Privacy & Complementarity

An analysis of the interaction between ISO/IEC 27701:2019 and the GDPR

University: Tilburg University

Master: Law & Technology

Department: Tilburg Institute for Law, Technology & Society (TILT)

Author: S.A. Slijkhuis

Date: February 2021

Student number: 2048212

First supervisor: E.D. Partiti

Second supervisor: A.K. Martin

Table of contents

1. Introduction

According to Bert-Jaap Koops and Ronald Leenes, both of whom are professor of Regulation and Technology at the Tilburg Institute for Law, Technology and Society, a significant part of technologies developed and used, have an eroding effect on privacy. They describe the increased ease of privacy violations as a side effect of technology, which appears to be accepted by the users of these technologies. "Examples in law enforcement and e-government show technology offers increasing opportunities for large-scale monitoring – from intercepting all telecommunications (…) to monitoring the movements of people. In the private sector, technology enables more control of people, from workplace and transaction monitoring to personalization of consumer relationships, with new applications like facial recognition and RFID, [Radio Frequency Identification], monitoring looming ahead. (…) People gladly adopt the new possibilities [technology brings forth]. In fact, after a lapse of time, one gets so used to this new control mechanism that one may no longer perceive it as a side-effect but as an intrinsic – and perhaps intended – characteristic of technology."[1] The acceptance of the eroding effect on privacy by technology is also identified by other authors. For example, it is argued that "[a]ll that we do, and much of what we say, is recorded and saved, and we largely accept it as being for our own good and our own protection. We do our best to ignore how much of our privacy we are giving up every day, if only to get through that day."[2] As apparent, due to the ease or convenience brought about by new technologies, people seem to take the negative effect on their privacy for granted. However, a certain caution and fear of the violation of one's privacy would most certainly be in order. "Big Brother is watching you" turns out to not be as fictional as George Orwell wrote in his novel '1984' in 1949[3] after all.

Rapid technological developments play a huge role in the growing risk of the violation of an individual's right to privacy. Drones, being "unmanned aerial vehicles",[4] are amongst others being used to record footage in non-accessible areas and deliver packages. The rising use of drones, and the drones' ability of collecting, retaining, using and disclosing personal

[1] B.J. Koops & R. Leenes, ''Code' and the Slow Erosion of Privacy' (2005) 12 Michigan Telecommunications and Technology Law Review 115, 176 – 177.
[2] J. Gibb & M. Farren, *Who's Watching You?* (The Disinformation Company 2007).
[3] G. Orwell, *Nineteen Eighty-Four* (Secker & Warburg 1949).
[4] A. Cavoukian, 'Privacy and Drones: Unmanned Aerial Vehicles' (*Information and Privacy Commissioner of Ontario,* August 2012) <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-drones.pdf> accessed 10 January 2021, 3.

information, lead to privacy concerns.[5] Another risk of the violation of an individual's right to privacy is the result of the rapid development and application of the Internet of Things and Artificial Intelligence, through which companies aim to make the life of users more convenient. As appealing as a voice-controlled appliance to turn up the heating might seem, IoT devices collect vast amounts of personal data, and use these data to improve the functioning and perfectly match the needs and desires of a specific user. If this is done without asking the user's permission, or without informing the user, serious privacy challenges arise. [6] Lastly, a topical example of a technological development that could potentially infringe the privacy of individuals, is 5G. 5G offers extended connectivity, higher data rates and lower latency. Think of 5G as the widening of the highway, which results in more lanes than before, allowing more traffic to drive on the road and enabling this traffic to drive faster.[7] All the improvements 5G brings about, result in the expectation that 5G will provide a massive amount of new services and a greater user experience: our world is digitizing even further and we as users of the services will be "always connected".[8] The sum of these new services, the ever-increasing amounts of data exchanged between different devices, providers and users and the ever-increasing speed involved, all as a result of 5G, leads to concerns regarding the privacy of individuals using 5G-enabled services.[9] "What if 5G dashcams, bikes, suitcases, umbrellas, garments, etc. become a thing? For each 5G equipped thing, there will be the possibility that an attacker or manufacturer abuses it to invade your privacy." This is how Sasa Radomirovic, senior lecturer in information security at the University of Dundee in the United Kingdom, describes his concern as to how 5G could become a threat to our privacy.[10]

Whenever the privacy of certain personal data is not preserved and such information is therefore not sufficiently secured, intruders may gather, whether or not through the use of sophisticated techniques that are able to demonstrate certain correlations between large amounts

[5] V. Chang, P. Chundury & M. Chetty, '"Spiders in the Sky": User Perceptions of Drones, Privacy and Security' (CHI '17: CHI Conference on Human Factors in Computing Systems, Denver, May 2017), p. 6765 – 6766.

[6] I. Psychoula, D. Singh, L. Chen, F. Chen, A. Holzinger & H. Ning, 'Users' Privacy Concerns in IoT based Applications' (2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, Guangzhou, October 2018), p. 1887.

[7] R. Chiavetta, '5G Raises Privacy Challenges and Opportunities' (*IAPP*, 16 April 2020) <https://iapp.org/news/a/5g-to-raise-privacy-challenges-and-opportunities/> accessed 21 July 2020.

[8] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne and M. Ylianttila, '5G Privacy: Scenarios and Solutions' (2018 IEEE 5G World Forum (5GWF), Silicon Valley, July 2018), 197 – 198.

[9] Ibid.

[10] E. Baig, '5G is Speedy, But Does it Also Raise the Stakes on Privacy, Security, Potential Abuse?' (*USA TODAY*, 16 December 2019) <https://eu.usatoday.com/story/tech/2019/03/27/will-new-5-g-wireless-network-threaten-your-privacy/3032281002/> accessed 21 July 2020.

of data such as data mining, daily patterns, activities, religion and even medical information, which they may ultimately use to hurt the individual whose personal data they hold.[11]

1.1. Problem statement, research question and sub-questions

By means of their article 'The Right to Privacy',[12] written as early as 1890, Warren and Brandeis were the first to identify and use the notion of privacy.[13] Nowadays, the right to privacy is consolidated in both international, regional as well as national legislation. In the international context, the right to privacy is embodied in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). The text of both articles is almost identical. According to Article 12 UDHR, "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." Article 17 ICCPR states that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation (1); and [e]veryone has the right to the protection of the law against such interference or attacks (2)."

In Europe, the GDPR is the leading data protection regulation, that is "binding in its entirety and directly applicable in all Member States" of the European Union. [14] According to recital 6 of the GDPR, globalization and technological developments led to the emergence of new challenges regarding the protection of personal data. As never before, both private and public companies and authorities are able to use personal data to conduct their activities, personal data is collected and shared extensively, and natural persons make their own information public on an international scale.

However, the potential of the law to channel and restrict behavior is limited. It is therefore highly unrealistic to think "that the law can do all the work in creating the right kind of environment for the development and application of new technologies".[15]

---

[11] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne and M. Ylianttila, '5G Privacy: Scenarios and Solutions' (2018 IEEE 5G World Forum (5GWF), Silicon Valley, July 2018), 197 – 198.

[12] S.D. Warren & L.D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

[13] W. Unger, 'Reclaiming Our Right to Privacy By Holding Tech. Companies Accountable' (2020) 27 Richmond Journal of Law & Technology 1, 5.

[14] GDPR, final sentence.

[15] R. Brownsword and M. Goodwin, *Law and the Technologies of the Twenty-First Century* (Cambridge University Press 2012), 20.

Regulation is traditionally perceived as a public function exercised by states, at national and international level (hereinafter referred to as "traditional regulation").[16] Yet, it seems that nowadays, the concept of regulation encompasses far more than it used to. Globalization, which clearly characterizes the past decades, has led to transnational governance expanding drastically, not only through public, but also through private standardization and regulation.[17] Transnational Private Regulation (TPR) is a good example of the change that regulation has undergone and still continues to undergo to this very day. For the purpose of this thesis, the interpretation attributed to TPR by Cafaggi is adopted. "Transnational private regulation constitutes a new body of rules, practices, and processes, created primarily by private actors, firms, NGOs, independent experts like technical standard setters and epistemic communities, either exercising autonomous regulatory power or implementing delegated power, conferred by international law or by national legislation."[18] Standards can be considered a form of transnational private regulation. In line with the research carried out in this thesis, the definition of this term is based on the interpretation given to it by the International Organization of Standardization (ISO). "Standards are the distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent."[19] It should be noted that, even though the term 'private' is used in this concept, TPR regimes can oftentimes be characterized as a hybrid form of regulation in which both public and private actors are involved.[20]

Two of the leading examples of organizations establishing global private regulation are the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). These are centrally coordinated global private networks consisting of large numbers of experts, from different industries, representing different groups, in order to develop technical standards that can be applied globally.[21] The Agreement on Technical Barriers to

---

[16] F. Cafaggi, 'Transnational Private Regulation: Regulation Global Private Regulators' in S. Cassesse (ed), *Research Handbook on Global Administrative Law* (Edward Elgar Publishing 2016), 213.

[17] T. Bartley, 'Transnational Governance as the Layering of Rules: Intersection of Public and Private Standards' (2011) 12 Theoretical Inquiries in Law 517, 518.

[18] F. Cafaggi, 'New Foundations of Transnational Private Regulation' (2011) 38 Journal of Law and Society 20, 20.

[19] 'Standards' (International Organization for Standardization) <https://www.iso.org/standards.html> accessed 5 May 2020.

[20] L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019), 30.

[21] T. Büthe and W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 1-6.

Trade, requires all World Trade Organization (WTO) member states to use the international standards drawn up by ISO and IEC, to serve as the technical basis for their own legislation, unless these are "ineffective or inappropriate".[22]

The interaction between public and private regulation, often referred to as 'complementarity', is a frequently discussed subject.[23] On the one hand, it is argued that private regulation leads to a higher quality standard, since professionals from the sector are involved in the development of private regulation. At the same time, the alleged flexibility of private regulation to adapt to changing circumstances is seen as a major advantage over public regulation, which enhances the quality of private regulation. On the other hand, it is believed that, since private regulation does not go through a legislative process, the quality of private regulation, as opposed to the quality of public regulation, is compromised.[24] Gunningham and Sinclair argue that combining regulatory instruments such as transnational private regulation and public regulation, allows actors to benefit from the strengths of these regulatory instruments, whilst compensating the weaknesses.[25] The combination of regulatory instruments is seen as a more effective regulatory approach compared to the use of one single regulatory instrument.[26] Others state that the quality of standards is determined by "the degree of precision, accessibility and practicability (…) [and] the degree of coherence between the applicable rules (…) [which] concerns complementarity".[27] It is assumed that where transnational private regulation reflects prevailing public standards, this will have a positive impact on the quality of regulation. Thus, a high degree of complementarity will lead to high-quality regulation.[28] It is this second component, being the degree of coherence between the applicable rules, of the quality of a standard that this thesis focuses on.

---

[22] TBT-Agreement, Article 2.4.

[23] T. Bartley, 'Transnational Governance as the Layering of Rules: Intersection of Public and Private Standards' (2011) 12 Theoretical Inquiries in Law 517, 524.

[24] T.E. Lambooij, 'Corporate Social Responsibility. Legal and Semi-Legal Frameworks Supporting CSR. Developments 2000 – 2010 and Case Studies' (PhD Thesis, Leiden University 2010), 252 – 256; N. Jägers, 'Regulating the Private Security Industry: Connecting the Public and the Private Through Transnational Private Regulation' (2012) 6 Human Rights & International Legal Discourse 56, 73.

[25] N. Gunningham & D. Sinclair, 'Regulatory Pluralism: Designing Policy Mixes for Environmental Protection' (1999) 21 Law & Policy 49, 50.

[26] L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019), 25.

[27] N. Jägers, 'Regulating the Private Security Industry: Connecting the Public and the Private Through Transnational Private Regulation' (2012) 6 Human Rights & International Legal Discourse 56, 73 – 75.

[28] Ibid, 75.

The noteworthy stance of transnational private regulation in regulating global markets,[29] combined with current privacy challenges, raises the question concerning the interaction between public and private regulation in this respect. Therefore, the specific research question that will be answered in this thesis reads as follows:

How do public and private regulation, more specifically, the GDPR and ISO/IEC 27701:2019, interact in mitigating the risks posed to the privacy of individuals?

The scope of assessing the interaction between public and private regulation is narrowed down to the GDPR and ISO/IEC 27701:2019 given the importance of these two specific documents in the privacy challenges posed to an individual, the importance of the GDPR for organizations globally, and the importance of the GDPR in ISO/IEC 27701:2019. Throughout this thesis, I will occasionally rely on technology-related examples. However, this thesis does not specifically focus on any particular technology, but rather focusses on the GDPR and ISO/IEC 27701:2019, both documents with a more generic, not technology-specific, application.

To be able to assess the interaction between the GDPR and ISO/IEC 27701:2019, it is important to first detail the framework in which this assessment will take place in this thesis. To this end, TPR, which is the underlying concept held alongside public regulation in this thesis, is discussed, followed by an overview of different conceptions of interaction between TPR and public regulatory regimes. The specific **first sub-question** concerning this topic reads as follows: What conceptions of interaction between public and private regulation that can be drawn from literature, shape the discussion surrounding complementarity and can be used to analyze the interaction between ISO/IEC 27701:2019 and the GDPR? The literature on complementarity between public and private regulation is, in terms of answering the second and third sub-question, particularly important. In light of the scope of this thesis, two different conceptions of complementarity are used to eventually determine the interaction between ISO/IEC 27701:2019 and the GDPR. The first conception of complementarity used, which is the Institutional Complementarity Theory (ICT) as developed by Büthe and Mattli,[30] relates to the interaction between the GDPR and ISO/IEC 27701:2019 in terms of the creation of the

[29] T. Büthe and W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 9.
[30] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011).

standard. This too is a type of interaction. In this regard, the **second sub-question** being answered is: How did the GDPR contribute to the creation of ISO/IEC 27701:2019? After determining the degree of interaction, complementarity, between the public and private form of regulation in the creation of the latter, the documents are be compared to determine the vertical interaction between them. The notion of vertical interaction is based on the conception of complementarity of Senden,[31] and concerns the interaction between ISO/IEC 27701:2019 and the GDPR in terms of alignment. Therefore, the **third sub-question** reads: To what extent are ISO/IEC 27701:2019 and the GDPR aligned? In answering this question, it is not the content of the documents that is considered, but rather the terminology, objectives of establishment, the presence of prerequisites, applicability, the type of document and whether or not the documents are risk-based are taken into consideration. In addition, the GDPR's stance in terms of certification is examined, since the GDPR allows certification and even states that certification should be encouraged. Should ISO/IEC 27701:2019 be considered as certification that is allowed under the GDPR, this would evidently have a positive impact on the interaction between these documents.

1.2. Methods and methodology

The research question can be categorized as a descriptive research question, aiming to describe the interplay between public and private regulation, more specific, the GDPR and ISO/IEC 27701:2019. Two methodologies underlying this research question can be distinguished: the interdisciplinary and the doctrinal methodology. The first sub-question can be answered through the interdisciplinary methodology, predominantly using the method of literature review, to which the snowball method is inextricably linked. The second chapter is largely based on Cafaggi's explanation of TPR,[32] the framework for investigating the influence that public and private regulation had on one another in the establishment of the latter, as established by Büthe and Mattli,[33] and the notion of vertical interaction of Senden[34]. An answer to the second sub-questions, provided in the third chapter, is based on the interdisciplinary

[31] L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019).
[32] F. Cafaggi, 'New Foundations of Transnational Private Regulation' (2011) 38 Journal of Law and Society 20.
[33] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011).
[34] L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019).

methodology, since this question is answered through literature review. The primary source used to answer the second sub-question is the book in which Büthe and Mattli define the ICT.[35] The fourth chapter, in which the third sub-question is answered, entails a combination of the interdisciplinary and the doctrinal methodology, since both literature review, and the black-letter method are used to determine the differences and similarities between ISO/IEC 27701:2019 and the GDPR and to assess the stance of the GDPR in terms of certification. An approach to complementarity established by Senden[36] is used in this chapter, to analyze the interplay between ISO/IEC 27701:2019 and the GDPR.

1.3. Chapter overview

One chapter will be devoted to each of the three sub-questions. In the second chapter, the first sub-question is answered, providing a basis for the rest of the thesis in terms of understanding the concept of TPR and the different notions on complementarity found in literature. The third chapter covers the second sub-question, which essentially dives into the interaction between the GDPR and ISO/IEC 27701:2019 in terms of the establishment of ISO/IEC 27701:2019. Subsequently, the last sub-question is answered in the fourth chapter, in which ISO/IEC 27701:2019 and GDPR are compared to enable to conclude on their vertical interaction. Finally, the fifth chapter contains a conclusion which answers the main question.

[35] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011).

[36] L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019).

2. Framing the relation between ISO/IEC and the GDPR

As explained, the aim of assessing the interplay between public and private regulation at the global level is, in consideration of feasibility, narrowed down to two specific regulatory instruments, one of which is a form of public, and the other of private, regulation, being respectively the GDPR and ISO/IEC 27701:2019. ISO/IEC 27701:2019 is a standard, which, in its turn, is a form of TPR. In order to be able to frame the relationship between ISO/IEC 27701:2019 and the GDPR, it is important to provide a solid understanding of TPR itself. Thereafter, the discourse on complementarity, which is the interaction between public and private regulation, is elaborated on, therewith providing a framework of conceptions based on which the interaction between ISO/IEC 27701:2019 and the GDPR can eventually be assessed in the third and fourth chapter.

2.1. An introduction to Transnational Private Regulation

As opposed to what could be expected in an era of liberalization, deregulation and privatization, the new global order is characterized by regulation, regulators and regulatory networks, resulting in what, according to Braithwaite, is best described as a 'regulatory explosion'. Due to this regulatory explosion, we now know 'regulatory capitalism',[37] being an economic, social and political order in which regulation, instead of the provision of public and private services, is the growing section of government. Regulatory capitalism is characterized by the increasing subjection of legal forms of power to functional, rather than territorial, conditions and the increasing allocation and regulation of power along functional lines. In relation to this, the distribution of power and the corresponding representation of interests is formed by the exact interaction of private and public forms of regulation, resulting in different degrees of economic, social and political effectiveness and legitimacy.[38]

A major example of the reallocation of power towards a hybrid public-private form of regulation, and the change of form of regulation based on function instead of territory, is the rise of TPR. As a result of the rise of TPR, the traditional thinking of regulation must be reconsidered, since TPR, in many areas, supplements, complements or anticipates this traditional regulation, but cannot, be regarded as similar to it, as became apparent in the

[37] A term coined by D. Levi-Faur: D. Levi-Faur, 'The Global Diffusion of Regulatory Capitalism' (2005) 598 The ANNALS of the American Academy of Political and Social Science 12, 14.
[38] J. Braithwaite, *Regulatory Capitalism: How It Works, Ideas for Making It Work Better* (Edward Elgar Publishing 2008), vii – viii.

previous chapter, with regard to ISO/IEC 27701:2019 and the GDPR.[39] The term "transnational" is used, as opposed to "international", since TPR is not based on international law treaties. However, the use of "transnational" does not mean that TPR is not global in its nature. TPR does in fact not necessarily have to, but can definitely, have an influence across the entire globe.[40]

Reasons for the emergence of TPR are found in globalization, the ability of TPR to contribute to the growth of regulatory capacity and compliance with the law, the fast-changing dynamics of certain markets and the expertise of private parties. A wide variety of actors is involved in TPR, forming different TPR regimes, being industry-driven, NGO-led, expert-led or multi-stakeholder. Furthermore, it appears that TPR is not solely regulation, but also comprises compliance, monitoring and enforcement. The tools used within TPR are primarily tools of private law, like agreements and contracts. Consequently, the field in which TPR plays an active role is not dependent on borders and can actually involve the whole world. [41]

2.2. A discourse on complementarity

The interplay between public and private regulation is a frequently discussed subject. This so-called "complementarity" between public and private regulation is however, not assigned the same meaning in all of these writings.[42] Some perceive complementarity as public and private regulators each covering a distinct area.[43] Others interpreted this term as being the result of the possibility of tightly regulated companies to provide support for stringent private standards,[44] or the possibility for companies with voluntary "beyond compliance" commitments to facilitate an upgrade of government regulation.[45] Besides, private regulation that is eventually integrated

[39] F. Cafaggi, 'Transnational Private Regulation: Regulation Global Private Regulators' in S. Cassesse (ed), *Research Handbook on Global Administrative Law* (Edward Elgar Publishing 2016), 212.
[40] P. Verbruggen 'Gorillas in the Closet? Public and Private Actors in the Enforcement of Transnational Private Regulation' (2013) 7 Regulation & Governance 512, 514.
[41] F. Cafaggi, 'New Foundations of Transnational Private Regulation' (2011) 38 Journal of Law and Society 20.
[42] T. Bartley, 'Transnational Governance as the Layering of Rules: Intersection of Public and Private Standards' (2011) 12 Theoretical Inquiries in Law 517, 524.
[43] M. Amengual, 'Complementarity Labor Regulation: The Uncoordinated Combination of State and Private Regulators in the Dominican Republic (2010) 38 World Development 405.
[44] B. Cashore, G. Auld, S. Bernstein & C. McDermott, 'Can Non-State Governance 'Ratchet Up' Global Environmental Standards? Lessons from the Forest Sector' (2007) 16 Review of European, Comparative & International Environmental Law 158.
[45] D. Vogel, *The Market for Virtue: The Potential and Limits of Corporate Social Responsibility* (Brookings Institution Press 2005).

in government legislation, is regarded a form of complementarity as well.[46] Despite the many interpretations of the concept of complementarity, there seems to be consensus between Büthe and Mattli, Cafaggi, Senden and Bartley on the importance of assessing the relation between private and public regulation, to evaluate the effectiveness of a specific TPR regime, since they all agree that private regulation is almost always in some way connected to, and oftentimes based on, public regulation.

In this regard, Büthe and Mattli answer the question of what defines power in global rule-making. They state that "those who set standards wield influence",[47] therewith referring to public and private institutions that are involved in the private rule-making process. Büthe and Mattli developed the Institutional Complementarity Theory (ICT), through which the ability of institutions to influence the outcome of private rule-making, and thus their dominance to be able to match the standard to their domestic regulation, can be assessed.[48]

Cafaggi argues that TPR can become an instrument, particularly at national level, to harden international soft law, thus creating vertical institutional complementarity. Institutional complementarity can be both horizontal as well as vertical. Horizontal institutional complementarity exists when public and private regimes coexist at transnational level. Vertical institutional complementarity is found when TPR is complemented by public regulation at national level or vice versa.[49] In an article written in collaboration with Renda, Cafaggi observes as one of the origins of private governance, the emergence of private regulation to complement, and facilitate implementation and compliance with, public regulation.[50]

In her contribution to a Cambridge study,[51] Senden states that the notion of complementarity is based on "the presumption that the combination of regulatory instruments and actors is often more effective than a single instrument and that instruments are thus complementary". Herewith, Senden aligns herself with the line of thought of Gunningham and

[46] C.F. Sabel & J. Zeitlin, 'Learning form Difference: The New Architectures of Experimentalist Governance in the European Union' (2008) 14 European Law Journal 271.
[47] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 41.
[48] Ibid, 43.
[49] F. Cafaggi, 'New Foundations of Transnational Private Regulation' (2011) 38 Journal of Law and Society 20, 41.
[50] F. Cafaggi & A. Renda, 'Public and Private Regulation: Mapping the Labyrinth' (2012) CEPS Working Document 370/2012, 16 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2156875> accessed 20 November 2020, 19 – 20.
[51] J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019).

Sinclair, as briefly outlined in the introduction.[52] The different mechanisms of interaction between public and private regulatory regimes, which could also be described as forms of complementarity, distinguished by Senden are "comparison (and benchmarking), collaboration, coercion, conceptual interaction, cognitive interaction and competition". Additionally, complementarity can be assessed looking through a different lens, taking the different levels of complementarity into consideration. Like Cafaggi, Senden distinguishes between vertical and horizontal complementarity. However, she refers to this as the level of vertical interaction and the level of horizontal interaction. Vertical interaction indicates the interaction between public and private actors and types of regulation, and horizontal interaction is referred to as the interaction between private actors and types of regulation. With this approach, Senden aims to identify the formal and informal connection, whether existing or not, between private and public actors and types of regulation.[53]

Bartley found that the assumption that new forms of transnational governance largely surpass the old power struggles and structures, is what unites much of the existing research into the origins of TPR. However, he argues, these findings support the perception that TPR is a response to a "governance gap" and a "regulatory void", by almost completely focusing on the global level and therewith ignoring existing rules at the domestic and regional levels. It might be true that transnational standard-based organizations do not face competition of state regulation and agencies at the global level they operate on, but eventually, implementation is carried out within a state, where domestic regulation is in place. Therefore, Bartley suggests to involve "substantive intersections with domestic law, regulation, and other rules" while assessing TPR, which will reveal the complexity of numerous, overlapping and ambiguous sets of rules that constitute a pivotal aspect of globalization and transnational governance. Consequently, he identifies the most common patterns found in the layering of public and private regulation. He states that private regulation may require compliance with national law; private regulation can require certain practices, which may be substantially different from those under national law; and legal compliance and complying to the private regulation is substantively similar.[54]

---

[52] N. Gunningham & D. Sinclair, 'Regulatory Pluralism: Designing Policy Mixes for Environmental Protection' (1999) 21 Law & Policy 49, 50.

[53] L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019), 30.

[54] T. Bartley, 'Transnational Governance as the Layering of Rules: Intersection of Public and Private Standards' (2011) 12 Theoretical Inquiries in Law 517, 521 – 525.

2.3. The Institutional Complementarity Theory

Büthe and Mattli observe that compliance with a set of international standards can be beneficial for all countries, but that these benefits may vary greatly from one country to another and especially from one company to another. This results in a strong incentive for countries and companies to influence the process of international regulation in order to ensure that international standards align with their domestic regulations as closely as possible and thus minimize so-called switching costs.[55] However, it should be noted that, whilst this incentive may certainly be present for many Western countries, it might not be the case for authoritarian regimes like China and Russia, for example. These countries might want to control information based on national standards, whenever the content of international standards is not in line with their regime.

Büthe and Mattli substantiate their stance on the incentive to influence international standards with a quote from Gerald Ritterbusch, who was part of several technical committees of the Society of Automotive Engineers and served as chairman of the technical committee on earthmoving machinery of ISO, stating: "How do standards impact our ability to compete internationally? (…) When we have domestic standards that are different from international standards, everybody loses. We lose domestically because we must build a product that is different from products we sell internationally. That raises (…) [our production] costs, hurt[ing] American consumers (…) [and] caus[ing for us] unfavorable opportunities in foreign markets. What is needed is that [our] domestic standards experts aggressively participate in international standards developments to get domestic standards accepted (…) The first to [propose a standard for adoption at the international level] (…) will most likely succeed. Thus, it is necessary (…) [to] get to the international arena ahead of standards experts from other countries."[56]

In the process of international regulation, governments do not play a significant role, since their traditional power in itself is, in most instances, not beneficial for influencing the content of an international standard. Rather, "technical expertise, financial means, good and timely information, and especially effective mechanisms of interest representation", are pivotal resources to influence international private standard-setting. [57]

---

[55] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 9.

[56] U.S. House of Representatives, Committee on Science (Hearing), *Standards-Setting and United States Competitiveness* (Serial No. 107-21, 2001), 11 – 50.

[57] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 9.

The incentive for countries and companies to influence the process of international regulation and the resources proved powerful in order to exert as much influence thereon as possible, have led Büthe and Mattli to develop a framework to identify the ability of domestic standard-setting institutions to influence the outcome of private rule-making, referred to as the Institutional Complementarity Theory (ICT).[58] Global regulators like ISO and IEC, focal regulatory institutions that are uncontested in the specific areas they operate in, hold a dominant position in international private standard-setting.[59] According to the ICT, if one single international organization is the focal point for establishing a certain transnational private standard, the extent to which domestic standard-setting institutions and the international organization are aligned, the technical expertise and the economic resources available to the domestic standard-setting institution, will determine its ability to influence the content of this standard. Domestic standard-setting institutions should provide stakeholders timely information to enable those with an interest in the content of the standard to influence it at an early stage of drafting, and domestic institutions should enable effective, undisputed representation of these stakeholders at the international level.[60] The degree of institutional complementarity between domestic and international standard-setting institutions has an impact on the ability of stakeholders to influence the content of a standard and therewith influence the benefits they can derive from it.[61] A domestic standard-setting institution that has a high degree of institutional complementarity with an international standard-setting institution provides stakeholders with access to such domestic institutions with a strategic advantage by strengthening their voice in the process of international standardization. Conversely, an international standard-setting institution having a high degree of institutional complementarity with a domestic standard-setting institution, will result in greater efficiency and legitimacy in the establishment of a global standard. This is the core idea of the ICT.[62]

To answer the question which characteristics of domestic standard-setting organizations are most likely to offer the highest degree of institutional complementarity, i.e. the advantage of being able to influence the content of an international standard, Büthe and Mattli focus on the degree to which the institutional structure of these domestic standard-setting organizations

[58] Ibid, 43.
[59] Ibid, 9.
[60] Ibid, 44.
[61] Ibid, 49.
[62] Ibid, 49 – 50.

is hierarchical. They distinguish two ideal types of institutional structures: hierarchical and non-hierarchical domestic standard-setting organizations.[63]

Hierarchical domestic standard-setting institutions can be characterized by institutional hierarchy and coordination. Mapping out the institutional structure creates a pyramid with one focal point of standardization at national level at the top, followed by specialized bodies that carry out the technical work, and a third layer consisting of even more specialized working groups and subcommittees. In other words, there is a decentralized structure, in which powers and tasks are distributed from a central point. The national focal point, however, coordinates the activities of all the bodies that fall under its responsibility, provides them with guidance and ensures that no more than one standard is developed for the same issue. All stakeholders, such as industry associations, consumer organizations, regulatory authorities, and so on, are expected to represent their interests by registering with, or participating in, the specialized groups engaged in standardization related to their interests. There is no competition between the issue-specific standardization bodies.[64]

Non-hierarchical domestic standard-setting institutions are, conversely, characterized by institutional fragmentation and competition. In such a system, different standardization organizations exist side by side, there are major differences between these organizations in terms of procedures and structure and these organizations compete with one another. One domestic standard-setting institution, or a neutral third party, is appointed to be the representing body at international level. This institution, however, lacks any kind of authority over, or the ability to coordinate the work of, the different standardization organizations connected to it, as a result of which multiple standards relating to the same problem frequently coexist and competition between the member organizations emerges.

2.4. The theory of vertical interaction

Senden identifies three modes of vertical complementarity. In the first scenario, the public regulator involves the private regulator in the regulatory process. Alternatively, it may be the other way around, with the private regulator involving the public regulator in the regulatory

[63] Ibid, 50.
[64] Ibid, 50 – 52.

process. Finally, there may be a mixed initiative of public and private, where it is not clear which party is "in the driver's seat".[65]

The first scenario, by Senden referred to as the public-to-private axis, refers to cases where complementarity of public and private regulation is established through public regulators involving private actors in the public regulatory process, or when rules for private regulation are set through co-regulation or conditioned self-regulation mechanisms. The nature of public involvement can range from a formal mandate to purely informal support of the public regulator, and the intensity of public involvement can range from establishing a detailed legal or sanctioning framework to much lighter modes of participation of public actors.[66] In the field of technical standard-setting, for example, private standard-setting organizations are often awarded a regulatory mandate or provided with formally delegated regulatory powers. For instance, private regulators can be assigned the task of drafting technical standards that observe and specify what the public regulator has established.[67] An example of this first scenario is the possibility for controllers or processors to transfer personal data to a country or international organization outside the EU, if appropriate safeguards are provided for by binding corporate rules, based on Article 46 (2) (b) and Article 47 GDPR. This is a clear example of conditioned self-regulation. The conditions for these binding corporate rules are laid down in Article 47 GDPR, but a precise specification of these rules is not stipulated. This is left to controllers or processors, that can very well be private actors. Thus, private regulation is involved through in public regulation.

The private-to-public axis, which is the second mode of vertical complementarity, points to the complementarity as a result of a private regulator leading the way in setting the basic standards and requirements of the regulatory system. In such a case, the private regulator is the party that ultimately engages the public regulator in this process of regulation. This type of complementarity typically emerges where a regulatory gap is left by the public regulator and when, in the event of such a gap, the public regulator is not, in any way, involved in the process of private regulation.[68] The International Standard for Business Aircraft Operations is a good example of the private-to-public axis. Since the International Business Aviation Council initiated this sector-specific standard and involved public regulation, the International Civil

[65] L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019), 31.
[66] Ibid.
[67] Ibid, 32.
[68] Ibid, 34 – 35.

Aviation Organization, to ensure that this would become an internationally accepted and used standard.[69]

The third category, the mixed public-private axis, refers to a situation in which it is not clear which party initiated a regulation, but rather the initiative seems to be a joint one. Such a joint initiative tends to focus not so much on developing new standards or rules, but rather on establishing institutional collaboration aimed at improving the implementation of and compliance with public and private standards, by promoting a consistent and integrated approach and reducing the overlap and duplication of work.[70] An example of this category is the agreement between the public International Civil Aviation Organization and the private International Air Transport Association to establishing common standards for the assessment and evaluation of crashes.[71]

The effectiveness of the combination of public and private regulation can be examined from several perspectives. A formal perspective would indicate that solely complying with the regulation is considered effective, and a substantive perspective would indicate that achieving the set policy goals is considered effective, the latter being one step further than merely complying with the set regulation. To this substantive perspective, Senden links a question which is important in this context: "what elements need to be part of a complementary public-private regulatory approach in order for it to be capable of providing such problem-solving effectiveness?" The elements identified in assessing whether the regulation can achieve the set policy goals, are the extent to which private and public actors are aligned, in terms of the content of the rules, as well as the formal and procedural elements of the regulation. These elements demonstrate the presumption that some degree of complementarity between the public and private regulation will strengthen its effectiveness, and are therefore, in assessing the vertical complementarity of private and public regulation, important questions to be considered.[72]

2.5. Concluding this chapter

The first sub-question answered in this thesis is a theoretical one, reading: What conceptions of interaction between public and private regulation that can be drawn from literature, shape the discussion surrounding complementarity and can be used to analyze the interaction between ISO/IEC 27701:2019 and the GDPR? In this regard, four different conceptions of the notion of

[69] Ibid, 35.
[70] Ibid, 35.
[71] Ibid, 37.
[72] Ibid, 37 – 38.

complementarity were briefly discussed to describe the discourse on complementarity. In view of the scope of this thesis, the ICT of Büthe and Mattli and the theory of vertical interaction of Senden were elaborated on further, to allow the second and third sub-question, and eventually the main research question, of this thesis to be answered in the following chapters.

3. Applying the Institutional Complementarity Theory to ISO/IEC 27701:2019 and the GDPR

The first conception of complementarity that is used to describe the interaction between the GDPR and ISO/IEC 27701:2019 is the Institutional Complementarity Theory of Büthe and Mattli.[73] This theory will enable us to conclude on the role of the national standard setting institutions of Member States of the EU, who all have an interest in international standards being in line with the GDPR, that must be observed in any transfer of personal data within the EU, as well as transfers to international organizations and third countries.

In the preceding chapter, in which the ICT is explained, it appeared that, assessing the institutional complementarity requires the need to know the institutional structure of the international standard-setting institution and its procedures, to determine the features of domestic standard-setting institutions that will position the stakeholders of that country or region in the most powerful position to influence the content of the global standard.[74] Therefore, the first section will discuss the institutional structure of ISO and IEC. The second section contains the assessment of the institutional structure of European domestic standard-setting institutions. Consequently, the third section regarding the role of regional standard-setting institutions, which comes down to the role of standards within the EU, is taken into consideration. Ultimately, the second sub-question can be answered in the conclusion of this Chapter 3. The sources relied on to ascertain the information laid down in this chapter consist mainly of information provided by ISO and IEC on their websites. Many of the facts and figures mentioned in this thesis are frequently subjected to change. Not every change results in an update of an ISO or IEC document, or a book or article written about ISO or IEC. However, the most recent and up to date information on ISO and IEC can be found on these websites. For this reason, the websites of ISO and IEC are an important source of information for this chapter. The information provided by ISO and IEC is predominantly complemented by information originating from the book of Büthe and Mattli central to this chapter, that is "The New Global Rulers".

[73] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011).
[74] Ibid, 50.

3.1. The institutional structure and procedures of ISO and IEC

After being recommended to take steps to establish a commission representing the world's technical societies and to contemplate standardization, IEC was officially born during a preliminary meeting on June 27th, 1906.[75] Starting in 1911, IEC formed specialized committees, named technical committees (TC) whose objective was to write standards and in 1926, IEC allocated a technical committees' secretariat to a national standards organization, that, from that moment on, would provide administrative support to IEC. The financial benefit this institutional innovation brought about, since the organization and management of a TC was now part of the responsibility of the national standards organization, allowed IEC to focus on the production of international standards and accelerate this process. [76]

ISO is the result of the merger of the International Federation of the National Standardizing Associations (ISA), which was established in 1926, and the United Nations Standards Coordinating Committee (UNSCC), which was established in 1944, during a conference of national standardization organizations that took place in London from the 14th to the 26th of October, 1946.[77] ISO followed IEC in its successful practice in which national standard organizations are closely involved in establishing international standards, since its members are national standard-setting bodies, i.e. the national organization of standardization that is the most representative of that country's standardization organizations. Similar to IEC, these national standardization organizations are private organizations predominantly financed by the industry, these members appoint experts representing their country in specific ISO TC's and cover 60 percent of the operational costs of the central ISO secretariat in Geneva by means of membership fees.[78]

Both IEC and ISO offer multiple memberships to accommodate all kinds of countries, including developing countries. The type of membership chosen reflects the member's participation possibilities and whether or not, or to a lesser extent, a membership fee must be paid.[79] IEC counts 62 full members who, after payment of their annual membership fee, can send experts to actively participate in a technical committee or subcommittee of their choice,

---

[75] 'How and why the IEC was started', (*International Electrotechnical Commission*) <https://www.iec.ch/history/how-why-iec-was-started> accessed 25 November 2020.

[76] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 138.

[77] W. Kuert, 'The Founding of ISO', in ISO, *Friendship Among Equals. Recollections from ISO's First Fifty Years* (ISO 1997), 15.

[78] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 138 – 139.

[79] Ibid, 139.

who can apply for management positions and positions in the IEC and have voting rights in the IEC Council.[80] ISO counts 122 full members that influence the development and strategy of the ISO standards by participating and voting in ISO's technical and policy meetings.[81] ISO decided to offer multiple types of membership in the 1970s, aiming to strengthen the credibility and legitimacy of ISO as a global organization by promoting membership outside the developed world.[82] The final result delivered by ISO originates from 792 TC's and subcommittees[83] and 2782 working groups[84]. IEC counts a total amount of 701 working groups and 210 TC's and subcommittees.[85] In these groups of both ISO and IEC, experts from industry (predominantly) and governments, academia, consumer organizations and NGO's from all over the world gather to develop international standards.[86] [87] To ensure consistency throughout the standards and to warrant that no more than one standard is developed for the same challenge or product, the Geneva secretariats coordinate the work performed within these fora. Decentralization of detailed technical work, strict coordination and an organizational hierarchy appear to be important characteristics of ISO and IEC.[88]

The supreme governing body of both ISO and IEC is the Council.[89] [90] The role of the Councils and related advisory committees can best be described as an addition to the extensive

[80] 'National Committees', (*International Electrotechnical Commission*) <https://www.iec.ch/national-committees> accessed 26 November 2020.
[81] 'Members', (*International Organization for Standardization*) <https://www.iso.org/members.html> accessed 26 November 2020.
[82] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 139.
[83] 'About Us', (*International Organization for Standardization*) <https://www.iso.org/about-us.html> accessed 26 November 2020.
[84] This is the most recent figure available, from the end of 2019. 'ISO in Figures 2019', (*International Organization for Standardization*) <https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/iso_in_figures/docs/iso-in-figures_2019.pdf> accessed 26 November 2020.
[85] 'IEC Technical Committees & Subcommittees', (*International Electrotechnical Commission*) <https://www.iec.ch/dyn/www/f?p=103:62:0::::FSP_LANG_ID:25> accessed 26 November 2020.
[86] 'What We Do', (*International Organization for Standardization*) <https://www.iso.org/what-we-do.html> accessed 26 November 2020.
[87] 'National Committees', (*International Electrotechnical Commission*) <https://www.iec.ch/national-committees> accessed 26 November 2020.
[88] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 141.
[89] 'ISO/Council', (*International Organization for Standardization*) <https://www.iso.org/committee/55010.html> accessed 26 November 2020.
[90] 'Council', (*International Electrotechnical Commission*) <https://www.iec.ch/dyn/www/f?p=103:65:0::::FSP_ORG_ID,FSP_LANG_ID:3227,25> accessed 26 November 2020.

structure of committees.[91] The ISO Council meets three times a year and reports to the General Assembly.[92] The IEC Council meets at least once a year during the IEC General Meeting.[93]

The procedure of standardization of ISO and IEC are similar as well. Both organizations require a multistage process to eventually establish a standard, in which fundamental issues are decided at the very beginning while the technical specification gradually become more detailed. The aim of both ISO and IEC is to reach the greatest possible degree of consensus in order to achieve a result that is desirable for as many stakeholders as possible. Ultimately, it will be decided based on a majority decision procedure whether or not to adopt the resulting technical specification as an international standard.[94]

3.2. The institutional complementarity of ISO and IEC and the GDPR

Büthe and Mattli conclude that, given the characteristics of the institutional structure of ISO and IEC and its procedures, the more hierarchical the structure of a domestic standard-setting institution is, the greater the institutional complementarity towards ISO and IEC is, thus the greater their ability to influence the content of the specific standard. This reasoning is based on the fact that hierarchical systems of standardization have clear procedures in place for the collection of stakeholder preferences, that such a system increases the probability of a single national standard preceding the international standard and that stakeholder preferences of a country are aligned. In a hierarchical system, the stakeholder preferences are merged into one single national point of view, with one single designated person or body representing this point of view with one single voice at the international level. ISO and IEC have "consensus" standards, which maximize the legitimacy and eventual adoption of the standards. If a domestic standard-setting institution makes it difficult, or even impossible, to appear on the world stage with a single view, the legitimacy and eventual adoption by stakeholders, and thus the effectiveness of the standard, will suffer. If stakeholders challenge the position presented on the world stage, they undermine the possibility of benefiting from the international consensus

[91] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 141.

[92] 'ISO/Council', (*International Organization for Standardization*) <https://www.iso.org/committee/55010.html> accessed 26 November 2020.

[93] 'Council', (*International Electrotechnical Commission*) <https://www.iec.ch/dyn/www/f?p=103:65:0::::FSP_ORG_ID,FSP_LANG_ID:3227,25> accessed 26 November 2020.

[94] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 50.

standards used by ISO and IEC, since it shows that whatever changes are made to the design of the standard, not all national stakeholders can be accommodated.[95]

3.2.1. The institutional structure of domestic standard-setting institutions

To be able to conclude on the level of institutional complementarity between ISO/IEC and domestic standard-setting institutions subject to the GDPR, it is important to first identify which countries, and the corresponding domestic standard-setting institutions, are subject to the GDPR. After all, the aim is to find out whether the countries that have to comply with the GDPR were able to exert a great deal of influence on the content of ISO/IEC 27701:2019, as a result of which the GDPR is largely taken into account in the formation of ISO/IEC 27701:2019. After that, the institutional structure of these organizations can be identified, based on the extensively discussed book of Büthe and Mattli, which brings us another step closer to concluding on the institutional complementarity between ISO/IEC and the domestic standard-setting institutions that must adhere to the GDPR.

The Member States of the European Union, and therefore the countries that are subject to the GDPR, are: Austria (ASI and OVE), Belgium (NBN and BEC), Bulgaria (BDS), Croatia (HZN), Cyprus (CYS), Czech Republic (UNMZ), Denmark (DS), Estonia (EVS), Finland (SFS and SESKO), France (AFNOR), Germany (DIN and DKE), Greece (NGIS ELOT), Hungary (MSZT), Ireland (NSAI), Italy (UNI and CEI), Latvia (LVS), Lithuania (LSD), Luxembourg (ILNAS), Malta (MCCAA), the Netherlands (NEN), Poland (PKN), Portugal (IPQ), Romania (ASRO), Slovakia (UNMS SR), Slovenia (SIST), Spain (UNE), Sweden (SIS and SEK). The domestic standard-setting institution of the countries are included between brackets. Where one institution is included, this institution is a member of both ISO and IEC. Where two institutions are included, the first is a member of ISO and the second is a member of IEC. All of these countries' domestic standard-setting institutions are 'Member Bodies' of ISO,[96] and most of these countries' domestic standard-setting institutions are 'Full Members' of IEC, except from the domestic standard-setting institutions of Cyprus, Estonia, Latvia, Lithuania and Malta, whose domestic standard-setting institutions are 'Associate Members' of IEC.[97] Whilst 'Full Members' and 'Member Bodies' are able to actively participate in standard-setting and have

[95] Ibid, 52 – 58.

[96] 'Members', (*International Organization for Standardization*) <https://www.iso.org/members.html> accessed 8 December 2020.

[97] 'National Committees', (*International Electrotechnical Commission*) <https://www.iec.ch/national-committees> accessed 8 December 2020.

voting rights,[98] being an 'Associate Member' of IEC implies that those institutions can access all working documents and are allowed to send experts to participate in a limited number of technical committees or subcommittees, but cannot occupy functions within IEC and are not allowed to vote in the IEC Council.[99]

Apart from the ability to influence transnational standard-setting derived from the type of membership of a country, as becomes apparent from the ICT, the institutional structure of domestic standard-setting institutions is of great importance to be able to conclude on the level of complementarity those institutions have towards the transnational standard ISO/IEC 27701:2019. There is no one single approach to standardization within the world nor within Europe. Where British firms can be characterized by liberalism, coordination is a key characteristic of German firms, and French firms rely on state and professional intervention.[100] However, taken as a whole, Büthe and Mattli argue that the institutional structure of European domestic standard-setting institutions can be characterized as hierarchical.[101]

3.2.2. Concluding on institutional complementarity between ISO/IEC and European domestic standard-setting institutions

Interestingly, and as a matter of example, in the context of data privacy for e-commerce, European regional standards have already surpassed United States regional standards as it was ultimately more important for companies engaged in transnational e-commerce to adopt a single set of privacy standards for their increasingly global activities. As a result, United States consumer information databases whose commercial use was illegal according to European standards have lost most of their value and European standards have risen to the international level, according to Büthe and Mattli.[102] In terms of the global importance of the GDPR, this proof of the mindset of organizations before, is highly likely to have reoccurred in the establishment of ISO/IEC 27701:2019. This is further stressed, since ISO/IEC 27701:2019 includes mapping to the GDPR in Annex D, and the GDPR being the only public regulatory

---

[98] 'National Committees', (*International Electrotechnical Commission*) <https://www.iec.ch/national-committees> accessed 8 December 2020; and 'Members', (*International Organization for Standardization*) <https://www.iso.org/members.html> accessed 8 December 2020.

[99] 'National Committees', (*International Electrotechnical Commission*) <https://www.iec.ch/national-committees> accessed 8 December 2020.

[100] J. Tate, 'National Varieties of Standardization' in P.A. Hall & D. Soskice (ed), *Varieties of Capitalism. The Institutional Foundations of Comparative Advantage* (Oxford University Press 2001), 468.

[101] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 147.

[102] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 34.

document ISO/IEC 27701:2019 refers to. Using the Institutional Complementarity Theory, an answer to the first sub-question can be provided, eventually enabling us to assess the influence European domestic standard-setting organizations have on the content of ISO/IEC standards.

Since all processing of personal data within the EU or across its borders is governed by the GDPR, and therefore the domestic standard-setting institutions in Europe providing standards relating to data protection within the EU must ensure these domestic standards comply with the GDPR as well, it is beneficial for these domestic standard-setting institutions for ISO/IEC standards to comply with the GDPR. This minimizes the 'costs' of complying with the standard. It can be concluded that there is a high degree of institutional complementarity between ISO/IEC and domestic standard-setting institutions in Europe based on the ICT. Considering the institutional structure of both ISO/IEC and the domestic standard-setting institutions that must comply with the GDPR, these institutions have the ability to exert a great deal of influence on the content of the final international standard, as a result of which they can ensure that there is agreement between the regulations that apply to them and the new international standard.

3.3. Regional standard-setting institutions

The Institutional Complementarity Theory is, as stressed before, all about the ability of national standard-setting institutions to influence the content of international standards. However, in Europe, standardization is not only settled at the national level, but also at the regional level. According to the European Commission, standardization plays an important role in the creation of the EU single market. Besides, "[s]tandards support market-based competition and help ensure the interoperability of complementary products and services. They reduce costs, improve safety, and enhance competition". In the EU, the use of standards is promoted, since standards offer a way in which regulation can be improved and competitiveness of the EU industry can be enhanced.[103]

The "New Approach" to technical harmonization and standards under EU internal market legislation reflects the EU's desire to use private regulation. With the introduction of this "new approach", European directives can be limited to only defining essential parts and requirements. Through harmonized standards, such as the development of technical specifications, such European directives can be supplemented. Harmonized standards are

[103] 'Standardisation Policy', (*European Commission*) <https://ec.europa.eu/growth/single-market/european-standards/policy_en> accessed 18 January 2021.

standards which have been established on the basis of a mandate of the European Commission. Harmonized standards are drafted according to a specific procedure, in which the European Commission has the final authority to judge whether the standard complies with the request and with applicable EU harmonization legislation. Formally, of course, such standards are a type of private regulation. However, the controlled and conditioned practice in which these standards are created, lead to the conclusion that public regulation and the public regulatory authority play a major role in its creation.[104] In 2016, the Court of Justice of the EU recognized harmonized standards as part of European law.[105]

The harmonization of standardization at the European level shows that national varieties within Europe are being brought together rather than eliminated. "In the larger world, Europe's multi-coordinated approach to standardization confronts a congeries of nationally coordinated market economies in Asia, led by Japan and China, as well as a hyper-liberal approach to standardization rooted in the USA." This is not only due to the fact that ISO and IEC standards tend to be more responsive to European needs compared to, for example, those of the United States, but also because of the formal collaboration between ISO and IEC and their European counterparts.[106] In 1991, by signing the Vienna Agreement, the technical cooperation between ISO and the European Committee for Standardization (CEN) was established. Among other things, it stipulates that, where possible, priority will be given to cooperation with ISO in order to ensure that international standards meet European legal and market-related requirements. In 1996, the Dresden Agreement was signed between IEC and the European Committee for Electrotechnical Standardization (CENELEC) to facilitate consensus between European and international standards in the electricity sector. The fruitful cooperation between IEC and CENELEC was reconfirmed in 2016, by signing the Frankfurt Agreement. The continuous cooperation between these parties on the basis of the Vienna Agreement and the Frankfurt Agreement facilitates the high degree of alignment between European and international standards.[107]

---

[104] L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019), 33.

[105] Case C-613.14 *Elliot* [2016] ECR I-821, paras. 40 – 43.

[106] J. Tate, 'National Varieties of Standardization' in P.A. Hall & D. Soskice (ed), *Varieties of Capitalism. The Institutional Foundations of Comparative Advantage* (Oxford University Press 2001), 469 – 472.

[107] 'ISO & IEC', (*CEN and CENELEC*) <https://www.cencenelec.eu/intcoop/StandardizationOrg/Pages/default.aspx> accessed 8 December 2020.

3.4. Concluding this chapter

The second sub-question reads: How did the GDPR contribute to the creation of ISO/IEC 27701:2019? Based on the foregoing, it can be concluded that the interplay between ISO, IEC and the GDPR in general can be characterized as a relation of complementarity, in which national standard-setting institutions have a strong possibility to exert influence on the content of the international standard developed by ISO and IEC, which is also reinforced by the long-standing cooperation between ISO and CEN, and IEC and CENELEC. Given the high degree of institutional complementarity between ISO and IEC and European national standard-setting institutions, the conclusion can be drawn that these national standard-setting institutions were able to influence, and thus contribute to, the content of ISO/IEC 27701:2019 to be in line with the GDPR, which is to their advantage as it allows them to minimize the so-called switching costs. The observation that ISO and IEC standards tend to be more responsive to European needs compared to for example those of the United States and the significance of European involvement in ISO and IEC international standard-setting support even more that ISO/IEC 27701:2019 can be of great value in compliance with the GDPR.

4. Vertical interaction between ISO/IEC 27701:2019 and the GDPR

In Article 42 (1) GDPR, it is explicitly stated that Member States of the EU, the supervisory authorities, the European Commission and the European Data Protection Board should encourage "the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with" the GDPR. Herewith, vertical complementarity to the GDPR is allowed. This statement in the GDPR leads, within the context of this thesis, to the question of whether or not ISO/IEC 27701:2019 is such a data protection certification mechanism. If so, this would evidentially contribute to the effectiveness of ISO/IEC 27701:2019. Therefore, this chapter starts with discussing potential vertical complementarity between ISO/IEC 27701:2019 and the GDPR based on Article 42 (1) GDPR.

Following this, substance will be given to the conception of complementarity that is used to describe the interaction between the GDPR and ISO/IEC 27701:2019. This is the theory of Senden, relating to vertical interaction between public and private regulation.[108] According to Senden, the effectiveness of the combination of public and private regulation can be examined from a formal and a substantive perspective. The substantive perspective requires to assess the extent to which private and public actors are aligned, in terms of the content of the rules, as well as the formal and procedural elements of the regulation.[109] To this end, the content of the GDPR and ISO/IEC 27701:2019 followed by a comparison of the terminology, objectives of establishment, the presence of prerequisites, applicability, the type of document and whether or not the documents are risk-based are assessed.

Ultimately, the third sub-question can be answered, allowing to draw a conclusion on the interaction between ISO/IEC 27701:2019 and the GDPR.

4.1. The GDPR and certification

The entry into force of the GDPR in 2018 has had a major impact, not only in the EU, but also beyond European borders, on any organization processing personal data.[110] The GDPR is

[108] L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019).
[109] Ibid, 37 – 38.
[110] E. Lachaud, 'ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification' (15 January 2020) <https://poseidon01.ssrn.com/delivery.php?ID=925001095006090087092121029125102031105056038064034051074003124118100095026073102029063026017056028045033096019081114095068073061007010028093003086024081067072010067093060076123115086079106105016100104069092091024075002015073066115071101099074093097097&EXT=pdf> accessed 13 January 2021, 14.

"binding in its entirety and directly applicable in all Member States" of the EU.[111] According to recital 6 of the GDPR, globalization and technological developments led to the emergence of new challenges regarding the protection of personal data. As never before, both private and public companies and authorities are able to use personal data to conduct their activities, personal data is collected and shared extensively, and natural persons make their own information public on an international scale. It is emphasized in recital 6 of the GDPR, that in terms of the free flow of personal data within the EU and the transfer of personal data to third countries or international organizations, a high level of protection of personal data must be ensured. Recital 100 of the GDPR stresses the importance of the flow of personal data to and from (organizations within) countries outside the EU, for international trade and cooperation. However, the level of protection ensured in the EU through the GDPR, must never be compromised whenever data is transferred to and from these third countries or international organizations. The same applies to further transfers of personal data from a third country or international organization. In any event, the transfer of personal data to third countries and international organizations may only take place while fully complying with the GDPR. Failure to comply with the rules laid down in the GDPR can incur significant financial consequences.[112]

One of the key principles of the GDPR is the principle of accountability laid down in Article 5 (2) GDPR, which holds the controller responsible for, and requires the controller to be able to demonstrate, compliance with the other principles relating to the processing of personal data as laid down in Article 5 (1) GDPR. This essentially comes down to the obligation to be able to demonstrate GDPR compliance, and thus the obligation to be GDPR compliant.[113] As becomes apparent from recitals 78 and 81 of the GDPR, the principle of accountability requires controllers and processors to implement appropriate technical and organizational measures. According to recital 81 of the GDPR, adherence to an approved certification mechanism can be used as a means of demonstrating GDPR compliance.

In some fields, such as product safety in EU, compliance with harmonized standards is equated to compliance with legal obligations. However, if a controller or processor has had its

---

[111] GDPR, final sentence.

[112] E. Lachaud, 'ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification' (15 January 2020) <https://poseidon01.ssrn.com/delivery.php?ID=925001095006090087092121029125102031105056038064034051074003124118100095026073102029063026017056028045033096019081114095068073061007010028093003086024081067072010067093060076123115086079106105016100104069092091024075002015073066115071101099074093097097&EXT=pdf> accessed 13 January 2021, 14.

[113] M. Rhahla, S. Allegue & T. Abedllatif, 'A Framework for GDPR Compliance in Big Data Systems' in S. Kallel, F. Cuppens, N. Cuppens-Boulahia & A. Hadj Kacem (eds), *Risks and Security of Internet and Systems* (Springer 2019), 211 – 212.

data processing activities certified, no such conclusion can be drawn. Indeed, certification under the GDPR plays a different role. In this context, certification serves as a means of demonstrating to the national supervisory authority that appropriate technical and organizational measures have been taken to meet the legal obligations arising from the GDPR. This is, as stated above, an important element of the principle of accountability. So, when a certification authority judges that a controller or processor meets the certification criteria, it cannot conclude that this controller or processor is GDPR compliant.[114]

4.2. The legal framework of GDPR certification

The question of whether certification should or could play a role in the European framework of data protection was raised well before the GDPR was finalized.[115] For example, the Article 29 Working Party (WP29), which is the predecessor of the European Data Protection Board (EDPB), argued in 2010 that "the provision on accountability may foster the development of certification programs or seals".[116] Around the same time, the European Commission has indicated that it will investigate the possibility of creating European certification schemes for privacy compliant processes, technology, products and services.[117] Eventually, certification was endorsed in the GDPR. Articles 42 and 43 GDPR set out the objectives, safeguards and roles of the actors, alongside the overarching principles for certification and accreditation processes.[118]

Article 42 (1) GDPR states that "the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors" must be encouraged by the Member States, the supervisory authorities, the European Commission and the Board. Thus, according to Article 42 (1) GDPR, the object of certification is one or more processing operation. Where applicable, the EDPB states that three core components

---

[114] I. Kamara, '4 GDPR-Certification Myths Dispelled' (*IAPP*, 28 January 2020) <https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/> accessed 14 January 2021.

[115] E. Lachaud, 'ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification' (15 January 2020) <https://poseidon01.ssrn.com/delivery.php?ID=925001095006090087092121029125102031105056038064034051074003124118100095026073102029063026017056028045033096019081114095068073061007010028093003086024081067072010067093060076123115086079106105016100104069092091024075002015073066115071101099074093097097&EXT=pdf> accessed 13 January 2021, 2.

[116] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010), 17.

[117] Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union' (Communication) COM (2010) 609 final, 12.

[118] Commission, 'Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679' (Final Report, February 2019), 20.

should be considered while assessing the processing operation, being the personal data, technical systems used, and processes and procedures relating to the processing operation(s).[119] The second paragraph of Article 42 further clarifies that the establishment of data protection certification mechanisms and of data protection seals and marks can be used as a tool to demonstrate that appropriate safeguards are taken by controllers or processors subject to the GDPR, as well as controllers and processors that are not subject to the GDPR, but that, in the context of transfers of personal data to third countries or international organizations, must demonstrate that appropriate safeguards are in place to protect personal data, pursuant to Article 46 (2) (f) GDPR. Article 42 (3) GDPR requires certification to be voluntary and available through a transparent process. Certification does not reduce the responsibility of the controller or processor to be compliant with the GDPR, as is laid down in Article 42 (4) GDPR. This underlines the statement of the European Commission that "[t]he focus is rather on the element of demonstration of compliance than on compliance as such".[120] Certification is, according to Article 42 (7) GDPR, issued for a maximum of three years and can be renewed, based on the same conditions, provided the relevant requirements are met. Whenever the requirements are no longer met, the certification body or relevant supervisory authority shall withdraw the certification.

It follows from Article 42 (5) GDPR, that a certification may be provided by a certification body, a competent supervisory authority or by the EDPB. Article 43 GDPR lays down the criteria and responsibilities accredited certification bodies that "have an appropriate level of expertise in relation to data protection" have to adhere to in issuing and renewing certification based on Article 42 GDPR. According to Article 57 (1) (o), (p), and (q) GDPR, the competent supervisory authority is responsible for approving the criteria of certification in accordance with Article 42 (5) GDPR, for carrying out a periodic review of certifications in accordance with Article 42 (7) GDPR, drafting and publishing accreditation criteria of a certification body and conducting the accreditation of a certification body. The same tasks are imposed on the EDPB based on Article 70 (o), (p), and (q) GDPR. In addition to Article 57 GDPR, Article 58 (1) (c) GDPR empowers the competent supervisory authority to carry out a review of certifications issued in accordance with Article 42 (7) GDPR. Article 58 (2) (h) GDPR empowers the competent supervisory authority to withdraw certification or to order a

[119] EDPB, 'Guidelines 1/2018 on certification and identifying criteria in accordance with Articles 42 and 43 of the Regulation' (Version 3.0, 4 June 2019), 15 – 16.
[120] Commission, 'Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679' (Final Report, February 2019), 20.

certification body to withdraw, or not to issue, a certification whenever the requirements of Article 42 and 43 GDPR are not, or no longer, met. Lastly, the competent supervisory authority has the power to, as follows from Article 58 (3) (e) and (f) GDPR, to accredit certification bodies and to issue certifications and approve certification criteria.

Multiple sources underline the complexity of Article 42 and 43 GDPR.[121] It is argued that through the complex certification mechanism of Article 42 and 43 GDPR, the existing certification system is updated to suit the needs of the protection of a fundamental right. This appears to be an attempt to accommodate both the need for certification schemes, seals and marks of the market and industry, to meet the skeptics of self-regulation, and to satisfy the demand for regulatory oversight, aiming to balance two different approaches on certification, being a strong European data protection seal issued by the supervisory authorities and various national certification mechanisms issued by certification bodies.[122] Besides, the European Commission finds complexity in the fact that the subject matter of certification under Articles 42 and 43 GDPR is not clear, as the subject matter is not limited to one specific topic, "potentially thus covering a legal obligation such as data security or even the full spectrum of controller and processor's GDPR obligations".[123]

4.3. Comparing the GDPR and ISO/IEC 27701:2019 based on the theory of vertical interaction

From the foregoing, it follows that certification was considered in the drafting of the GDPR as a possible means of demonstrating GDPR compliance. However, a statement of the European Commission explicitly asserts that ISO/IEC 27701:2019 is not a data protection certification mechanism in terms of Article 42 and 43 GDPR, stating that "[s]ome relevant international standards promote a management system that conflicts with the scope of certification as specified in Article 42 (1) GDPR." In this regard, the Information Security Management System of ISO/IEC 27001:2013 and Privacy Information Management System.

---

[121] E. Lachaud, 'ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification' (15 January 2020) <https://poseidon01.ssrn.com/delivery.php?ID=925001095006090087092121029125102031105056038064034051074003124118100095026073102029063026017056028045033096019081114095068073061007010028093003086024081067072010067093060076123115086079106105016100104069092091024075002015073066115071101099074093097097&EXT=pdf> accessed 13 January 2021, 4.

[122] I. Kamara & P. de Hert, 'Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a Reformed Landscape' in R. Rodrigues & V. Papakonstantinou (eds), *Privacy and Data Protection Seals* (Information Technology and Law Series 28, Springer 2018), 10 – 14.

[123] Commission, 'Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679' (Final Report, February 2019), 21.

PIMS) of ISO/IEC 27701:2019[124] are mentioned as examples.[125] So, if ISO/IEC 27701:2019 is not a certification mechanism under the GDPR, how does interaction between these particular private and public forms of regulation take place?

To answer this question, it is essential to juxtapose and compare the two documents. The content, terminology, objectives of establishment, the presence of prerequisites, applicability, the type of document and whether or not the documents are risk-based are taken into consideration in the following sections.

4.3.1. The content

In Annex D of ISO/IEC 27701:2019, a 'mapping to the GDPR' is provided to show that compliance with this standard can be helpful in complying with obligations of the GDPR. Even though this mapping provides a purely indicative list, and organizations are responsible for assuring compliance with requirements of the GDPR themselves, this list clearly indicates which articles of the GDPR are kept in mind while drawing up ISO/IEC 27701:2019. This mapping shows that Article 5 and 6 GDPR, Articles 12 to 39 GDPR, and Article 44 to 48 GDPR have been taken into account when establishing ISO/IEC 27701:2019, so the PIMS will comply with the GDPR.[126] Besides, ISO/IEC 27701:2019 requires the context of national regulation and legislation to be taken into account when implementing the standard, explicitly referring to the GDPR.[127] Even though ISO/IEC 27701:2019 aims to align with the GDPR, and clearly does based on the mapping provided in Annex D, compliance with this standard is not equal to compliance with the GDPR. ISO/IEC 27701:2019 frames requirements for a management system, which can be a useful component of demonstrating GDPR compliance, but cannot lead to the conclusion that a controller or processor is GDPR compliant.[128]

4.3.2. Objectives of establishment

"Almost every organization processes Personally Identifiable Information (PII). Further, the quantity and types of PII processed is increasing, as is the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII.

[124] The source refers to ISO/IEC DIS 27552, which is now published as ISO/IEC 27701:2019.
[125] Commission, 'Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679' (Final Report, February 2019), 166.
[126] ISO/IEC 27701:2019, Annex D.
[127] ISO/IEC 27701:2019, subclause 0.1.
[128] I. Kamara, '4 GDPR-Certification Myths Dispelled' (*IAPP*, 28 January 2020) <https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/> accessed 14 January 2021.

Protection of privacy in the context of the processing of PII is a societal need, as well as the subject of dedicated legislation and/or regulation all over the world."[129] With this in mind, ISO/IEC 27701:2019, of which the title in full reads 'ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines', is created to. Recital 6 and 7 of the GDPR refer to technological developments bringing forth new challenges to the protection of personal data, as the objective of the establishment of the GDPR. In combination with globalization, "[t]he scales of the collection and sharing of personal data has increased significantly", requiring a strong and coherent framework for the protection of personal data in the European Union. Article 1 (2) of the GDPR stresses the aim of this regulation to protect "fundamental rights and freedoms of natural persons and in particular the right to the protection of personal data". Clearly, the objective of the establishment of both ISO/IEC 27701:2019 and the GDPR is the protection of privacy/personal data.

4.3.3. Security as a prerequisite

ISO/IEC 27701:2019 complements ISO/IEC 27001:2013, which was preceded by ISO/IEC 27001:2005 and is now confirmed and amended with ISO/IEC 27001:2013/COR1:2014 and ISO/IEC 27001:2013/COR2:2015,[130] and ISO/IEC 27002:2013, which is amended by ISO/IEC 27002:2013/COR1:2014 and ISO/IEC 27002:2013/COR2:2015 and is now under review and will be replaced by ISO/IEC CD 27002.2[131]. ISO/IEC 27701:2019 extends these two information security standards to cover the protection of PII.[132] ISO/IEC 27001:2013, the full name of which reads 'ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements', is created to define requirements and provide guidance through the process of the establishment, implementation, maintenance and continuous improvement of an information security management system (ISMS).[133] ISO/IEC 27000:2018 describes an ISMS as an information security management system designed to help organizations develop and implement a framework for managing the security

[129] Ibid.
[130] 'ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements' (*ISO*) <https://www.iso.org/standard/54534.html> accessed 5 November 2020.
[131] 'ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls' (*ISO*) <https://www.iso.org/standard/54533.html> accessed 5 November 2020.
[132] 'ISO 27701, an international standard addressing personal data protection' (*CNIL*, 2 April 2020) <https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection> accessed 5 November 2020.
[133] ISO/IEC 27001:2013, title.

of their information assets[134] by ensuring the confidentiality, integrity and availability of those information assets.[135] In addition, authenticity, accountability, non-repudiation and reliability can play a critical role in ISMS.[136] An ISMS as included in ISO/IEC 27001:2013 serves to ensure the confidentiality, integrity and availability of information through the application of a risk management process, by "establishing, implementing, maintaining and continually improving an [ISMS] within the context of the organization", including "requirements for the assessment and treatment of information security risks tailored to the needs of the organization".[137]

ISO/IEC 27002:2013, to which the full name 'ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls' has been assigned, is meant as a reference for organizations for selecting controls while implementing an ISMS based on ISO/IEC 27001:2013, or can serve as a guideline for organizations to implement commonly accepted information security controls.[138] The ISMS as laid down in ISO/IEC 27001:2013 is open to the addition of context specific requirements, without the need for a new management system, as this standard requires the specific context of an organization to be taken into account when implementing an ISMS. The protection of PII by means of an ISMS can thus be connected to the requirements that are imposed on a particular organization by amongst others national laws and regulations and sector specific norms. The Personal Information Management System (PIMS) as defined in ISO/IEC 27701:2019 is such an addition, since a PIMS is defined as being an ISMS addressing the protection of privacy of those whose privacy is potentially affected by processing PII.[139] Besides, it is stated that ISO/IEC 27701:2019 "is a sector-specific document related to ISO/IEC 27001:2013 and to ISO/IEC 27002:2013".[140] This is also clearly reflected in chapter 5, 6 and 7 of this standard, where repeatedly additional requirements to these standards are stipulated, existing requirements are refined, or additional guidance and information is provided for, in order to fit the scope of ISO/IEC 27701:2019. ISO does not provide the definition of a PIMS, but considering the definition of an ISMS and the aim of a PIMS, one can define a PIMS being a set of policies and procedures serving to protect the personal information that is processed by a

[134] ISO/IEC 27000:2018, subclause 0.1 – clause 1.
[135] ISO/IEC 27000:2018, subclause 3.28.
[136] ISO/IEC 27000:2018, subclause 3.28.
[137] ISO/IEC 27001:2013, subclause 0.1.
[138] ISO/IEC 27002:2013, subclause 0.1.
[139] ISO/IEC 27701:2019, subclause 3.2.
[140] ISO/IEC 27701:2019, subclause 4.1.

company.[141] In sum, ISO/IEC 27701:2019 requires compliance with ISO/IEC 27001:2013 before being applied: the prerequisite of compliance with the PIMS, is to make sure that personal data managed by the organization seeking certification is incorporated in the ISMS.[142] The GDPR does not contain any prerequisites, but rather includes security of data protection as one of the GDPR's basic principles relating to the processing of personal data, as follows from Article 5 (1) (f) of the GDPR.[143]

4.3.4. Terminology

The terminology used in ISO/IEC 27701:2019 is based on the terminology used in ISO/IEC 29100:2011. ISO/IEC 29100:2011 establishes the framework with common basic principles, rules and terminology to be used in the ISO standards dealing with data protection issues.[144] Some important terms used in ISO/IEC 27701:2019 differ from the ones used in the GDPR, however, the meaning of those important terms is nearly the same. This includes the use of 'privacy', 'Personally Identifiable Information (PII)' and 'PII principles' in ISO/IEC 27701:2019, instead of, respectively, 'data protection', 'personal data' and 'data subject' in the GDPR.[145] However, slight differences in terms used, are not the only difference in terms of terminology. ISO/IEC 27701:2019 introduces additional terms that are not used in the GDPR, like 'privacy controls', and the interpretation of terms used in the standard is sometimes more accurate compared to the interpretation of the equivalents of these terms used in the GDPR, and vice versa.[146] For example, 'sensitive data' is defined more precisely in Article 9 (1) of the GDPR.[147] And a more precise definition of 'data processor' is used in ISO/IEC 27701:2019,[148] compared to the definition of this term in Article 4 (8) of the GDPR.

---

[141] E. Lachaud, 'ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification' (15 January 2020) <https://poseidon01.ssrn.com/delivery.php?ID=925001095006090087092121029125102031105056038064034051074003124118100095026073102029063026017056028045033096019081114095068073061007010028093003086024081067072010067093060076123115086079106105016100104069092091024075002015073066115071101099074093097097&EXT=pdf> accessed 9 December 2020, 6.

[142] Ibid.

[143] Ibid.

[144] ISO/IEC 29100:2011, clause 1.

[145] E. Lachaud, 'ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification' (15 January 2020) <https://poseidon01.ssrn.com/delivery.php?ID=925001095006090087092121029125102031105056038064034051074003124118100095026073102029063026017056028045033096019081114095068073061007010028093003086024081067072010067093060076123115086079106105016100104069092091024075002015073066115071101099074093097097&EXT=pdf> accessed 9 December 2020, 12.

[146] Ibid.

[147] Compared to the definition used in ISO/IEC 27701:2019, stemming from ISO/IEC 29100:2011, subclause 2.26.

[148] ISO/IEC 29100:2011, subclause 2.26.

4.3.5. Applicability

As appears from Article 2 (1) of the GDPR, the GDPR is applicable "to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system". The GDPR is thus applicable to both structured and unstructured, whether or not by automated means, sets of data. ISO/IEC 27701:2019, on the other hand, only focuses on sets of data organized in IT assets, so-called structured datasets.[149]

4.3.6. Type of document

ISO/IEC 27701:2019 is a private standard, adopted based on the procedure of standardization of ISO and IEC, in which requirements for a management system, a PIMS, are laid down. Besides, ISO/IEC 27701:2019 can be regarded as a form of management-based regulation, which does not specify technologies, but rather requires organizations to "engage in their own planning and internal rule-making efforts that are supposed to aim towards the achievement of specific public goals".[150] Whether or not an organization wants to comply with ISO/IEC 27701:2019 is up to them, since TPR certification is voluntary.[151] The GDPR is a public regulatory document, laying down a legal framework for the protection of personal data, applicable in all Member States of the EU and to all transfers of personal data to third countries and international organizations. A link between the GDPR and certification schemes like ISO/IEC 27701:2019 is laid down in Article 42 (1) of the GDPR, "the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors" must be encouraged by the Member States, the supervisory authorities, the European Commission and the Board. However, as stated before, the European Commission argues that ISO/IEC 27701:2019 conflicts with the scope of certification as specified in Article 42 (1) GDPR.

---

[149] E. Lachaud, 'ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification' (15 January 2020) <https://poseidon01.ssrn.com/delivery.php?ID=925001095006090087092121029125102031105056038064034051074003124118100095026073102029063026017056028045033096019081114095068073061007010028093003086024081067072010067093060076123115086079106105016100104069092091024075002015073066115071101099074093097097&EXT=pdf> accessed 13 January 2021, 6.

[150] C. Coglianese & D. Lazer, 'Management-Based Regulation: Prescribing Private Management to Achieve Public Goals' (2003) 37 Law & Society Review 691, 692.

[151] F. Cafaggi, 'New Foundations of Transnational Private Regulation' (2011) 38 Journal of Law and Society 20, 22.

4.3.7. Risk-based

ISO/IEC 27701:2019 stimulates a risk-based approach by establishing requirements for a risk management process which is defined by ISO as "the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, identifying, analyzing, evaluating, treating, monitoring and reviewing risk".[152] The way in which an organization that is certified based on ISO/IEC 27701:2019 eventually complies with the requirements, depends on the level of risk, in what way this risk is detected and evaluated within the organization, and the context of the data processing.[153] The GDPR, however, can be considered as being partially risk-based, since provisions ensuring lawfulness, proportionality and transparency of the processing of personal data[154] are not based on the risk to the right of a data subject: all data processing must, at any time, fulfill these basic requirements, according to Article 5 of the GDPR. According to Gellert, the concept of risk as laid down in the GDPR should be understood as a 'compliance risk', in which the risk is both an event as well as a consequence. The lack of compliance can be understood as the event, whereas the risk to the rights and freedoms of the data subject are the consequence of the lack of compliance.[155] In his view, the risk-based approach in the GDPR is intended to allow the controller to 'calibrate' its obligations in line with the nature and level of risks that threaten the fundamental rights of data subjects laid down in the GDPR.[156] Quelle argues that, in line with the meaning Hood, Rothstein and Baldwin assign to 'risk regulation',[157] the GDPR can be characterized as being risk regulation, intended to addressed the risk posed to the privacy of individuals as a consequence of the digitization and globalization of our society. Though clearly stated that a risk-based approach of regulation and risk regulation should not be conflated, the risk-based approach of the GDPR does rely on the designation of data protection as a system

[152] ISO/IEC 27000:2018, subclause 3.69.

[153] E. Lachaud, 'ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification' (15 January 2020) <https://poseidon01.ssrn.com/delivery.php?ID=925001095006090087092121029125102031105056038064034051074003124118100095026073102029063026017056028045033096019081114095068073061007010028093003086024081067072010067093060076123115086079106105016100104069092091024075002015073066115071101099074093097097&EXT=pdf> accessed 9 December 2020, 7.

[154] Ibid.

[155] R. Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279, 280.

[156] R. Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279, 279 – 288.

[157] They define risk regulation as "governmental interference with market or social processes to control potential adverse consequences". See: C. Hood, H. Rothstein & R. Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxfort University Press 2001), 3.

of risk regulation, since the concept of 'risk' guides controllers in implementing data protection legislation in order to achieve its purpose.[158] Thus, Quelle argues as well, that the GDPR can be characterized by a risk-based approach, "providing a flexible safety net in a fast-moving field".[159] In the GDPR itself, the risk-based approach becomes apparent from Article 24 (1) and Article 25 (1) of the GDPR stating that "the risk of varying likelihood and severity for the rights and freedoms of natural persons" must be taken into account. A bridge from the risk-based approach of the GDPR to certification allowed under the GDPR can be found in recital 77 of the GDPR, in which is laid down that "[g]uidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, (…) could be provided in particular by means of (…) approved certifications".

4.4. Concluding this chapter

The key principle of the GDPR in relation to certification is the principle of accountability laid down in Article 5 (2) GDPR. The accompanying obligation of a controller is to be able to demonstrate compliance with the other principles relating to the processing of personal data. In this context, the GDPR refers to approved certification mechanisms as a suitable means of demonstrating compliance. It is important to note that, within the meaning of the GDPR, certification serves as a means of demonstrating that appropriate technical and organizational measures have been taken to meet the legal obligations arising from the GDPR. Thus, the focus of certification within the GDPR is on demonstrating compliance with specific measures, instead of compliance with the GDPR as such.

The GDPR acknowledges the importance of the flow of personal data to and from international organizations and third countries, and the importance of the level of protection ensured in the EU through the GDPR to be ensured in these data transfers to and from third countries and international organizations that are not directly bound by the GDPR. Certification could serve as a means for international organizations to show their compliance with the GDPR.

In the GDPR, certification is covered in Article 42 and 43 GDPR, which set out the objectives, safeguards and roles of the actors, alongside the overarching principles for certification and accreditation processes. But even though certification is included in the GDPR, there is consensus on the complexity of the rules relating to certification.

---

[158] C. Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2019) 9 European Journal of Risk Regulation 502, 508 – 510.
[159] Ibid, 525.

The third sub-question is: To what extent are ISO/IEC 27701:2019 and the GDPR aligned? From this chapter, it can be concluded that in terms of comparing the GDPR and ISO/IEC 27701:2019, these documents do not nearly appear to be similar. Besides from the fact that these documents align in terms of content, have similar objectives for the establishment of either of the documents and both pursue a risk-based approach to the protection of personal data, ISO/IEC 27701:2019 and the GDPR differ significantly in terms of terminology, prerequisites, applicability and the type of document both documents can be identified as being. Although it is important to highlight these differences, ISO/IEC 27701:2019 can be considered as complementary to the GDPR, within the meaning ascribed to complementarity by Senden and Cafaggi, but not to a particularly high degree of complementarity. This is because of the fact that effectiveness of ISO/IEC 27701:2019 as being a tool to demonstrate compliance with the GDPR can be doubted, since, based on the foregoing, it is not likely that ISO/IEC 27701:2019 will be recognized as such, based on Article 42 of the GDPR.

5. Conclusion

To finalize this thesis, a summary of all findings is provided, followed by the answer to the main research question. Finally, a brief reflection on the limitations of this research is provided.

5.1. Summary of the findings

ISO and IEC are internationally active private standard-setting institutions. They can be regarded as a clear example of TPR in practice, since standardization is a form of TPR. TPR emerged as an answer to globalization, fast-changing dynamics, the need to incorporate expertise of private parties in regulation and the ability to contribute to the growth of regulatory capacity and compliance with the law.

The interplay between public and private regulation is a frequently discussed subject matter. Several scholars and researchers have studied the interaction between public and private regulation and define it as a relationship of complementarity. The discourse on complementarity is shaped by Büthe and Mattli, Cafaggi, Senden and Bartley. Büthe and Mattli state that "those who set standards, wield influence",[160] therewith referring to public and private institutions that are involved in the private rule-making process. They developed the ICT, through which the ability of institutions to influence the outcome of private rule-making, and thus their dominance to be able to match the standard to their domestic regulation, is assessed. Cafaggi argues that vertical institutional complementarity is found when TPR is complemented by public regulation at national level or vice versa. Senden argues that vertical interaction indicates the interaction between public and private actors and types of regulation, and horizontal interaction is referred to as the interaction between private actors and types of regulation. The substantive perspective on vertical complementarity requires to assess the extent to which private and public actors are aligned, in terms of the content of the rules, as well as the formal and procedural elements of the regulation. Ultimately, Bartley considers the interaction between public and private regulation to be the layering of rules. He suggests to involve domestic law, regulation and other rules while assessing TPR. This will reveal the complexity of multiple, overlapping and ambiguous sets of rules. The most common patterns in the layering of rules according to Bartley are private regulation requiring compliance with national law; private regulation requiring certain practices, which may be substantially different from those under national law; and legal compliance and complying to the private regulation being substantively similar.

[160] T. Büthe & W. Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), 41

One of the theories developed with regard to complementarity is the ICT, which is used to answer the second sub-question aiming to figure out the way in which interaction between ISO/IEC 27701:2019 and the GDPR in the establishment of ISO/IEC 27701:2019 took place. The ICT assumes that the degree of institutional complementarity defines the extent to which national standard-setting institutions are able to influence the outcome of private rule-making and thus are able to match the standard to their domestic regulation as far as possible, which, in its turn, minimizes switching-costs. According to Büthe and Mattli, the institutional structure of a national standard-setting institution is important in determining whether a high level of institutional complementarity between ISO and IEC and the GDPR exists. Considering the institutional structure of ISO and IEC, hierarchical domestic standard-setting institutions, characterized by institutional hierarchy, a decentralized structure that is being coordinated, and no competition, are, most likely to have a higher degree of institutional complementarity. This is in contrast to non-hierarchical domestic standard-setting institutions, that can be characterized by institutional fragmentation, competition and multiple standards on the same issue due to a lack of coordination. The higher the degree of hierarchy, the higher the degree of institutional complementarity.

It can be concluded that European national standard-setting institutions can be characterized as highly hierarchical institutions, which enables us to conclude that those institutions have a high degree of institutional complementarity with regard to ISO and IEC, are thus able to influence the outcome of private rule-making to a great extent and to match the standard to their domestic regulation as far as possible. Given the high degree of institutional complementarity between ISO and IEC and European national standard-setting institutions, the conclusion can be drawn that these national standard-setting institutions were able to influence, and thus contribute to, the content of ISO/IEC 27701:2019. With this, these parties were able to try to align the content of ISO/IEC 27701:2019 with the GDPR, which is to their advantage as it allows them to minimize the so-called switching costs.

Not only national standard-setting institutions are subject to the GDPR, but also regional standard-setting institutions within Europe. In this regard, an important observation leads to the finding that ISO and IEC standards tend to be more responsive to European needs compared to for example those of the United States. Besides, the cooperation between ISO and IEC and their European counterparts stresses the significance of European involvement in ISO and IEC international standard-setting.

The last sub-question aims to explore the extent to which ISO/IEC 27701:2019 and the GDPR are aligned. Prior to examining these two documents, the framework provided for

certification in the GDPR itself is discussed. ISO/IEC 27701:2019 could potentially be approved certification in line with the GDPR, which would contribute to the effectiveness of this standard and the interaction with the GDPR. However, the European Commission clarifies that ISO/IEC 27701:2019 is not a data protection certification mechanism in terms of Article 42 and 43 GDPR, by stating that "[s]ome relevant international standards promote a management system that conflicts with the scope of certification as specified in Article 42 (1) GDPR." ISO/IEC 27701:2019 will therefore not be(come) a certification mechanism based on Article 42 (1) GDPR, but this does not mean it cannot be a building-block for organizations to demonstrate compliance with the GDPR. This will not lead to the conclusion of compliance, but may serve as a component of this conclusion.

In comparing the GDPR and ISO/IEC 27701:2019, it appeared that these documents are, apart from the fact that given their nature these documents could never be equal to each other, not nearly equal. The content of ISO/IEC 27701:2019 does align with the requirements of the GDPR, which follows from the mapping to the GDPR in Annex D of ISO/IEC 27701:2019. With regard to terminology, it can be concluded that ISO/IEC 27701:2019 has not adhered to the terminology used in the GDPR, but rather built upon the terminology it is using in other standards. Different terms are used for concepts having the same meaning as concepts laid down in the GDPR, ISO/IEC 27701:2019 provides its own definitions for several terms and, besides, introduces terms that do not appear in the GDPR. This is a logical consequence of the fact that ISO/IEC 27701:2019 establishes a management system that builds upon a management system defined in ISO/IEC 27001:2019 and ISO/IEC 27002:2019. The objectives for the establishment of both of these documents are similar, since both aim to provide protection of personal data, or PII in the case of ISO/IEC 27701:2019, in a world that is characterized by globalization and rapid technical developments. The more specific objective for the establishment of ISO/IEC 27701:2019 is to define an ISMS which allows to add sector specific requirements to the PIMS defined in ISO/IEC 27001:2019 and ISO/IEC 27002:2019, without having to develop a new management system. Given the fact that ISO/IEC 27701:2019 builds upon ISO/IEC 27001:2013 and ISO/IEC 27002:2013, private standards requiring the implementation of a management system providing with information security, ISO/IEC 27701:2019 can be characterized by having security as a prerequisite. In the GDPR on the other hand, security is one of the basic requirements of compliance with this regulation, instead of a prerequisite. This prerequisite of ISO/IEC 27701:2019 follows from the fact that ISO/IEC 27701:2019 builds upon ISO/IEC 27001:2013 and ISO/IEC 27002:2013, in which a PIMS requiring security is laid down. As a result, when an organization seeks compliance based on

ISO/IEC 27701:2019, ISO/IEC 27001:2013 and ISO/IEC 27002:2013 must already be complied with. With regard to the applicability, it can be stated that the GDPR applies to the processing of personal data by both automated and non-automated means, whereas ISO/IEC 27701:2019 only relates to the processing of PII structured in IT assets. Finally, ISO/IEC 27701:2019 is considered exerting a fully risk-based approach, as the way an organization implements ISO/IEC 27701:2019 depends on risk. Even though the GDPR is not regarded as being fully risk-based, since some of its requirements are not dependent on the occurrence of a risk of invasion of someone's privacy by a certain processing activity. Every processing operation must meet these requirements. Nevertheless, in the literature the GDPR is seen as a document adopting a risk-based approach, as the concept of risk guides controllers to the implementation of data protection law. Furthermore, a risk-based approach also appears from Articles 24 (1) and 25 (1) of the GDPR. In addition, Recital 77 prescribes approved certification as a means of implementing appropriate measures and demonstrating compliance with the GDPR, especially with regard to identifying risks relating to the processing of personal data. The GDPR and ISO/IEC 27701:2019 are clearly different types of documents, the first being a form of public regulation, the latter a private standard, which is a form of TPR. It can however be concluded that there is a certain level of complementarity between ISO/IEC 27701:2019 and the GDPR. Even though the fourth chapter shows the differences between ISO/IEC 27701:2019 and the GDPR, ISO/IEC 27701:2019 could very well complement the GDPR. This does not constitute high degree of complementarity, because of the fact that effectiveness of ISO/IEC 27701:2019 as being a tool to demonstrate compliance with the GDPR can be doubted, considering the statement of the European Commission.

5.2. The answer to the research question

Now all sub-questions have been answered and a summary of the findings is presented, an answer to the main research question can be provided. This main question, reading ‘How do public and private regulation, more specifically, the GDPR and ISO/IEC 27701:2019, interact in mitigating the risks posed to the privacy of individuals?’ can be answered based on different conceptions of complementarity found in literature. Based on the theory of institutional complementarity, the fact that ISO and IEC closely cooperate with CEN and CENELEC, and the finding that ISO and IEC standards tend to be more responsive to European needs, it can be stated that in general, ISO and IEC cooperate very well with both regional and domestic standard-setting institutions located in Europe – countries that are obviously subject to the GDPR and benefit from the standards developed by them to correspond with the GDPR. This

contribution to the establishment of ISO and IEC standards, more specifically ISO/IEC 27701:2019, is one of the ways in which the GDPR and ISO/IEC 27701:2019 interact, based on the interaction between ISO, IEC and European countries in general. However, it appeared that GDPR and ISO/IEC 27701:2019 are nowhere near comparable, since these documents differ in terms of terminology, applicability, prerequisites and the type of documents they are. As one cannot compare apples and oranges, it would make sense to stop here and argue that real interaction between the GDPR and ISO/IEC 27701:2019 cannot occur. However, a closer look into the specific provisions of both documents shows that all important provisions required by the GDPR are taken into account in the establishment of ISO/IEC 27701:2019. ISO/IEC 27701:2019, being a private regulatory standard to which organizations can voluntarily be certified, does thus, besides the influence the GDPR had on the content of the standard in the process of its establishment, interact with the GDPR. It can be concluded that here is not a high degree of complementarity between the GDPR and ISO/IEC 27701:2019, based on the theory of vertical interaction and the accompanying assessment of the extent to which private and public actors are aligned, in terms of the content of the rules, as well as the formal and procedural elements of the regulation. This is backed by the fact that the European Commission explicitly excludes the possibility of ISO/IEC 27701:2019 to be a permitted method of certification under the GDPR, since ISO/IEC 27701:2019 promotes a management system that conflicts with the scope of certification as specified in Article 42 (1) GDPR. Therefore, in terms of alignment based on the theory of vertical interaction and in line with the assumption that a high degree of complementarity will lead to high-quality regulation, the effectiveness of ISO/IEC 27701:2019 in practice can be questioned.

5.3. Reflecting on the research

This research was conducted with a major focus on literature review, using the interpretation and perspective of academics as a framework for analyzing the interaction between ISO/IEC 27701:2019 and the GDPR. This, however, can be regarded as a limitation of the research, since the actual interaction in practice is not reflected in literature. This is primarily caused by the fact that both documents are fairly new and the fact that few organizations are yet ISO/IEC 27701:2019 certified. While literature review certainly is an important part, it should be acknowledged that a more profound research would have been accomplished through interviewing experts in the field of ISO/IEC or interviewing European organizations that are certified based on ISO/IEC 27701:2019. Using this thesis as a basis elaborating on the discourse on this subject in the literature, a further study on the interaction between ISO/IEC 27701:2019

and the GDPR will be able to generate a deeper and more specific understanding on this, when such interviews are conducted.

6. Literature overview

A distinction can be made between primary and secondary sources, which have been used to answer the questions. Below are all sources with full reference based on the Oscola (Oxford University Standard, 4th edition) guide.

6.1. Primary sources

- 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 [2016] OJ L119/1.
- Agreement on Technical Barriers to Trade [1995].
- ISO/IEC 27701:2019.
- ISO/IEC 27001:2013.
- ISO/IEC 27002:2013.
- ISO/IEC 29100:2011.
- ISO/IEC 27000:2018.

6.2. Secondary sources

The secondary sources can be divided into a section covering books, journals, conference papers, websites and 'other documents'.

6.2.1. Books

- J. Gibb & M. Farren, *Who's Watching You?* (The Disinformation Company 2007).
- G. Orwell, *Nineteen Eighty-Four* (Secker & Warburg 1949).
- Roger Brownsword and Morag Goodwin, *Law and the Technologies of the Twenty-First Century* (1st edn, Cambridge University Press 2012).
- F. Cafaggi, 'Transnational Private Regulation: Regulation Global Private Regulators' in S. Cassesse (ed), *Research Handbook on Global Administrative Law* (1st edn, Edward Elgar Publishing 2016).
- L. Senden, 'Smart Public-Private Complementarities in the Transnational Regulatory and Enforcement Space' in J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019).
- Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (1st edn, Princeton University Press 2011).

- J. Braithwaite, *Regulatory Capitalism: How It Works, Ideas for Making It Work Better* (Edward Elgar Publishing 2008).
- D. Vogel, *The Market for Virtue: The Potential and Limits of Corporate Social Responsibility* (Brookings Institution Press 2005).
- J. van Erp, M. Faure, A. Nollkaemper & N. Philipsen (eds), *Smart Mixes for Transboundary Environmental Harm* (Cambridge University Press 2019).
- W. Kuert, 'The Founding of ISO', in ISO, *Friendship Among Equals. Recollections from ISO's First Fifty Years* (ISO 1997).
- J. Tate, 'National Varieties of Standardization' in P.A. Hall & D. Soskice (ed), *Varieties of Capitalism. The Institutional Foundations of Comparative Advantage* (Oxford University Press 2001).
- M. Rhahla, S. Allegue & T. Abedllatif, 'A Framework for GDPR Compliance in Big Data Systems' in S. Kallel, F. Cuppens, N. Cuppens-Boulahia & A. Hadj Kacem (eds), *Risks and Security of Internet and Systems* (Springer 2019).
- Kamara & P. de Hert, 'Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a Reformed Landscape' in R. Rodrigues & V. Papakonstantinou (eds), *Privacy and Data Protection Seals* (Information Technology and Law Series 28, Springer 2018).
- C. Hood, H. Rothstein & R. Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxfort University Press 2001).

6.2.2. Journals

- B.J. Koops & R. Leenes, ''Code' and the Slow Erosion of Privacy' (2005) 12 Michigan Telecommunications and Technology Law Review 115, 176 – 177.
- S.D. Warren & L.D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
- W. Unger, 'Reclaiming Our Right to Privacy By Holding Tech. Companies Accountable' (2020) 27 Richmond Journal of Law & Technology 1.
- T. Bartley, 'Transnational Governance as the Layering of Rules: Intersection of Public and Private Standards' (2011) 12 Theoretical Inquiries in Law 517.
- F. Cafaggi, 'New Foundations of Transnational Private Regulation' (2011) 38 Journal of Law and Society 20.

- N. Jägers, ‘Regulating the Private Security Industry: Connecting the Public and the Private Through Transnational Private Regulation’ (2012) 6 Human Rights & International Legal Discourse 56.
- N. Gunningham & D. Sinclair, ‘Regulatory Pluralism: Designing Policy Mixes for Environmental Protection’ (1999) 21 Law & Policy 49.
- D. Levi-Faur, ‘The Global Diffusion of Regulatory Capitalism’ (2005) 598 The ANNALS of the American Academy of Political and Social Science 12.
- P. Verbruggen ‘Gorillas in the Closet? Public and Private Actors in the Enforcement of Transnational Private Regulation’ (2013) 7 Regulation & Governance 512.
- M. Amengual, ‘Complementarity Labor Regulation: The Uncoordinated Combination of State and Private Regulators in the Dominican Republic (2010) 38 World Development 405.
- B. Cashore, G. Auld, S. Bernstein & C. McDermott, ‘Can Non-State Governance ‘Ratchet Up’ Global Environmental Standards? Lessons from the Forest Sector’ (2007) 16 Review of European, Comparative & International Environmental Law 158.
- C.F. Sabel & J. Zeitlin, ‘Learning form Difference: The New Architectures of Experimentalist Governance in the European Union’ (2008) 14 European Law Journal 271.
- C. Coglianese & D. Lazer, ‘Management-Based Regulation: Prescribing Private Management to Achieve Public Goals’ (2003) 37 Law & Society Review 691.
- R. Gellert, ‘Understanding the Notion of Risk in the General Data Protection Regulation’ (2018) 34 Computer Law & Security Review 279.
- C. Quelle, ‘Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach’ (2019) 9 European Journal of Risk Regulation 502.

6.2.3. Conference papers

- V. Chang, P. Chundury & M. Chetty, ‘“Spiders in the Sky”: User Perceptions of Drones, Privacy and Security’ (CHI ’17: CHI Conference on Human Factors in Computing Systems, Denver, May 2017).
- Psychoula, D. Singh, L. Chen, F. Chen, A. Holzinger & H. Ning, ‘Users’ Privacy Concerns in IoT based Applications’ (2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, Guangzhou, October 2018).
- M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne and M. Ylianttila, ‘5G Privacy: Scenarios and Solutions’ (2018 IEEE 5G World Forum (5GWF), Silicon Valley, July 2018).

6.2.4. Websites

- Cavoukian, 'Privacy and Drones: Unmanned Aerial Vehicles' (*Information and Privacy Commissioner of Ontario*, August 2012) <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-drones.pdf> accessed 10 January 2021.
- Ryan Chiavetta, '5G Raises Privacy Challenges and Opportunities' (*IAPP*, 16 April 2020) <https://iapp.org/news/a/5g-to-raise-privacy-challenges-and-opportunities/> accessed 21 July 2020.
- E. Baig, '5G is Speedy, But Does it Also Raise the Stakes on Privacy, Security, Potential Abuse?' (*USA TODAY*, 16 December 2019) <https://eu.usatoday.com/story/tech/2019/03/27/will-new-5-g-wireless-network-threaten-your-privacy/3032281002/> accessed 21 July 2020.
- 'Standards' (International Organization for Standardization) <https://www.iso.org/standards.html> accessed 5 May 2020.
- 'How and why the IEC was started', (*International Electrotechnical Commission*) <https://www.iec.ch/history/how-why-iec-was-started> accessed 25 November 2020.
- 'National Committees', (*International Electrotechnical Commission*) <https://www.iec.ch/national-committees> accessed 8 December 2020.
- 'Members', (*International Organization for Standardization*) <https://www.iso.org/members.html> accessed 8 December 2020.
- 'About Us', (*International Organization for Standardization*) <https://www.iso.org/about-us.html> accessed 26 November 2020.
- 'ISO in Figures 2019', (*International Organization for Standardization*) <https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/iso_in_figures/docs/iso-in-figures_2019.pdf> accessed 26 November 2020.
- 'IEC Technical Committees & Subcommittees', (*International Electrotechnical Commission*) <https://www.iec.ch/dyn/www/f?p=103:62:0::::FSP_LANG_ID:25> accessed 26 November 2020.
- 'What We Do', (*International Organization for Standardization*) <https://www.iso.org/what-we-do.html> accessed 26 November 2020.
- 'ISO/Council', (*International Organization for Standardization*) <https://www.iso.org/committee/55010.html> accessed 26 November 2020.

- 'Council', (*International Electrotechnical Commission*) <https://www.iec.ch/dyn/www/f?p=103:65:0::::FSP_ORG_ID,FSP_LANG_ID:3227,25> accessed 26 November 2020.
- 'ISO & IEC', (*CEN and CENELEC*) <https://www.cencenelec.eu/intcoop/StandardizationOrg/Pages/default.aspx> accessed 8 December 2020.
- 'Standardisation Policy', (*European Commission*) <https://ec.europa.eu/growth/single-market/european-standards/policy_en> accessed 18 January 2021.
- Kamara, '4 GDPR-Certification Myths Dispelled' (*IAPP*, 28 January 2020) <https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/> accessed 14 January 2021.
- 'ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements' (*ISO*) <https://www.iso.org/standard/54534.html> accessed 5 november 2020.
- 'ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls' (*ISO*) <https://www.iso.org/standard/54533.html> accessed 5 november 2020.
- 'ISO 27701, an international standard addressing personal data protection' (*CNIL*, 2 April 2020) <https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection> accessed 5 November 2020.

6.2.5. Other documents

- T.E. Lambooij, 'Corporate Social Responsibility. Legal and Semi-Legal Frameworks Supporting CSR. Developments 2000 – 2010 and Case Studies' (PhD Thesis, Leiden University 2010).
- F. Cafaggi & A. Renda, 'Public and Private Regulation: Mapping the Labyrinth' (2012) CEPS Working Document 370/2012, 16 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2156875> accessed 20 November 2020.
- U.S. House of Representatives, Committee on Science (Hearing), *Standards-Setting and United States Competitiveness* (Serial No. 107-21, 2001).
- E. Lachaud, 'ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification' (15 January 2020) <https://poseidon01.ssrn.com/delivery.php?ID=925001095006090087092121029125102031105056038064034051074003124118100095026073102029063026017056028045033096019081114095068073061007010028093003086024081067072010067093060076123115086079

061050161001040690920910240750020150730661150711010990740930970 97&EXT=pdf> accessed 13 January 2021.

- Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010).
- Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union' (Communication) COM (2010) 609 final.
- Commission, 'Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679' (Final Report, February 2019).
- EDPB, 'Guidelines 1/2018 on certification and identifying criteria in accordance with Articles 42 and 43 of the Regulation' (Version 3.0, 4 June 2019).