Chapter 1
Data Protection Around the World: An Introduction

Elif Kiesow Cortez

Contents

1.1 Introduction ................................................................. 1
1.2 Overview ..................................................................... 3
References ......................................................................... 6

Abstract This book serves as an up-to-date resource on the applications and practice-relevant examples of data protection laws in different countries. The snapshot of privacy laws and practices from a varied set of jurisdictions it provides reflects national and international contemporary issues regarding the processing of personal data. The ever-increasing emergence of privacy violations, due to evolving technology and new lifestyles linked to an intensified online presence of ever more individuals, has required the design of a novel data protection and privacy regulation. The contributors to this book offer an in-depth analysis of the national data protection legislation of various countries across different continents, not only including country-specific details but also comparing the idiosyncratic characteristics of these national privacy laws to the EU General Data Protection Regulation (GDPR). Valuable comparative information on data protection regulations around the world is provided in one concise volume.

Keywords Data protection around the world · GDPR · Privacy · European data protection · Privacy law · Right to privacy

1.1 Introduction

Evolving technology and new lifestyles linked to an intensified online presence of ever more individuals have put privacy increasingly at risk. An individual’s personal
data is an extremely profitable resource for companies and a tool to increase government surveillance. It is very difficult to balance these interests against an individual’s fundamental right to privacy and protection of personal data. People have little control over their personal data and sometimes even lack knowledge of which personal data is collected and when and what conclusions governments and companies can draw from collected personal data. The resulting information asymmetry between individuals and the companies that collect their data makes it easy for companies to infringe individual fundamental rights without individuals even knowing the infringement has occurred. To address this problem, the EU General Data Protection Regulation (GDPR) was adopted in April 2016 and came into force in May 2018 to supersede the outdated Data Protection Directive 95/46/EC of 1995. The drafters of the GDPR announced that it would cohere to the EU Digital Single Market Strategy, which aims to create incentives for digital networks and services to flourish by providing trustworthy infrastructure and effective regulations. The efforts aimed at supporting the privacy respecting practices through the GDPR enforcement also meant that administrative fines were issued in the first year of the GDPR and several organizations updated their privacy policy to become compliant with the GDPR. A significant part of this was to create the conditions that would lead EU citizens to trust digital services enough to use them. GDPR has been seen as having created new control mechanisms that allow individuals to decide how much data they are willing to share and with whom.

Following the GDPR’s first application year, the UK Information Commissioner’s Office reported that individuals were taking more control of their data. For example, between 25 May 2018 and 1 May 2019, the commissioner received 14,000 personal data breach reports, more than quadruple the 3000 the office received in the prior year. Likewise, supervisory authorities of 11 European economic area countries already imposed fines under the GDPR amounting to a total of approximately €56 million fines. GDPR has extraterritorial application as well, which has led the European Data Protection Supervisor to describe it as the “gold standard” for the protection of personal data. However as national legislation around the world has increasingly defined the right to protection of personal data, the stringency of the EU-based gold standard led to many objections from lobbying groups. Academics and practitioners struggle to pinpoint applicable laws, especially for transnational cases that might violate the right to the protection of personal data.

Regulating the right to protection of personal data requires attention to the normative dimensions of privacy as a concept. There are benefits as well as risks in the

---

1European Commission 2015.
2European Union Agency for Fundamental Rights 2019.
3Information Commissioner’s Office 2019.
4European Data Protection Board 2019.
5Buttarelli G (April 2016) The EU GDPR as a clarion call for a new global digital gold standard. https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_fr. Accessed 25 February 2020.
6Schwartz 2013.
large-scale collection and processing of personal data.\footnote{For a discussion of the economic value of right to privacy see Posner 1981, 1983. For counterarguments, see Solove 2007.} The benefits include a more connected society, fast access to products and services and receiving customized, tailored suggestions for products and services. Risks of commercial uses of personal data include being profiled and having limited access to products and services due to the relevant profiling. Law enforcement uses may have greater risks, which have led to right to privacy discussions where significant attention was devoted to the potential *privacy vs. security trade-off*. As of early 2020, an important debate takes place with respect to governments’ objective to collect individual’s personal data regarding coronavirus infections. Especially relevant in this context is individual’s right to protection of their health data which under the GDPR is categorized as sensitive personal data. This recent development showed that right to protection of personal data is also at the center of the discussion on potential *privacy vs. public health trade-offs*.

This book provides a snapshot of privacy laws and practices from a varied set of jurisdictions in order to offer guidance on national and international contemporary issues regarding the processing of personal data. It also serves as an up-to-date resource on the applications and practice-relevant examples of data protection laws in different countries. Our objective was to show the applications of the GDPR within European countries and a selection of national data protection laws from different continents with a focus on how the GDPR has influenced these laws. The jurisdictions covered in this book include European countries—Belgium, Estonia, France, Greece and the Netherlands—as well as Indonesia, Tanzania, Turkey, and United States.

The authors of this book offer an in-depth analysis of the national data protection legislation of various countries across different continents, not only including country-specific details but also comparing the idiosyncratic characteristics of these national privacy laws to the GDPR. Valuable comparative information on data protection regulations around the world is provided in one concise volume.

### 1.2 Overview

In Chap. 2, Els De Busser provides an overview of the application of data protection regulation in Belgium. As she explains, the Belgian Privacy Commission has taken a proactive approach to GDPR implementation. Indeed, Belgium created a special function within the government, the Secretary of State for Privacy (later Federal Minister), that oversees implementation. To explain the impact of this, Dr. De Busser describes how the country’s Privacy Commission became the Belgian Data Protection Authority and the high-profile case it subsequently brought against Facebook in 2015.

In Chap. 3, Kärt Saluuma-Leplik, Tanel Kerikmae and Nele Nisu cover GDPR implementation issues and related topics from an Estonian perspective, as Estonia is one of the recognized pioneers and leaders concerning modern digital society. The
authors explain the roots of Estonian data protection and provide an overview of the latest developments related to GDPR and case law in that matter. After clarifying how GDPR interacts with Estonian jurisdiction and the most notable differences and similarities, the authors conclude by highlighting the most prominent issues in Estonian jurisdiction regarding data protection regulations with a focus on e-governance.

In Chap. 4, Aurelien Lorange focuses on the data protection law and practices in France by providing a detailed overview on the policy origins and evaluation. The author highlights the importance of the role of the French Data Protection Authority, which received more competences and a territorial application than it had before the GDPR, leading to better definition of and maintenance of its role of controlling the regime of the most sensitive data (justice and police) and informing individuals of their rights with respect to their data. As Chap. 4 explains, the French Data Protection authority created many informative sources in the first application year of the GDPR and has since moved on to enforcement and increased cooperation with the other national authorities in charge of protection of personal data in the European Union.

In Chap. 5, Georgios Bouchagiar and Nikos Koutras deliver a detailed analysis of the data protection law in Greece. They provide an overview of case law of the Supreme Administrative Court and the Supreme Civil and Criminal Court, as well as indicating the relevant national laws and passages of the Constitution of Greece. They then explain the core concepts that have driven this body of law, such as “control” and “consent.” The analysis highlights the similarities and differences between the GDPR and Greek law. The conclusion examines the risks emerging from new technologies. It underlines ignorance and confusion that may affect people with respect to these issues, referencing data portability as a trust-enhancing tool that could strengthen controllership and promote transparency in the interests of data subjects.

In Chap. 6 Edmon Makarim explores Indonesia’s data protection regulations. He provides an overview of the data protection laws implemented by the Communication and Informatics Ministry Regulation No.20 in 2016 about personal data protection in e-systems. Chapter 6 also provides an in-depth analysis of the Bill for Personal Data Protection introduced in the Indonesian legislature in 2008, explaining how it responds to GDPR and existing information and communication laws in Indonesia.

The first section of Chap. 7 discusses the existing generic personal data protection regime in the Netherlands and recent and expected legislative changes in and related to this regime. Godelieve Alkemade and Joeri Toet then provide an informative overview of sector specific personal data protection legislation and explain key distinguishing elements of the Dutch personal data protection environment, focusing specifically on the latitude the GDPR provides member states for implementation or deviation. The chapter concludes with the authors’ expectations as to how GDPR will affect these prominent issues in the Netherlands.

In Chap. 8, Alex Makulilo offers an overview of the influence the GDPR on the Tanzanian data privacy law and practice. The author states that the Constitution of the United Republic of Tanzania provides for constitutional protection of individual privacy even if the country has no general data protection legislation. The country’s constitution states that all people are entitled to respect and protection of
their persons; the privacy of their own person, family, and matrimonial lives; and respect and protection of their residence and private communications. The author lays out the limitations of these rights and provides an in-depth analysis of whether these limitations align with the GDPR.

In Chap. 9, Başak Erdoğan dissects Turkey’s approach to personal data protection and compares it to the GDPR by analysing the current state of affairs after the adoption of Law no. 6698 on the Protection of Personal Data in 2016 and the establishment of the Turkish Data Protection Authority. The chapter analyses Turkey’s main laws and regulations and case-law with regard to the protection of personal data, then compares of Turkish data protection law with the GDPR. Following a review of prominent issues with regard to data protection in Turkey, the chapter concludes with discussing the possible application of the GDPR in Turkey and its impact on Turkish data protection law.

In Chap. 10, Muge Fazlıoğlu focuses on U.S. information privacy and data protection laws and compares them to the GDPR as well as discussing how the GDPR is likely to affect privacy and data protection in the United States in the years ahead. The author explains that U.S. privacy laws are “sectoral” in nature, meaning that businesses in different economic sectors are subject to different privacy rules and regulations, which differs from the EU’s omnibus approach to data protection. The author provides a thorough analysis regarding the interaction between the GDPR and U.S. law, the interplay between the right to be forgotten and the protection of speech and of the press provided by the First Amendment. The chapter concludes with insights on understanding the interaction of state-level consumer privacy laws, such as the California Consumer Privacy Act of 2018 and legislative efforts at the federal level.

In Chap. 11, Ambrogino Awesta first elaborates on the meaning and scope of the concept of privacy in the EU. Subsequently the applicability of privacy in relation to technologies that are employed for tracking and targeting in cyberspace is scrutinized. The author concludes by focusing on the impact of obligations that are imposed on digital enterprises by the new legal instruments and the actual effectiveness of these instruments in protecting and securing the privacy of users against the technologies deployed by digital enterprises.

In the final chapter, Elif Kiesow Cortez shares an overview of selected future challenges for the protection of personal data in the domains of automated decision making and artificial intelligence, blockchain technology, and also with respect to the newly emerged discussions on public health with regards to the coronavirus pandemic and contact tracing apps. The chapter focuses on providing an analysis of these three new and emerging areas based on the relevant guidelines of the European Data Protection Board.

The present volume aims to shed light on the fast-moving legal field of data protection regulation. It aims to provide practitioners and scholars alike with information on the distinct ways with which different jurisdictions across the globe approach this thorny subject whose relevance is expected to continue to grow, given the ongoing transformation towards more digital economies and the cultivation of social ties occurring increasingly via electronic means.
Parallel to the interaction of national privacy laws and the GDPR we are witnessing GDPR itself consolidating and evolving in response to unforeseen challenges linked to dynamic behavioral responses, external factors like the COVID-19 pandemic and interplay involving citizens and firms. The worldwide impact of the GDPR will likely not be fully uniform but rather adapted to and filtered through the national legal landscape of privacy laws in occasionally unexpected ways, yielding country-specific reactions and results. The present collection of chapters aims to illustrate how this process can take place in a variety of jurisdictions and what specific commonalities and potential frictions exist between GDPR and national legal privacy regimes.

References

European Commission (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: a digital single market strategy for Europe. https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-com2015-192-final. Accessed 25 February 2020
European Data Protection Board (2019) 2019 Annual report: working together for stronger rights. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_annual_report_2019_en.pdf. Accessed 25 February 2020
European Union Agency for Fundamental Rights (2019) The General Data Protection Regulation – One year on. Civil society: awareness, opportunities and challenges. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-gdpr-one-year-on_en.pdf. Accessed 25 February 2020
Information Commissioner’s Office (2019) GDPR: One year on, May 2019, Version 1.0. https://ico.org.uk/media/about-the-ico/documents/2614992/gdpr-one-year-on-20190530.pdf. Accessed 25 February 2020
Posner R (1981) The economics of privacy. Am Econ Rev 71(2):405–409
Posner R (1983) The economics of justice. Harvard University Press, Cambridge
Schwartz P (2013) The EU-US privacy collision: a turn to institutions and procedures. Harvard Law Rev 126:1
Solove D (2007) “I’ve got nothing to hide” and other misunderstandings of privacy. San Diego Law Rev 44:745

Dr. Elif Kiesow Cortez is a senior lecturer and researcher in data protection and privacy regulation in the International and European Law Program at The Hague University of Applied Sciences (THUAS), the Netherlands.