC 27701 was carried out together with the alignment of the ISMS with ISO/IEC 27001, since the foundation of controls and control objectives

are common, as well as the clauses related to organisational context, leadership, support, planning, operation, performance evaluation and improvement.

In order to respond to the additional privacy requirements established in the clauses 5, 6, 7 and 8 of the ISO/IEC 27701, all PMS documentation and practices were reviewed. During the preparation of the PMS for the certification audit, all these changes were followed and implemented while keeping in mind the necessary adaptation to also ensure compliance with the GDPR.

Based on the alignment of Celfocus' PMS with ISO/IEC 27701, in which I participated since the beginning, it is possible to state that the perception of improved compliance with the GDPR has increased significantly, despite the existing divergences between the standard and the Regulation, there is no doubt that certification in this ISO has made the PMS more solid, with better defined processes, procedures and responsibilities, resulting in greater involvement, awareness and sense of accountability by all employees, including senior management and third parties with influence on Privacy management.

Being ISO/IEC 27701 certified means that there will be a more systematic and regular monitoring, including by auditors external to the organisation, which results in a deeper knowledge of the personal data processing activities carried out, as well as the personal data processing procedures to be followed and also in a greater commitment from all to the Privacy requirements. In fact, the need to document data protection practices in place and their respective disclosure to the entire organisation makes employees, in general, more aware of their duties towards the management system and their rights as data subjects, which is fundamental in ensuring the company's compliance with the imposed normative and regulatory requirements.

The existence of a Privacy culture in the organisation, sustained by the evolution and growth of the PMS processes, with focus on continuous improvement, enhances the understanding of the GDPR requirements and the ability of employees to act naturally in compliance. Another added value for improving compliance with the GDPR is related to greater knowledge of data protection risks, whose assessment and control can prevent possible situations of non-compliance. It should also be noted that there were no privacy breaches at Celfocus reported to the *Comissão Nacional de Proteção de Dados* (CNPD), or any other control authority, nor were any fines applied for failure to comply with the data protection duties imposed by the GDPR, which proves that, in fact, the best practices implemented in the PMS, based on ISO 27701 as a complement to the requirements of ISO 27001 implemented in the ISMS, ensure a secure processing of personal data also in accordance with the requirements of the Regulation.

At Celfocus, the alignment of the PMS with ISO/IEC 27701 complemented the prior work around GDPR's requirements and has consolidated some practices, which made the establishment of technical and organisational measures possible that support the secure processing of personal data. It also enabled to determine the organisation's role as Controller and Processor; appoint a DPO; record personal data processing activities; identify the assets in which personal data is stored and processed; carry out periodic privacy risk assessments; provide training on personal data protection to all employees; implement the principle of privacy by design

and by default in the systems; define the internal and external communication needs; ensure the proper management of security incidents involving personal data and their notification to the control authorities; review contracts both with employees and with suppliers or other third parties, to include clauses on data protection; and increase the guarantee of confidentiality, integrity, availability and permanent resilience of the systems where personal data is processed. Also, the requirements for collecting personal data, obtaining consent, exercising data subjects' rights and ensuring lawful and transparent processing have been implemented at Celfocus in compliance with the standard and the GDPR. Practices for the secure transfer of personal data, ensuring the protection of data and its holders, have also been defined in full compliance with both documents.

Celfocus is aware that PMS certification in ISO/IEC 27701 has boosted the compliance of its practices with the requirements of the GDPR, however, it remains the responsibility of the Privacy team to know and incorporate the emerging legal and regulatory requirements applicable to the context and objectives of the organisation, so that the alignment of the PMS is as complete, up-to-date and comprehensive as possible. In essence, the entire journey taken to align the PMS with ISO 27701 served simultaneously to implement policies, processes, procedures and practices in compliance with the GDPR. During this process, it was needed to adjust the PMS in those points where the approach of the standard and the Regulation is not equivalent, so as not to compromise, on the one hand, the alignment of the PMS with ISO, as attested by the recently obtained certification and, on the other hand, ensuring compliance with the requirements of the GDPR, which, by legal imposition, are of mandatory implementation.

After all the preparation work was carried out around the ISO/IEC 27701:2019 certification, it was demonstrated that the alignment of the Celfocus PMS with this standard has ensured the integration of all the requirements of the GDPR applicable to the organisation in its system, which proves that the implementation of this standard has a key role in ensuring compliance with the GDPR, being a useful and effective tool for a rigorous and transparent Privacy management.

Conclusions

Information Security management plays a key role in ensuring the secure processing of personal data, but it is clearly insufficient if, in parallel, there is no commitment to comply with the applicable privacy legislation. In fact, the protection of personal data became a key issue for organisations when the GDPR came into force, which caused deep changes in the modus operandi of companies, with the aim of demonstrating compliance with this Regulation, ensuring secure processing of personal data. From this perspective, the standard under study, ISO/IEC 27701:2019, is undoubtedly an important tool for companies, as it provides guidelines for the establishment of a PMS in line with the applicable legislation.

The PMS alignment with ISO/IEC 27701:2019 brings benefits to organisations through an approach based on the integrated management of Privacy and Information Security, two inseparable domains, in which the controls' implementation seeks to ensure an adequate

protection of all organisational information, including personal data. Thus, it is consensual that this standard provides organisations, which act as Controllers and/or Processors, with guidelines that make it possible to streamline the implementation of practices that ensure a safe and transparent processing of personal data, contributing to the dissemination of compliance with the requirements of the GDPR.

The comparative analysis between the standard and the Regulation, documents with different nature and purpose, shows that requirements established by both are not fully equivalent. However, it is possible to conclude that the points of convergence largely outweigh the divergences found, being clear the benefit associated with the alignment of the PMS with ISO/IEC 27701:2019, mirrored in the aid of compliance with the applicable legislation on data protection, with a focus on GDPR, of course with proper adaptation to its requirements in situations where the approaches are not equivalent.

The case study carried out in the company Celfocus, S.A. corroborates the importance of the role of ISO/IEC 27701:2019 in ensuring compliance with the GDPR in organisations, since the certification, as well as all the preparatory work, demonstrated an effective integration of both the normative requirements and the requirements of the GDPR, applicable to the management system, making the organisation suitable and with proven consolidated data protection practices.

References

ALMEIDA TEIXEIRA, Gonçalo Villa de Freitas de,
"The Critical Success Factors of GDPR Implementation", Thesis to obtain the Master of Science Degree in Information Systems and Computer Engineering, Instituto Superior Técnico da Universidade de Lisboa, 2019. [Online]. Disponível em: https://fenix.tecnico.ulisboa.pt/downloadFile/1689244997260442/82070-goncalo-teixeira_dissertacao.pdf [Consultado a 25/07/2022].

ANWAR, Memoona Javeria; GILL, Asif Qumer,
"Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model", Australasian Conference on Information Systems, 2020. [Online]. Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1055&context=acis2020 [Consultado a 04/12/2021].

CROCETTI, Paul; PETERSON, Stacey; HEFNER, Kim,
"What is data protection and why is it important?", 2021. [Online] Disponível em: https://www.techtarget.com/searchdatabackup/definition/data-protection [Consultado a 01/08/2022].

International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. 1ª edição de agosto de 2019.

KNUUTI, Olli; TUUMI, Antti-Jussi; EVESTI, Antti,
"ISO 27701 Privacy Certification". KPMG Webinar Presentation. 2020, pp. 16-24. [Online] Disponível em: https://assets.kpmg/content/dam/kpmg/ru/pdf/2020/06/ru-en-iso-iec-27701-2019-certification.pdf [Consultado a 11/12/2020].

LACHAUD, Eric,
"ISO/IEC 27701: Threats and Opportunities for GDPR Certification". 2020, pp. 2-14. [Online] Disponível em: https://www.researchgate.net/publication/338676835_ISOIEC_27701_Threats_and_Opportunities_for_GDPR_Certification [Consultado a 17/12/2021].

LAMEIRAS, André,
"5 reasons why GDPR was a milestone for data protection", 2022. [Online]. Disponível em: https://www.welivesecurity.com/2022/05/25/5-reasons-why-gdpr-milestone-data-protection/ [Consultado a 01/08/2022].

LOPES, Isabel Maria; OLIVEIRA, Pedro; GUARDA, Teresa,
"Implementation of ISO 27001 Standards as GDPR Compliance Facilitator". 2019, pp.1-8. [Online]. Disponível em: https://www.researchgate.net/publication/335358551_Implementation_of_ISO_27001_Standards_as_GDPR_Compliance_Facilitator [Consultado a 10/12/2021].

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Consultado a 25/01/2022].