ASSER PRESS

Information Technology and Law Series | IT&LAW 29

EU Personal Data Protection in Policy and Practice

Bart Custers
Alan M. Sears
Francien Dechesne
Ilina Georgieva
Tommaso Tani
Simone van der Hof

Foreword by Kenneth A. Bamberger and Deirdre K. Mulligan

Springer

Information Technology and Law Series

Volume 29

More information about this series at http://www.springer.com/series/8857

Bart Custers · Alan M. Sears
Francien Dechesne · Ilina Georgieva
Tommaso Tani · Simone van der Hof

EU Personal Data Protection in Policy and Practice

ASSER PRESS

Springer

Bart Custers
Leiden Law School, eLaw
(Center for Law and Digital Technologies)
Leiden University
Leiden, The Netherlands

Ilina Georgieva
Leiden Law School, eLaw
(Center for Law and Digital Technologies)
Leiden University
Leiden, The Netherlands

Alan M. Sears
Leiden Law School, eLaw
(Center for Law and Digital Technologies)
Leiden University
Leiden, The Netherlands

Tommaso Tani
Leiden Law School, eLaw
(Center for Law and Digital Technologies)
Leiden University
Leiden, The Netherlands

Francien Dechesne
Leiden Law School, eLaw
(Center for Law and Digital Technologies)
Leiden University
Leiden, The Netherlands

Simone van der Hof
Leiden Law School, eLaw
(Center for Law and Digital Technologies)
Leiden University
Leiden, The Netherlands

ISSN 1570-2782 ISSN 2215-1966 (electronic)
Information Technology and Law Series
ISBN 978-94-6265-281-1 ISBN 978-94-6265-282-8 (eBook)
https://doi.org/10.1007/978-94-6265-282-8

Library of Congress Control Number: 2018962778

Published by T.M.C. ASSER PRESS, The Hague, The Netherlands www.asserpress.nl
Produced and distributed for T.M.C. ASSER PRESS by Springer-Verlag Berlin Heidelberg

Parts of this book are translations of Dutch-language texts in the report De bescherming van persoonsgegevens - Acht Europese landen vergeleken, published by Sdu Uitgevers, The Hague, The Netherlands, ISBN 9789012400862, 2017.

This T.M.C. ASSER PRESS imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Series Information

The *Information Technology & Law Series* was an initiative of IT*e*R, the national programme for Information Technology and Law, which was a research programme set-up by the Dutch government and The Netherlands Organisation for Scientific Research (NWO) in The Hague. Since 1995 IT*e*R has published all of its research results in its own book series. In 2002 IT*e*R launched the present internationally orientated and English language *Information Technology & Law Series*. This well-established series deals with the implications of information technology for legal systems and institutions. Manuscripts and related correspondence can be sent to the Series' Editorial Office, which will also gladly provide more information concerning editorial standards and procedures.

Editorial Office

Foreword

When we wrote *Privacy on the Ground* several years ago, we did so with the aim of painting a picture of how people charged with protecting privacy and personal data actually do their work and what kinds of regulation, as well as other internal and external forces, effectively shape their behaviour. We compared five countries and discovered that countries with more ambiguous legislation—Germany and the USA—had the strongest privacy management practices, despite very different cultural and legal environments. They embedded privacy into business and risk management practices and built privacy into products, not just into legal texts. The more rule-bound countries—like France and Spain—trended instead towards compliance processes, not embedded privacy practices. Comparing privacy and personal data protection in practice thus revealed best practices, provided guidance to policymakers, and offered important lessons for everyone concerned with privacy and personal data protection.

In many ways, *EU Personal Data Protection in Policy and Practice* is a continuation of our work, as it examines the practical implementation of privacy and data protection practices on the ground. While the countries analysed differ from those that we examined, the findings in this book confirm our previous results regarding the overlapping countries (the UK, Germany and France). Additionally, this book examines several additional countries in Europe such as Ireland, Sweden, Romania, Italy and the Netherlands, enriching our previous results with insights from more countries. Altogether, this provides an interesting cross section of countries from several regions in Europe with differing legal systems, economies and cultural backgrounds, resulting in different approaches towards privacy and personal data protection.

EU Personal Data Protection in Policy and Practice is based on a myriad of sources, including consultations with representatives from data protection authorities, civil society and academics that specialize in data protection. Not only are the legal bases for privacy and personal data protection examined in this book, but also the practical implementation of the laws, the enforcement by data protection authorities, the attitudes of the public in response to regulation and the effectiveness of the protection the legislators envisioned. While the approach is distinct from the

in-depth qualitative approach we chose, the combined methods used provide a comprehensive overview of data protection frameworks across the European Union.

This book provides an interesting snapshot of these privacy and personal data protection frameworks and their practical implementation under the EU Data Protection Directive (DPD), with references to the EU General Data Protection Regulation (GDPR), which entered into force in May 2018. As such, *EU Personal Data Protection in Policy and Practice* is a vital resource and an interesting point of comparison for further research and study into the development and implementation of data protection laws and regulations on the ground under the GDPR, especially in Europe, as well as further abroad.

Berkeley, USA

Kenneth A. Bamberger
Berkeley Center for Law and Technology
University of California, Berkeley

Deirdre K. Mulligan
Berkeley Center for Law and Technology
University of California, Berkeley

Contents

About the Authors

Bart Custers holds Ph.D., M.Sc., LLM and is Associate Professor and Director of Research at eLaw, Center for Law and Digital Technologies at Leiden University. He has a background in both law and physics and is an expert in the area of law and digital technologies, including topics like profiling, big data, privacy, discrimination, cybercrime, technology in policing and artificial intelligence. He is a seasoned researcher and project manager who acquired and executed research for the European Commission, NWO (the National Research Council in the Netherlands), the Dutch national government, local government agencies, large corporations and SMEs. Until 2016, he was the head of the research department on crime, law enforcement and sanctions of the scientific research centre (WODC) of the ministry of security and justice in the Netherlands. Before that, he worked for the national government as a senior policy advisor for consecutive ministers of justice (2009–2013) and for a large consultancy firm as a senior management consultant on information strategies (2005–2009).

Dr. Custers published three books on profiling, privacy, discrimination and big data, two books on the use of drones and one book on the use of bitcoins for money laundering cybercrime profits. On a regular basis, he gives lectures on profiling, privacy and big data and related topics. He has presented his work at international conferences in the USA, Canada, China, Japan, Korea, Malaysia, Thailand, Africa, the Middle East and throughout Europe. He has published his work, over a hundred publications, in scientific and professional journals and in newspapers.

Alan M. Sears is a Researcher at Leiden University's eLaw Centre for Law and Digital Technologies, where he conducts research as part of a team within the EU-funded e-SIDES Project, which sets out to explore the ethical, social and legal challenges surrounding privacy-preserving big data technologies. His research interests include freedom of expression and privacy/data protection online, and he has also researched issues ranging from Internet governance to intermediary liability and telecommunications regulations (particularly net neutrality and zero rating). Alan has worked as a researcher with Article 19 Mexico and Central America and with Derechos Digitales in Chile, as a law clerk and researcher for Justice

Madlanga of the Constitutional Court of South Africa and as a Google Policy Fellowship with Fundación para la Libertad de Prensa (FLIP) in Colombia. He received a B.A. in Psychology and Business Administration from Baylor University, a J.D. from the University of Notre Dame and an LLM in Law and Digital Technologies from Leiden University.

Dr. Francien Dechesne works as a Researcher at Leiden University Law School's Center for Law and Digital Technologies (eLaw), the Netherlands. She investigates the interaction between information technology and fundamental values in society. With a background in mathematics, computer science and philosophy, she analyses how values are either effectuated or compromised through the technology and to which extent technological design can play a role in preventing or solving ethical problems. She is particularly interested in cybersecurity, privacy, and fairness and accountability in data analytics. She currently works on the SCALES-project on responsible innovation with data.

Ilina Georgieva is a Ph.D. candidate of 'The Hague Programme for Cyber Norms' at Leiden University's Institute of Security and Global Affairs (ISGA). In her research, she is focusing on the capacity of networks of intelligence agencies to shape the international community's perception of what is normal in cyberspace. For that purpose, she investigates the networks' normative power by looking into their practice of foreign electronic surveillance. Prior to joining ISGA, she served as a researcher on the Sweetie Project and on the European DPC Project at eLaw, the Center for Law and Digital Technologies at Leiden University. Before joining eLaw's team, she worked as an editor at the Utrecht Journal of International and European Law (October 2013–September 2014). She was also a part of Heidelberg University's Cluster of Excellence 'Asia and Europe in a Global Context' (December 2012–August 2013) and of the Austria Institute for European and Security Policy (summer of 2012) in her capacity as a research assistant. From January 2009 to June 2010, she worked at the Max Planck Institute for Comparative Public Law and International Law in Heidelberg. She also served as a Senior Research Associate and later on as a Counsel for the Public International Law and Policy Group (PILPG) from September 2014 to October 2016.

Tommaso Tani is an Italian legal expert on IT and data protection. After studying computer engineering, he completed his law studies in Alma Mater Studiorum University of Bologna in 2015 with a thesis on Media and the Right to be Forgotten. After two years of litigation practice in a local law firm, he joined the Advanced Master in Law and Digital Technologies in Leiden University and graduated with a thesis about 'Legal Responsibility for False News', which has been presented at the Southwestern Law School in California and is being published on the Journal of International Media & Entertainment Law. He is now working as Privacy Counsel for Europe in a multinational IT corporation.

Simone van der Hof is the Director of the Center for Law and Digital Technologies (eLaw) at Leiden Law School, programme director of the Advanced Studies Programme in Law and Digital Technologies and one of the directors of the Leiden Law School research profile area interaction between legal systems. She coordinates and teaches various courses, amongst which 'Regulating Online Child Safety' (Master Youth Law), 'Digital Child Rights' and 'Digital Government' (both Advanced Master Law and Digital Technologies), 'The Rights of the Child in the Digital World' (Advanced Master International Children's Rights). She is a key lecturer at the Cyber Security Academy. Simone's particular academic interest is in the field of privacy and data protection, children's rights in the digital world and the regulation of online child safety. She was involved in the Sweetie 2.0 project on online webcam child sex abuse, commissioned by children's rights organization Terre des Hommes as well as a project on the levels of protection of personal data of European citizens commissioned by WODC (Research and Documentation Centre of the Ministry of Justice and Security). She participates in the SCALES project (big data and privacy) and leads the ethics by design work package of the Game Changers Project on the development of health games for children. Simone is part of the EU Kids Online III Dutch research team and the deputy chair of the NICAM complaints committee dealing with complaints on age classification for television and movies ('De Kijkwijzer'). She is a member of the Leiden Center for Data Science and the Advisory Board of the SIDN fund for innovative internet projects as well as the European Law and Technology Network. Moreover, she is the chair of the editorial board of the T.M.C. Asser Press IT & Law Series.

Summary

As of May 2018, the protection of personal data in the European Union (EU) is regulated by the General Data Protection Regulation (GDPR, Regulation 2016/679). Prior to that, the EU legal framework was already harmonized via the EU Data Protection Directive (DPD, Directive 95/46/EC). The legal framework determines the rights and obligations of persons whose data are collected and processed (data subjects) and for companies and governments that collect and process these personal data (data controllers and processors). The GDPR, just like its predecessor the DPD, contains many open norms. This offers room for different approaches towards the interpretation, implementation and enforcement of the legal framework. Hence, despite a strongly harmonized legal framework across the EU, much of the actual protection of personal data strongly depends on the policies and practices of individual EU member states.

Under the DPD, the differences in personal data protection policies and practices were mostly due to the legal implementation of the data protection framework. However, some differences were (and still are under the GDPR) due to additional sector-specific legislation and policies. Additionally, the open norms in legislation and the cultural differences in EU member states have resulted in different practices and policies across EU member states. These differences in the actual protection of personal data raise the question as to which country has the best policies and practices for protecting personal data, which is an important aspect of the protection of privacy in modern times.

This book presents a study in which personal data protection policies and practices across the EU are compared with each other. A selection of eight different EU member states is used to compare not only 'laws on the books', but also 'laws in practice'. This study is based on material from a previous study, in which the level of personal data protection in the Netherlands was determined. This book presents a much wider range of materials, now for the first time accessible for an international audience, in which the Netherlands is not the central focus point, but rather the relative positions of various European countries are compared. The research results show areas for improvement in the protection of personal data,

particularly data protection policies and practices, for individual EU member states. The central research question of this study is:

What is the position of different countries with regard to the protection of personal data in comparison with other EU member states?

This question was addressed by comparing different EU member states on the following topics: (1) the general situation regarding personal data protection, (2) the national government's policies regarding personal data protection, (3) national laws and regulations regarding personal data protection, (4) the practical implementation of legislation and policies and (5) the organization of supervisory authorities and actual enforcement. These topics were further divided into a total of 23 aspects of comparison. For the general situation, these aspects are internet use, control, awareness, trust, protective actions, national politics, media attention, data breaches and civil rights organizations. For national government policies, these are national policies and Privacy Impact Assessments, privacy and data protection in new policies, societal debate and information campaigns. For laws and regulations, these are implementation of the EU directive, sectoral legislation, self-regulation and codes of conduct. For implementation, these are privacy officers, security measures and transparency. For regulatory authorities and enforcement, these are supervisory authorities, main activities, the use of competences and reputation. All 23 aspects were compared between a total of eight EU member states: The Netherlands, Germany, Sweden, the UK, Ireland, France, Romania and Italy. The comparison of privacy and data protection regimes across the EU shows some remarkable findings, revealing which countries are front runners and which countries are lagging behind in specific aspects. With the group of countries compared in this research, Germany is front runner in most aspects, and Italy and Romania are at the other end of the spectrum for many aspects. Most of the other countries perform around or above average, depending on the particular aspect that is considered. For instance, the Netherlands is a leader regarding data breach notification laws and Privacy Impact Assessments. Ireland has recently become the front runner regarding the budgets for its data protection authority (DPA) and the number of employees serving at the DPA. At the same time, the Irish people are the least aware of the use of personal information by website owners.

In Ireland and Romania, there is hardly any political debate on privacy and data protection issues. The political debate in Sweden may not be the fiercest, but it could be characterized as perhaps the broadest, in the sense that economic aspects, societal aspects and human rights aspects all play a role in the Swedish political debate, whereas only one of these aspects is focused on in most of the other countries. In terms of media attention for privacy and data protection issues, Sweden and Italy have lower levels of media attention and Romania very little media attention, but other countries show high levels of media attention.

Civil rights organizations are more professional, better equipped, and more influential in the UK and Germany and, to a lesser extent, in France. However, in countries like Sweden and Romania, civil rights organizations have limited budgets

and influence. For instance, the Swedish organization DFRI mainly operates on the basis of volunteers.

Privacy Impact Assessments (PIAs) were not mandatory in most countries prior to the GDPR. An exception, to some extent, is France, where a legal obligation for data controllers to map the risks of processing personal data already existed. However, PIAs are not mandatory for new legislation or regulation in France. In the Netherlands, the situation is more or less the opposite: data controllers were not under any obligation to perform PIAs prior to the GDPR, but the national government has the duty to perform PIAs for legislative proposals that involve the processing of personal data (which is not required in the GDPR). In other countries, like the UK and Italy, the data protection authorities have issued guidelines for executing PIAs. In some countries, like the UK and France, models and standards for PIAs are available, and guidance is offered by the DPAs.

Differences in the implementation of the Data Protection Directive into national legislation are very small in the countries investigated: although EU member states are allowed to implement more provisions than those mentioned in the EU Data Protection Directive, only a few countries implemented such additional provisions for further protection. Typical examples are breach notification laws in the Netherlands, data protection audits in Germany, privacy by design methods in the UK and special provisions for healthcare data and children in France. Many countries introduced additional, more specific sectoral legislation in many areas, however.

Germany has by far the largest number of privacy officers and is the only country in which a legal obligation exists in particular situations to appoint a privacy officer. Romania has virtually no privacy officers. Since privacy officers were not mandatory in most countries prior to the GDPR, there are no data available to compare. Moreover, transparency on personal data processing practices is low in all countries investigated.

The resources of the DPAs are comparable in many of the countries investigated, but the DPAs in Germany and Ireland have relatively (i.e. in comparison with their GDP) the largest budgets. Romania has the smallest budget. Most of the DPAs manage to get comparable amounts of employees for their budgets. Only Romania and the UK manage to employ considerably more employees within the available budgets. In Italy, the number of employees of the DPA is relatively low in comparison with the DPA's budget. In comparison with the number of people in each country, Ireland and Germany have the most employees serving in their DPAs.

The research results presented in this book offer many opportunities for policymakers, legislators, data controllers and data protection authorities throughout Europe and abroad to learn from experiences, practices and choices made in other countries. It shows that although the protection of personal data largely was harmonized within the EU by Directive 95/46/EC, many differences existed in the actual protection of personal data. Even though the protection of personal data is further harmonized by the General Data Protection Regulation (GDPR) since 2018, it may be expected that differences in national laws and practices will continue to exist. Hence, we believe this research should be replicated after the GDPR has been in force for a few years.

Chapter 1
Introduction

1.1 Scope and Context

Increasing numbers of people are concerned about their privacy. This is a worldwide trend, which may be due to increased numbers of people who are active on social media and technological developments that enable or even force people to perform more and more actions and transactions online. People indicate that they have limited knowledge about who is processing their personal data and for which purposes.[1] Also, people experience limited control over their personal data.[2]

Since technological developments take place on an international level rather than on a national level, the European Commission adopted the General Data Protection Regulation (GDPR),[3] which is in force as of May 2018. This regulation replaced the 1995 Data Protection Directive (DPD)[4] that already harmonized the protection of personal data in the European Union. In comparison with the DPD, the GDPR is directly binding on all EU residents, companies, and (most) government agencies. It also contains several new elements for data subjects (such as a right to data portability and the right to be forgotten) and new obligations for data controllers (such as data breach notifications, mandatory data protection officers, Data

[1] Only two out of 10 EU citizens indicate that they are informed on which personal data is collected about them and what happens with these data. Eurobarometer 431 2015, p. 81.

[2] Only 15% of EU citizens indicate that they have full control over the personal data they put online. At the same time, 31% indicate that they have no control whatsoever. Some control is experienced by 50%. Two out of three EU citizens indicate that they are concerned about this lack of control over their personal data. Eurobarometer 431 2015, pp. 9, 12.

[3] 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 (General Data Protection Regulation).

[4] DIRECTIVE (EU) 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

B. Custers et al., *EU Personal Data Protection in Policy and Practice*,
Information Technology and Law Series 29,
https://doi.org/10.1007/978-94-6265-282-8_1

Protection Impact Assessments and Data Protection by Design). Another very important aspect of the GDPR is the possibility for supervisory authorities to impose administrative fines in the case of non-compliance. These fines can be considerable, to a maximum of 10 or 20 million euros (depending on the type of violation) or, in the case of a company, up to 2 or 4% of the total worldwide annual turnover of the preceding financial year, whichever amount is higher.[5] This obviously raises concerns for organizations about whether they are completely compliant with the GDPR.

The introduction of the GDPR clearly is an attempt to reinforce data subject rights. Stronger data subject rights, it is hoped, will increase levels of control over their personal data (or at least perceived levels of control), which in turn may increase trust in the data economy. At the same time, by increasing the harmonization of data protection law within the EU, the GDPR aims to further facilitate the transfers of personal data within the EU, which also is an attempt to advance the data economy.[6]

It is clear that in most areas of society legislation sets the level of protection that residents actually have. In the area of privacy and data protection, the GDPR sets the levels of protection for EU residents. The GDPR predominantly determines the legal framework for rights and obligations of persons whose data are collected and processed (data subjects) and for companies and governments that collect and process these personal data (data controllers). The actual protection, however, does not only depend on the legal framework, but also on the actual implementation and interpretation of the legislation and the ways in which it is enforced by courts and Data Protection Authorities (DPAs). As many scholars already have pointed out, there are many forces beyond the law that affect human behavior. For instance, IT law professor Lawrence Lessig distinguishes four different modalities of regulation.[7] Besides the law, he identifies norms, the market and architecture as regulating modalities. An action may be legal, but nevertheless considered unethical or impolite (such as smoking, adultery or stigmatization). In the case of personal data, which represent monetary value,[8] data controllers may have many business and market related incentives to collect and process data in particular ways. Architecture, including the design of online environments, enables or disables particular behavior (such as obligations to complete a form before you can continue on a website or to accept all terms and conditions before being able to register an account). Obviously, the law must to be complied with, but within the confines of the legal framework, the other regulating modalities clearly influence the practical ways in which personal data are collected and processed.

The legislation on privacy and the protection of personal data contains many open norms that need further translation and elaboration into workable,

[5] General Data Protection Regulation, Article 83(4) and (5).

[6] Custers and Bachlechner 2018.

[7] Lessig 2006.

[8] Malgieri and Custers 2017. See also Prins 2004; Purtova 2015.

sector-specific, and context-specific rules and practices. A typical advantage of this approach is that the legislation is more technology neutral, depending less on how and when technology further evolves. Another advantage of these open norms is that each case or situation – for instance, in specific sectors of society – can be judged on a case-by-case basis, allowing for modifications and further interpretation where necessary. As such, EU member states are encouraged to view the data protection legislation as a minimum level of protection that is provided, on top of which additional legislation can be created where it is considered necessary.

As a result of differences in legal systems and cultures, the *legal* implementation of the Data Protection Directive varied across EU member states. For the legal implementation of the GDPR, some countries may also choose to draft additional legislation, for instance, for specific sectors of society. Similarly, open norms combined with cultural differences also result in different *practical* implementations of the protection of personal data in EU member states, such as different interpretations of the legal provisions and different levels of enforcement. Although the GDPR aims to further harmonize law and practice, it may be expected that the differences that existed between countries under the DPD, in both the legal and the practical implementation, will continue to exist under the GDPR.

In their groundbreaking book,[9] Privacy on the Ground, US law professors Kenneth Bamberger and Deirdre Mulligan compare the different ways in which countries apply the legal rules for the protection of privacy and personal data protection.[10] They compare Germany, Spain, France, the United Kingdom and the United States. Even though the legal framework in the EU was substantially harmonized two decades ago, they demonstrate that there is considerable variation on the ground. Their comparison shows that in Spain, privacy and the protection of personal data is mainly regarded as legal text and an administrative burden. In France, protection of personal data was prescribed by the regulator, which led to diminished attention and resources within firms and fostered a compliance only mentality. By contrast, in Germany and the United States activist privacy regulators made firms responsible for determining what privacy protection required driving corporate attention and resources toward the task. In the United Kingdom, privacy was largely viewed as risk management, but the level of resources allocated was below that of the United States and Germany. In Germany and the United States, privacy professionals appeared to have the strongest approach towards privacy management. Particularly in the United States, there is a surprisingly deep chasm between privacy law in the books and privacy practice on the ground. In Germany, the focus is on an ethical and human rights-based approach of privacy and data protection law, whereas in the United States, the focus is on a reputation-based approach. Privacy is progressively becoming a strategic topic for organizations,

[9] Earlier work includes: Flaherty 1989; Bennett 1992.

[10] See also Mulligan and Bamberger 2015.

going beyond merely compliance issues: privacy is increasingly seen as a function of social license and corporate responsibility.[11]

Although some scholars may disagree,[12] it may be argued that the EU legislation for personal data protection (both the DPD and the GDPR) focus on procedural fairness rather than substantive fairness. The entire legal framework is based upon the so-called OECD principles for the fair processing of personal data.[13] These principles focus on issues like transparency, data quality, accountability and use and collection limitation. However, they do not address the fairness of the outcome of data analytics, such as profiling, algorithmic decision-making, fake news, nudging, etc. In fact, companies can be entirely compliant with EU data protection law, and still people may perceive interference with their privacy. Also, people feel concerned about their privacy online, but do not act in ways that confirm to these concerns – the so-called privacy paradox.[14] Hence, from the perspective of (substantive) fairness, privacy and personal data protection require more than only compliance with legislation.[15] For this reason, some scholars are already looking into other areas of law,[16] such as consumer law,[17] intellectual property law, anti-discrimination law[18] and even competition law.[19] Many of these areas of law also determine the extent to which personal data is protected, but within the EU they are not all harmonized.

The differences in the levels of protection of privacy and personal data raise the question as to which country best protects personal data (which is an important aspect of privacy). This question was also raised in the Dutch parliament. During the debate on the budgets for the Ministry of Justice in the Netherlands in November 2014, two members of parliament submitted a motion in which they requested the government to investigate the position of the Netherlands regarding the protection of privacy in comparison to other EU member states. The question underlying this request was how the Netherlands was doing: is the Netherlands a frontrunner or is it lagging behind? An answer to this question is required for the Dutch parliament to decide whether supplementing measures are required, and if so, which measures should be adopted.

As a result of these parliamentary proceedings, the Minister of Justice assigned the WODC, the research center of the Ministry of Justice to investigate the position of the Netherlands among other EU member states in the area of personal data protection. To limit the scope of this research, the focus was constrained to the

[11] Mulligan and Bamberger 2015. See also Cannataci 2016; Vedder and Custers 2009.

[12] Clifford and Ausloos 2017.

[13] See https://www.oecd.org/sti/ieconomy/49710223.pdf.

[14] Norberg et al. 2007.

[15] Vedder and Custers 2009.

[16] For an overview, see Ursic and Custers 2016.

[17] Helberger et al. 2017.

[18] Custers et al. 2013.

[19] Stucke and Ezrachi 2015.

protection of personal data as opposed to (the right to) privacy in a broad sense.[20] To ensure an objective comparison, the WODC split the research into two parts. In the first part, aspects for the envisioned comparison and a possible selection of countries for the comparison were mapped. This part was performed by TNO (the Netherlands Organization for Applied Scientific research – an independent research organization in the Netherlands that focuses on applied science) and published in 2015.[21] This report provided the guidance for the scope and design of the second part. This subsequent part concerned the actual comparison of eight countries on the aspects proposed by TNO, with the aim of positioning the Netherlands in relation to other countries. For the second part of the research, the WODC commissioned eLaw, the Center for Law and Digital Technologies at Leiden University. The results of the second part were published in 2017 (in Dutch).[22] The main results were also published in a journal paper so that an international audience could have access to the research results of the project.[23] After witnessing great international demand for more detailed research results, we decided to publish them in this book. However, this book is not a mere translation of the Dutch report, providing access to the research results for an international audience. The major difference is that the Dutch report puts the Netherlands in a central position, whereas in this book, we provide an international comparative approach, in which there is not a specific country as a central point of comparison, but rather show the interrelated positioning of all countries investigated. Another difference is that the Dutch report focused on an audience of legal professionals and policymakers, whereas this book also addresses an academic audience.

1.2 Research Questions

The differences in the extent to which personal data are protected raise the question as to which country best protects personal data (which is an important aspect of privacy). In this research, the personal data protection frameworks of eight different EU member states are compared.[24] This comparison shows the position of these different countries in relation to each other. Based on this research, areas for improvement concerning the protection of personal data can be identified in the event that a particular country provides less protection in comparison to other EU member states. The central research question of this study is:

[20] In other words, the focus is on informational privacy, rather than on spatial, relational, or physical privacy.

[21] Roosendaal et al. 2015.

[22] Custers et al. 2017.

[23] Custers et al. 2018.

[24] For the full report, see Custers et al. 2017.

What is the position of different countries with regard to the protection of personal data in comparison with other EU member states?

In order to be able to answer this question, the scope of this research needs to be limited and several choices need to be made. First, the protection of privacy, as indicated in the previous section, focuses on the protection of personal data (i.e., informational privacy). Second, some choices need to be made regarding the topics and aspects that will be compared. Third, choices need to be made in regards to the countries that will be included in the comparison.

For these choices, the abovementioned TNO research was used for guidance.[25] In that research, a framework was provided for the relevant topics to use in the comparison. To ensure a comprehensive qualitative comparison, it was suggested to include several cultural aspects as well as topics or aspects that the government cannot directly or indirectly influence, but that are nevertheless important to provide a deeper understanding of the protection of personal data and privacy in a particular country. The topics used in the comparison are (1) general situation regarding the protection of personal data, with a focus on awareness and trust, (2) government policies for personal data protection, (3) applicable laws and regulations, (4) implementation of those laws and regulations, and, (5) supervision and enforcement.

The suggested framework leads to the following subquestions that need to be answered for each country examined:

1. What is the general situation regarding personal data?
   This question leads to a description of how the protection of personal data is addressed, what role national politics have, what media attention exists for this topic, whether there are major incidents, and what role civil rights organizations play.
2. What are the national government's policies regarding personal data protection?
   This question concerns both policies that focus on the government itself and policies that focus on residents, and private companies and organizations. Both existing policies and policy development are taken into consideration. Furthermore, the role of the government in social debate is investigated and the extent to which the government provides information and raises awareness.
3. What are the national laws and regulations regarding personal data protection?
   On the basis of the 1995 EU Data Protection Directive, legislation throughout the EU was harmonized. The GDPR further harmonizes the protection of personal data.[26] This question maps the national laws and regulations that

[25] Roosendaal et al. 2015.

[26] Note that the GPDR revokes the DPD, but not the national legislation that implements the DPD. It is for each member state to decide whether such national legislation will be revoked or amended. In case the national legislation is not revoked or amended, it may serve as an addition to the GDPR provisions. In case of conflicting provisions, the GDPR obviously prevails over national legislation.

implemented the DPD and further details the legislation on lower echelons, such as sectoral legislation and self-regulation.

4. How are legislation and policies implemented in practice?
   This question focuses on the implementation of legislation and policies within organizations.[27] Here, it is investigated to what extent self-regulation and codes of conduct are used, whether there are privacy officers, to what extent organizations have taken technical and organizational measures and to what extent data controllers ensure transparency.
5. How are supervisory authorities organized and how is enforcement carried out?
   On the basis of EU data protection law, each EU member state is obliged to establish a supervisory authority in the area of personal data protection, the so-called Data Protection Authority (DPA). This question aims to provide an overview of the general characteristics of each DPA, the way in which the DPA positions itself, the extent and nature of enforcement actions and the perceptions that individuals and organisations have of the DPA.

These subquestions will be answered for each of the eight countries examined in this research, in Chaps. 2 through 9 of this book, respectively. For more details on how the countries were selected, see Sect. 1.3.2. By answering the questions above for each country, a description is provided of how each country performs with regard to the protection of personal data. Obviously, this is not yet a comparison between countries. However, the answers to these subquestions provide sufficient material to make the comparison described in the central research question. This question, "what is the position of different countries with regard to the protection of personal data in comparison with other EU member states?", is answered in the final chapter of this book (Chap. 10) by first comparing all countries examined on each aspect, showing which countries are doing well or not so well on each aspect, and then integrating these results, in turn showing which countries are frontrunners and which countries are lagging behind.

1.3 Research Approach

An international comparison requires decisions to be made on which aspects of the protection of personal data to compare as well as which countries to compare. After explaining the conceptual approach of this research (in Sect. 1.3.1), these topics will be discussed below (in Sects. 1.3.2 and 1.3.3).

[27] This is referring to "law in practice" or "law in action" as opposed to "law in the books". Or, in the words of Mulligan and Bamberger 2015: "privacy on the ground".

1.3.1 Conceptual Approach

This research is primarily qualitative in nature. The eight countries that were selected (see Sect. 1.3.3) are likely to provide a representative overview of the different stances that EU member states may have towards the protection of personal data. However, the number of countries examined in this research and the qualitative nature of the aspects compared allow only limited quantitative analysis of the collected material.

The focus of this research is on the protection of personal data (informational privacy), and not on the protection of privacy in a broad sense. Although a considerable number of the research questions have a legal nature, this is not typical legal or legally positivistic research. Rather, the focus is on the question of how the protection of personal data for EU residents is implemented in practice and experienced by them. Previous research has shown that the way people experience privacy does not always match the goals of legislation.[28] In this research, no extensive survey was used to investigate citizen perceptions, but previous EU-wide and national surveys performed by others were used (see Sect. 1.3.4).

This research does not provide a normative judgment on where a country should be positioned in comparison with other European countries, but it does provide suggestions for how a country could move in a specific direction regarding particular aspects of its data protection framework. This allows policymakers and legislators from different countries to decide for themselves which proposals for new policies or legislation may be appropriate.

Since the GDPR harmonizes EU legislation even further than the DPD did, the focus of this research will not primarily be on the GDPR (which is the same for each country), but rather on national legislation, including sector specific legislation, soft law and policies, as well as the practical implementation of legislation (which may differ for each country). Typical examples of sector-specific legislation are found in health law, criminal law, national security law and administrative law.

The underlying research of this book was performed from August 2016 until May 2017. During this period, the DPD was still in force, which is now replaced by the GDPR. Since this research does not always focus on the GDPR, this is not problematic, but rather helps to identify the difference between countries.

1.3.2 Aspects to Compare

Based on preparatory research,[29] five topics were determined as points of comparison in this research. These topics are: (1) general situation, (2) national government policies, (3) laws and regulations, (4) implementation, and (5) regulatory

[28] Custers et al. 2014.

[29] Roosendaal et al. 2015.

Table 1.1 The 23 aspects that are compared in this research, categorized into 5 topics

Topics	Aspects to compare (labels)
1. General situation	Internet use, control, awareness, trust, protective actions, national politics, media attention, data breaches, and civil rights organizations
2. National government policies	National policies and Privacy Impact Assessments, privacy and data protection in new policies, societal debate, and information campaigns
3. Laws and regulations	Implementation of the EU directive, sectoral legislation, self-regulation and codes of conduct
4. Implementation	Privacy officers, security measures, and transparency
5. Regulatory authorities and enforcement	Supervisory authorities, main activities, the use of competencies, and reputation

[*Source* The authors]

authorities and enforcement. Using an extensive questionnaire (see Appendix A) several questions were formulated on these five topics. Using desk research and expert consultation (see Sect. 1.3.3), these questions were answered for each country examined.

Finally, the collected material was clustered into 23 aspects or labels to compare, see Table 1.1. For the general situation, these are internet use, control, awareness, trust, protective actions, national politics, media attention, data breaches, and civil rights organizations. For national government policies, these are national policies and Privacy Impact Assessments, privacy and data protection in new policies, societal debate, and information campaigns. For laws and regulations, these are implementation of the EU directive, sectoral legislation, self-regulation and codes of conduct. For implementation, these are privacy officers, security measures, and transparency. For regulatory authorities and enforcement, these are supervisory authorities, main activities, the use of competencies, and reputation.

1.3.3 Countries to Compare

The research questions 1 through 5 put forward in the previous section were answered for a total of eight countries. The following countries were analyzed in this comparison: Germany, Sweden, the United Kingdom, Ireland, France, the Netherlands, Romania and Italy (see Fig. 1.1). The countries were selected to ensure a distribution on several selection criteria. These selection criteria are:

- Strict versus lenient approaches toward privacy protection
- Different approaches to personal data protection (due to cultural dimensions, the legal system, and the monistic/dualistic approach to international law)