AN AMERICAN'S GUIDE TO THE GDPR

MEG LETA JONES[†] & MARGOT E. KAMINSKI[††]

"[W]e feel a little bit betrayed in terms of [the] spirit of the GDPR . . ."

- Giovanni Buttarelli, European Data Protection Supervisor (2014–2019) (also known as "Mr. GDPR")[1]

ABSTRACT

The European Union's (EU) General Data Protection Regulation (GDPR) went into effect in May 2018. The GDPR impacts companies, individuals, and countries around the world. The GDPR is long and notoriously complex. A number of helpful, influential, and practical overviews exist. None of these overviews, however, have squarely taken aim at what we understand to be the most significant hurdles for U.S.-based readers. Understanding the GDPR requires knowing what it contains, how to read it, and a basic understanding of data protection and broader European law.

This Article aims to provide a concise one-stop-shop that includes necessary background context and pointers to reliable resources for GDPR novices, dabblers, and would-be experts based in the United States. We endeavor to correct common misconceptions about the GDPR: that it is primarily founded on individual consent (it is not); that it is about privacy (it is about data protection); and that it is primarily about individual rights and control (it is equally about risk management and corporate compliance). We hope to thus inform legal practice, legal scholarship, and ongoing policy conversations about the enactment of data privacy law in the United States.

---

† Associate Professor in Communication, Culture & Technology; core faculty in Science, Technology, and International Affairs; faculty fellow in the Ethics Lab; and affiliate faculty in the Institute for Technology Law & Policy at Georgetown University. Visiting affiliate faculty at the Brussels Privacy Hub at Vrije Universiteit Brussel.

†† Associate Professor of Law, Colorado Law School, Director of the Privacy Initiative at Silicon Flatirons Center. Thanks to Ronald Leenes and workshop participants for very helpful feedback at Privacy Law Scholars Conference (PLSC) Europe 2019, to Claudia Quelle for detailed comments and references, and to the juniors workshop at Colorado Law School. Thanks, too, to Thomas Streinz for extensive comments.

1. *Enforcing Data Privacy: A Conversation with Giovanni Buttarelli*, COUNCIL ON FOREIGN RELS. (Nov. 20, 2018), https://www.cfr.org/event/enforcing-data-privacy-conversation-giovanni-buttarelli. Mr. Buttarelli, described as "a colossus in our field" and a "beloved and much-admired member of the privacy and data protection community," passed away in 2019 at the age of 62. *In Memoriam: Giovanni Buttarelli, 1957–2019*, IAPP, https://iapp.org/resources/article/memoriam-giovanni-buttarelli/ (last visited Oct. 30, 2020).

TABLE OF CONTENTS

INTRODUCTION

The EU's GDPR went into effect in May 2018, binding EU Member States and impacting companies, individuals, and countries around the world.[2] The GDPR is a long and complex law, consisting of 99 Articles and a 173-section Preamble.[3] A number of helpful and influential overviews exist.[4] None of these overviews, however, have squarely taken aim at what we understand to be the most significant hurdles for U.S. attorneys, academics, and policymakers attempting to understand the GDPR.

Even now, more than two years after the GDPR went into effect, many Americans—including government officials, law firm partners, academics, and journalists—continue to get the law wrong. They claim that the GDPR is "about giving individuals complete control over their personal information in all contexts."[5] Some claim that the GDPR creates

2. Regulation 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), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

3. *Id.*

4. *See* Lilian Edwards, *Data Protection: Enter the General Data Protection Regulation*, *in* LAW, POLICY AND THE INTERNET (Lilian Edwards ed., 2018); Bart van der Sloot & Frederik Zuiderveen Borgesius, The EU General Data Protection Regulation: A New Global Standard for Information Privacy 1 (2018) (working draft), https://bartvandersloot.com/onewebmedia/SSRN-id3162987.pdf; Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What it is and What it Means*, 28 INFO. & COMMC'NS TECH. L. 65, 65 (2019); Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 115–16 (2017).

5. Kate Patrick, *DOJ Pushes Back on Idea of Consumer Control in a Federal Privacy Law*, INSIDESOURCES (Apr. 3, 2019), https://www.insidesources.com/doj-pushes-back-on-idea-of-consumer-control-in-a-federal-privacy-law/; *see also* Kate Fazzini, *Europe's Sweeping Privacy Rule*

a property right in personal data.[6] Some reduce the GDPR to a law that is, like a number of much-criticized privacy laws in the United States, "based on the principles of notice and choice."[7] And some claim that "[i]n the end, GDPR is all about consent and it's an approach to privacy that is very European."[8]

These mischaracterizations have consequences. Telling a company trying to comply with the GDPR that "[t]he rule requires opt-in consent from users before data can be collected" is wrong.[9] U.S. companies, too, may think that obtaining consent is the end of the story, foregoing other ongoing obligations. Given the GDPR's system of fines, being wrong can be very expensive.[10] Erroneous claims about the bases and require-

---

Was Supposed to Change the Internet, but so Far it's Mostly Created Frustration for Users, Companies, and Regulators, CNBC (May 5, 2019, 6:00 AM), https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html ("Known as GDPR, the regulation gave sweeping new powers to individuals in how they can control their data.").

6. Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, HARV. BUS. REV. (Jan. 30, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data.

> One solution is to create mechanisms that give users direct ownership of their data. There are many proposals jostling for attention . . . . Europe's General Data Protection Regulation (GDPR), which is arguably the most comprehensive legislative measure thus far, offers provisions for data portability, giving citizens greater digital agency.

Id.; *see also* Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 518–19 (2013) (conveying a nuanced understanding of "property").

7. John Rothchild, *New European Rules May Give US Internet Users True Privacy Choices for the First Time*, CONVERSATION (June 14, 2018, 6:44 AM), https://theconversation.com/new-european-rules-may-give-us-internet-users-true-privacy-choices-for-the-first-time-97982 ("Like many privacy rules, the GDPR is based on the principles of notice and choice."); David McCabe, *The Sun May Be Setting on the Old Privacy Rulebook*, AXIOS (Mar. 8, 2019), https://www.axios.com/sun-sets-old-privacy-rulebook-notice-consent-5642a827-9a86-454a-ae47-54c74691e8ae.html ("Europe is also heavily invested in the notice and consent approach, which forms the backbone of the General Data Protection Regulation that went into effect last year and has become the *de facto* global standard."); Woodrow Hartzog & Neil Richards, *There's a Lot to Like About the Senate Privacy Bill, if it's Not Watered Down*, HILL (Dec. 6, 2019, 11:00 AM), https://thehill.com/opinion/technology/472892-theres-a-lot-to-like-about-the-senate-privacy-bill-if-its-not-watered ("Unfortunately, though, COPRA also takes on many of the same shortcomings of existing data protection frameworks such as the GDPR that over-leverage concepts of consent, notice and choice."); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1719 (2020) [hereinafter *Privacy's Constitutional Moment*]; Gabriela Zanfir-Fortuna, *10 Reasons Why the GDPR is the Opposite of a 'Notice and Consent' Type of Law*, MEDIUM (Mar. 13, 2019) [hereinafter *Notice and Consent*], https://medium.com/@gzf/10-reasons-why-the-gdpr-is-the-opposite-of-a-notice-and-consent-type-of-law-ba9dd895a0f1 (critiquing these characterizations of the GDPR).

8. Fazzini, *supra* note 5 (quoting Odia Kagan, chair of the GDPR compliance program at law firm Fox Rothschild); *see also* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 795 (2020); Meera Narendra, *#PrivSecNY: Tim Wu on GDPR and Data Privacy Practices in the US*, PRIVSEC REP. (Nov. 18, 2019), https://gdpr.report/news/2019/11/18/privsecny-tim-wu-on-gdpr-and-data-privacy-practices-in-the-us/ ("I don't think that GDPR is the right model for the United States. I think it's overly consent-driven and doesn't change enough."); *Privacy's Constitutional Moment*, *supra* note 7, at 1727–28.

9. Michael S. Malone & William Davidow, *Corporations Shouldn't be Allowed to Own Your Personal Data at All*, SALON (Feb. 15, 2020, 7:00 PM), https://www.salon.com/2020/02/15/corporations-shouldnt-be-allowed-to-own-your-personal-data-at-all/.

10. *See* GDPR, *supra* note 2, at art. 83.

ments of the GDPR have further consequences, too, for U.S. policymakers' conversations about enacting new U.S. data privacy laws.[11] If an aspect of that discussion is whether or not to enact U.S. law that mimics the GDPR, we should know what it is that we are copying or rejecting.

In drafting this Guide, we aim to resolve common inaccuracies, frame data protection approaches, and inform technology policy. This Guide provides an overview of the GDPR's coverage and requirements. It does not give step-by-step compliance advice, which can be obtained elsewhere; instead, we endeavor to correct common misconceptions about the GDPR, situate it against familiar U.S. regimes, and provide necessary context that an American reader might lack. Understanding the GDPR requires knowing not only what it contains but how to read it, and some basic understanding of both data protection law and broader European law. The most common mistake Americans make, we find, is to focus on an individual GDPR requirement (such as the right to be forgotten), while missing both context and overview.

Thus, this American's Guide to the GDPR begins with background: an overview of what data protection is and how it contrasts with familiar U.S. privacy regimes, such as notice-and-choice or consumer protection. The GDPR as a data protection regime offers protections that follow the data and imposes data governance duties on companies regardless of whether individuals invoke their rights.[12] Corporate governance is the core of the GDPR's worldwide impact, a central aspect of the EU's approach to data protection, and is strikingly often missing in discussions of the GDPR in the United States. This Guide then provides an introduction to the EU and its various institutions, and their respective roles in data protection law.

In Part II, we discuss what is in the GDPR: where it reaches, what it covers, and what it requires. Again, we find that the GDPR as a data protection regime imposes significant corporate responsibilities in addition to a substantive system of individual rights.[13] In Part III, we provide a practical guide to reading the GDPR's text. The GDPR often imposes broad standards rather than specific rules, befuddling U.S. readers who do not know what interpretive resources to look to beyond the text. We characterize the GDPR as a process rather than a set of clear legal requirements. Finally, we point our readers to a number of useful sources and methodologies for researching legal questions about the GDPR.

We make four observations throughout. First, the GDPR is based on fundamental rights. In Europe, these rights entail protections provided by

11. Anupam Chander et al., *Catalyzing Privacy Law*, MINN. L. REV. (forthcoming 2020) (manuscript at 31–35) (on file with authors); *see Privacy's Constitutional Moment*, *supra* note 7, at 1721–22.

12. *See* GDPR, *supra* note 2, at arts. 12–23.

13. *Id.*

the state, rather than just restrictions on the state. Second, data protection in Europe is importantly distinct from privacy and consumer protection laws, which include their own set of rules and regulations that interact with the GDPR. Third, the GDPR harmonizes data protection across EU countries, but still leaves much to Member States. As such, domestic law and politics remain relevant to understanding the GDPR and European data protection. Fourth, the GDPR is better understood as a process rather than a law. Therefore, to claim to be able to automate GDPR compliance—or provide a clear checklist—is to misrepresent the nature of the law.

We hope that our readers can use this Guide to understand necessary concepts and practical tools about the GDPR. It is hard to create American-friendly shorthand for precisely what the GDPR is. We hope, however, to make our readers think twice before defaulting to shorthand that is incorrect.

I. ESSENTIAL BACKGROUND: ON DATA PROTECTION, EUROPEAN INSTITUTIONS, & BASIC MISCONCEPTIONS ABOUT THE GDPR

We begin this Guide with essential background, starting with the distinction between privacy law and data protection law. The GDPR is a data protection law. Data protection and privacy are not the same thing.[14] In Europe, they are distinct concepts that stem from different, though intertwined, sources of law.[15] An American reading the GDPR is likely to be familiar with the oft-repeated statement that "data protection is a fundamental right," but may not necessarily understand what that means. Thus, in this first Part, we offer an introduction to data protection law and its relationship to privacy, situated in European institutions and legal instruments. We also discuss what data protection is not: (a) a primarily consent-based or notice-and-choice-based regime, and (b) a regime where individuals have absolute control over their data. This leads to a discussion of common misconceptions about the GDPR. We then conclude with an overview of two often-missed but core principles of the GDPR: lawfulness and accountability, leading us into the next Part about GDPR coverage and substance.

A. Privacy Versus Data Protection

We begin with an overview of how U.S. lawyers think of privacy. When most Americans think of privacy, they think of protecting individuals from the dissemination of a particular piece of harmful information,

14. GLORIA GONZÁLEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 5 (Law, Governance & Tech. Ser. Vol. 16, 2014).

15. *Id.*

or against particularly intrusive information collection.[16] This puts privacy laws in tension with the First Amendment's protection of free speech, although courts have recognized that privacy can be necessary for speech as well.[17] The other privacy touchstone for Americans is the Fourth Amendment, which protects individuals against warrantless government surveillance that violates a "reasonable expectation of privacy."[18] The Fourth Amendment emphasizes protections for the home, and courts have struggled until only very recently with addressing large-scale surveillance in public places, or surveillance conducted online.[19]

These U.S. conceptions of privacy are largely black-and-white—you either have privacy or you do not—and often depend on keeping information private or secret. Until very recently, sharing information with a third-party was largely understood in both the privacy tort context and the Fourth Amendment context to preclude having a privacy interest.[20] The U.S. Supreme Court is only beginning to grapple with expanding its understanding of privacy in the information age.[21]

Data protection is more akin to what many in the United States call "data privacy" or "information privacy": protections that attach to data sets (of personal data) that are stored and analyzed en masse. The accumulation of digital dossiers raises not just concerns that disclosure of a piece of information will harm someone but systemic concerns about power, fairness, accuracy, security, and accountability when governments and companies hold large amounts of information about individuals.

---

16. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (listing the four torts that comprise the law of privacy); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 10–11, 106–07, 161–64 (2008).

17. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000). *But see* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 466-67 (2015); Neil M. Richards, *The Limits of Tort Privacy*, 9 J. ON TELECOMMS. & HIGH TECH. L. 357, 365 (2011); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 387–93 (2008); Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1501 (2015); Scott Skinner-Thompson, *Recording as Heckling*, 108 GEO. L.J. 125, 127–28 (2019).

18. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

19. Kyllo v. United States, 533 U.S. 27, 31 (2001) (emphasizing protection for the home); *see* United States v. Knotts, 460 U.S. 276, 281–82 (1983); United States v. Karo, 468 U.S. 705, 712–14 (1984); Oliver v. United States., 466 U.S. 170, 179 (1984). *But see* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

20. United States v. Miller, 425 U.S. 435, 442 (1976); *see* Smith v. Maryland, 442 U.S. 735, 743–45 (1979); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1839–40 (2010).

21. United States v. Jones, 565 U.S. 400, 406–08 (2012); *see* Riley v. California, 573 U.S. 373, 385–86 (2014); *Carpenter*, 138 S. Ct. at 2213–14; Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 358–60 (2019).

As early as the 1960s, these concerns gave rise in the United States and elsewhere[22] to a set of principles for mass data collection, handling, and processing: the Fair Information Practices (FIPs).[23] The FIPs include a substantial set of individual process-like rights—rights of access, correction, and erasure—and affirmative obligations for data handlers (to specify a purpose for processing, limit data use to that purpose, and use reasonable security safeguards, among other things).[24] While the FIPs are no panacea, they form the backbone of data protection laws, or data privacy laws, both within the United States and around the world.[25]

In the U.S. context, constitutional protections for information privacy are limited and do not fully reflect the FIPs. Constitutional information privacy protects only against government action and consists in practice of multifactor balancing tests that weigh the potential harm in disclosure against the adequacy of any safeguards.[26] These constitutional safeguards are a relatively blunt policy instrument, focused still on preventing the dissemination of sensitive information with harmful consequences. By contrast, a series of sectoral U.S. statutes enacted starting in the 1970s take a more data-protection-like approach, building protections and rights against the government (the Privacy Act) and against private actors in particular sectors (e.g., the Fair Credit Reporting Act).[27]

Later in this Part, we return to distinctions between the U.S. and EU approaches to data privacy. For now, we note that while both systems are ostensibly founded on the FIPs, they have significant differences in scope, emphasis, and substance.

The distinction between privacy and data protection also exists in European law, much more formally than it does in the United States. European law explicitly protects both privacy and data protection as "fundamental human rights."[28] But it is important for Americans to understand that there is a significant difference between rights under U.S.

---

22. Most notably in the United Kingdom, where the Younger Report included principles established by the British Computer Society. *See* Gerald Dworkin, *The Younger Committee Report on Privacy*, 36 MOD. L. REV. 399, 400–06 (1973).

23. *See* Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIV. F. (Dec. 19, 2007), https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

24. Org. for Econ. Co-Operation & Dev., The OECD Privacy Framework 14–15 (2013) [hereinafter OECD GUIDELINES].

25. Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 953–54 (2017).

26. Whalen v. Roe, 429 U.S. 589, 598–600 (1977); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980).

27. William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 1025 (2016).

28. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Europ. T.S. No. 5, art. 8 (Nov. 4, 1950) [hereinafter European Convention on Human Rights]; Charter of Fundamental Rights of the European Union, arts. 7–8, 2012 O.J. (C 364) 391 [hereinafter Charter of Fundamental Rights].

constitutional law and rights under EU law.[29] While the U.S. Bill of Rights is a list of restrictions on the government based on individual protections, the 2000 Charter of Fundamental Rights of the European Union (the Charter) includes a list of rights to services provided by the state—that is, positive rights, not just negative rights.[30] These rights include, for example, affirmative rights to education and health care.[31]

Additionally, fundamental rights in the EU are far from absolute.[32] They are usually balanced against each other, and sometimes against other government interests, through an approach to human rights called "proportionality analysis."[33] Thus, to say that data protection is a fundamental right in the EU is not to say that courts will always overturn laws that impinge on it. The fundamental rights to privacy and data protection may fall in this analysis to other rights or interests.

The fundamental rights to privacy and data protection are related, but not the same.[34] One pair of scholars helpfully distinguishes between privacy and data protection as two different means for addressing power disparities: privacy through requiring opacity as a check on power, and data protection through establishing processes and transparency as a means of channeling power when it is exercised.[35] That is, privacy law at its core prohibits certain behavior and checks information flows, while data protection law provides "rules of the game" for processing data.[36] Another important difference is that privacy law tends overall towards vaguer standards, while data protection comprises a more precise set of rules.[37]

Data protection arguably has a different scope than privacy—in some ways broader and in some ways narrower. Data protection is lim-

---

29. *Compare* U.S. CONST. amends. I–X, *with* Charter of Fundamental Rights, *supra* note 28, at arts. 1–54.

30. *Compare* U.S. CONST. amends. I–X, *with* Charter of Fundamental Rights, *supra* note 28, at arts. 1–54.

31. *See* JEAN-FRANÇOIS AKANDJI-KOMBE, COUNCIL OF EUR., POSITIVE OBLIGATIONS UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS 47, 56 (HUM. RIGHTS HANDBOOKS SER. NO. 7, 2007).

32. *Data Protection*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection (last visited Oct. 30, 2020).

33. Alec Stone Sweet & Jud Mathews, *Proportionality Balancing and Global Constitutionalism*, 47 COLUM. J. TRANSNAT'L L. 72, 75–76 (2008).

34. *See, e.g.*, DOUWE KORFF & MARIE GEORGES, DATA PROTECTION OFFICER HANDBOOK 9–14 (2019); *see also* Gloria González Fuster & Serge Gutwirth, *Opening Up Personal Data Protection: A Conceptual Controversy*, 29 COMPUT. L. & SEC. REV. 531, 531–32 (2013).

35. SERGE GUTWIRTH & PAUL DE HERT, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *in* PRIVACY AND THE CRIMINAL LAW (Erik Claes et al. eds., 2006). To be clear, in the EU, both privacy and data protection apply to private actors, too. *See* Schwartz & Peifer, *supra* note 4, at 115–16.

36. HIELKE HIJMANS, *Privacy and Data Protection as Values of the EU that Matter, Also in the Information Society*, *in* THE EUROPEAN UNION AS GUARDIAN OF INTERNET PRIVACY 17, 66 (Law, Governance & Tech. Ser. Vol. 31, 2016). *But see* González Fuster & Gutwirth, *supra* note 34, at 531–32 (arguing for a prohibitive approach to data protection).

37. HIJMANS, *supra* note 36, at 66.

ited to covering personal data (versus, say, preventing an intrusion into the home), but follows that data outside of context more traditionally understood to be private. Data protection law, too, often refers to other complementary fundamental rights besides privacy, such as the right to nondiscrimination.[38]

For a U.S. lawyer accustomed to dealing with state privacy torts, data protection law's core focus on principles of transparency and accountability—rather than on stopping information from spreading—may be surprising. The emphasis on access rights (known in the EU as Subject Access Rights (SARs)) makes data protection law in some ways more resemble an open government law, such as the Freedom of Information Act (FOIA), rather than a traditional U.S. privacy tort that seeks to suppress information.[39] This makes data protection regimes more compatible with U.S. free speech values than is often acknowledged. A large component of data protection is about increasing information flow, not decreasing it. Only through knowing about and participating in what information governments and companies hold on them can individuals check unchecked power, regain some (but not absolute!) control, and push back against manipulation in the information age.

B. European Institutions

To further understand what Europeans mean when they refer to data protection as a fundamental right, it is necessary to understand some background about European institutions. Many of these institutions share confusingly similar names—for example, the Council of Europe, the Council of the European Union, and the European Council, which are each separate bodies in two distinct legal regimes.[40] Additionally, there

---

38. *Id.*; Paul De Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Actio*n, *in* REINVENTING DATA PROTECTION? 3, 9 (Serge Gutwirth et al. eds., 2009).

39. *See* De Hert & Gutwirth, *supra* note 38, at 28. *But see* Joined Cases C-141/12 & C-372/12, YS v. Minister voor Immigratie, Integratie en Asiel & Minister voor Immigratie, Integratie en Asiel v. M, S,, ECLI:EU:C:2014:2081, ¶¶ 1–70 (July 17, 2014). Edwards characterizes this case as establishing that data protection law does not establish an access right with respect to information about the law itself, in contrast to a true open government law such as FOIA. Edwards, *supra* note 4, at 16.

40. For the curious: the Council of Europe, discussed below, is an international organization founded by European countries shortly after World War II. *About the Council of Europe: Brief Facts*, COUNCIL OF EUR., https://www.coe.int/en/web/yerevan/the-coe/about-coe (last visited Oct. 30, 2020). The Council of the European Union is one of three legislating bodies of the EU. *Council of the European Union*, EUR. UNION, https://europa.eu/european-union/about-eu/institutions-bodies/council-eu_en (last updated Jan. 10, 2020). The European Council is also part of the EU, comprises the heads of state of the EU Member States, and lays out overall policy goals but does not legislate. *European Council*, EUR. UNION, https://europa.eu/european-union/about-eu/institutions-bodies/european-council_en (last updated July 29, 2020). When it comes to EU lawmaking, there are five central institutions. The European Council sets the "political direction" of the EU but has no power to pass laws. *Id.* Three institutions are involved in actual legislating: the European Parliament; the Council of the European Union (not to be confused with the European Council); and the European Commission. *See Institutions and Bodies*, EUR. UNION, https://europa.eu/european-union/about-eu/institutions-bodies_en (last updated May 20, 2020). The Court of Justice of the EU (CJEU, also

are a number of distinct—but overlapping—sets of laws, not just between Member States and transnational institutions, but between different transnational regimes.[41]

With respect to data protection, it is important to understand that there are two different Europe-wide sources of fundamental rights.[42] The first is the European Convention on Human Rights (ECHR, or Convention), which entered into force in 1953.[43] The Council of Europe, which is not a body of the EU but a separate international organization founded in 1949, drafted the Convention.[44] The European Court of Human Rights (ECtHR), often referred to as the Strasbourg Court because of where it sits, interprets the Convention.[45]

The right to data protection is outlined in a different document, originating in a different legal regime, the EU.[46] The EU Charter, which is interpreted by the Court of Justice of the EU (CJEU, also known as ECJ, or the Luxembourg Court), is the source of fundamental rights for the EU's legal regime.[47] The Charter echoes a number of the rights in the Convention, but also adds to it. The Charter was originally a political document intended to recognize a synthesized set of national and international obligations for EU Member States, but it became a legally binding treaty with direct force on EU Member States in 2009 under the Lisbon Treaty.[48]

The two courts have a complex, even competitive, relationship, with the CJEU referring to ECtHR case law, but not holding itself directly bound by it.[49] And to complicate things further, all Member States of the EU are also parties to the Convention and thus subject to decisions made

known as ECJ) interprets these laws. *See Court of Justice of the European Union (CJEU)*, EUR. UNION, https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (last updated Mar. 26, 2020). The Commission also acts like an "executive branch" in that it implements CJEU decisions and otherwise ensures that laws are properly implemented in Member States. *European Commission*, EUR. UNION, https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en (last updated July 5, 2020).

41. *See Types of EU Law*, EUR. COMM'N, https://ec.europa.eu/info/law/law-making-process/types-eu-law_en (last visited Oct. 30, 2020) (listing and describing the types of laws and regulations in effect in the European Union).

42. Member States also have their own constitutions. But we will leave those for another day. Thanks Claudia Quelle for the reminder of the complex relationship of "federated constitutionalism" between the EU and its Member States.

43. *About the Council of Europe – Overview: History*, COUNCIL OF EUR., https://www.coe.int/en/web/yerevan/the-coe/about-coe/overview (last visited Oct. 30, 2020). The Statute of the Council of Europe was signed in St. James's Palace, London, on May 5, 1949. *Id.*

44. *Id.*; *see also* GEORGE LETSAS, A THEORY OF INTERPRETATION OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 1 (2007).

45. GONZÁLEZ FUSTER, *supra* note 14, at 81; *see also* De Hert & Gutwirth, *supra* note 38, at 5.

46. Charter of Fundamental Rights, *supra* note 28, at art. 8.

47. *Id.*

48. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1.

49. Jasper Krommendijk, *The Use of ECtHR Case Law by the Court of Justice After Lisbon: The View of Luxembourg Insiders*, 22 MAASTRICHT J. EUR. & COMPAR. L. 812, 812–13 (2015).

by the ECtHR.[50] This has allowed the CJEU to use ECtHR case law as a legal floor in this space, technically not binding on the court itself, but binding on all of the Member States to which the CJEU's rulings also apply.[51]

We begin with the Convention, interpreted by the ECtHR. Article 8 of the Convention provides a "right to respect for . . . priva[cy] and family life, his home and his correspondence."[52] This is often referred to as a "right to respect for private life," and is similar to historic understandings of privacy in the United States.[53] As in the United States, privacy is understood to create a barrier between the state and individuals, and otherwise enables individual autonomy.[54] Privacy is largely invoked to require the state—or, unlike in the United States, a private actor—to stop intrusions into the private sphere.[55]

By contrast, the Charter contains both the right to privacy in Article 7 and the additional right to data protection in Article 8.[56] Article 8 of the Charter states that everyone has a right to the protection of personal data concerning them, data must be processed fairly for a specified purpose—either on the basis of consent or some other legitimate bases in law—and an independent authority shall handle compliance.[57]

The fundamental right to data protection thus reflects the core elements of many data protection laws that pre-existed the Charter. But it also does more. It gives the CJEU the explicit authority to evaluate whether laws and practices are adequately protective of the fundamental right to data protection, providing a human rights backstop to any data

---

50. *See* Jonas Christoffersen & Mikael Rask Madsen, *Introduction: The European Court of Human Rights Between Law and Politics*, *in* THE EUROPEAN COURT OF HUMAN RIGHTS BETWEEN LAW AND POLITICS 1, 1–5 (Jonas Christoffersen & Mikael Rask Madsen, eds., 2011).

51. Additionally, most countries have incorporated the Convention into their own national laws, allowing national courts to interpret provisions similar or identical to the convention. *See, e.g.*, Paul Meredith, *Incorporation of the European Convention on Human Rights into UK Law*, 2 EUR. J. EDUC. L. & POL'Y 7, 7 (1998) (describing the proposal to incorporate the ECHR into UK law).

52. EUR. CT. OF HUM. RIGHTS, GUIDE ON ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 7 (2020).

53. González Fuster & Gutwirth, *supra* note 34, at 536.

54. De Hert & Gurtwirth, *supra* note 41, at 9–11.

55. *Id.* at 6.

56. Article 7 reads: "Everyone has the right to respect for his or her private and family life, home and communications." Charter of Fundamental Rights, *supra* note 28, at art. 7. Article 8 reads:

> 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

Id. at art. 8.

57. *Id.* at art. 8.

protection legislation.[58] Additionally, it provides the EU with the justification to directly regulate data protection, which resulted in the GDPR.[59]

As discussed above, there has been much discussion in Europe of just how distinct data protection and privacy really are. Despite the apparently clear textual distinction between the Convention and the Charter, in practice, court decisions are often muddled.[60] Again, the Convention does not provide for an explicit right to data protection.[61] However, in recent years, the ECtHR has interpreted the Convention's right to privacy more broadly and has included aspects of data protection.[62] The ECtHR is likely influenced in its understanding of privacy by the rise of European data protection laws over time, before the GDPR, and even before the earlier EU-wide Data Protection Directive (DPD). As scholars note, "changing case law of the [ECtHR] . . . has been progressively incorporating elements of data protection . . . in its construal of the content of Article 8."[63] That is, the ECtHR began referring to data protection as an aspect of the Article 8 privacy right, drawing on elements of existing data protection laws, despite no explicit right to data protection in the Convention.[64]

Why should all of this matter to U.S. lawyers, policymakers, and academics? Because it is crucial to understand that the requirements of the GDPR do not stand in isolation. Rather, the CJEU may someday in-

---

58. EUR. UNION AGENCY FOR FUNDAMENTAL RTS. & COUNCIL OF EUR., HANDBOOK ON EUROPEAN DATA PROTECTION LAW 205–06 (2018) [hereinafter EUROPEAN DATA HANDBOOK].

59. The Lisbon Treaty did more than grant the Charter binding legal status on Member States; it also gave the EU a legal basis for comprehensive data protection legislation across the Community. *See* OTTAVIO MARZOCCHI, EUR. PARLIAMENT, THE PROTECTION OF FUNDAMENTAL RIGHTS IN THE EU 3 (2019). Prior to the agreement, the EU was limited to legislating based on the internal market legal basis, which justified only directing national laws to approximate one another so as not to inhibit the free flow of data across borders (something like the Commerce Clause, but far weaker). *See The Lisbon Treaty and Privacy*, EPIC.ORG, https://epic.org/privacy/intl/lisbon_treaty.html (last visited Oct. 30, 2020) (stating the Lisbon Treaty makes the Charter legally enforceable on the EU, its institutions, and the Member States). In January 2012, after the Charter went into direct effect, the EU Commission published its proposal for data protection law and in doing so began the EU legislative process with the European Parliament and Council. Press Release, Eur. Comm'n, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012) (on file with authors). The European Parliament published the agreed-upon language in spring 2014, and the Council in 2015. The General Data Protection Regulation was published officially in April 2016 and, to much international fanfare, went into effect on May 25, 2018. GDPR, *supra* note 2, at art. 99.

60. *See, e.g.*, Phillip N. Yannella, *Making Sense of EU Cookie Law in the Wake of CJEU's Planet49 Ruling*, BALLARD SPAHR: CYBERADVISER (Oct. 3, 2019), https://www.cyberadviserblog.com/2019/10/making-sense-of-eu-cookie-law-in-the-wake-of-cjeus-planet49-ruling/ (discussing the confusion that remains after the CJEU's decision in Case C-673/17, Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, 2019 ECLI:EU:C:2019:801, ¶¶1–82 (Oct. 1, 2020)).

61. *See* European Convention on Human Rights, *supra* note 28, at art. 8 (describing many rights but not explicitly conferring a right to data protection).

62. HIJMANS, *supra* note 36, at 66 ("[I]n the case law of the [ECtHR] and the [CJEU], the right to privacy has been broadly interpreted and is not confined to the right to be left alone as it extends to areas outside the private sphere.").

63. González Fuster & Gutwirth, *supra* note 34, at 536.

64. *See id.*

tervene to interpret those requirements or to find them (or Member States' implementations of them) in violation of fundamental rights. Further, the ECtHR may decide cases on privacy and data protection that later influence CJEU interpretations of the fundamental right to data protection and the GDPR.

It is also crucial to understand that although the GDPR was a shock to American systems, in the European context, it was far from surprising or new. Some EU Member States have had data protection laws in place since the 1970s.[65] The Council of Europe's instrument on data protection, known as Convention 108, entered into force transnationally back in 1985, and was modernized in 2018.[66] Even within EU institutions, data protection is not new. The GDPR replaced the Data Protection Directive (DPD), which had been in place since 1995.[67]

Thus, despite its apparent novelty to many Americans, much of the GDPR is not new to Europe. For example, the much-discussed "right to be forgotten" was established under the DPD's right to object and right to access and erasure,[68] and many of the other GDPR individual rights were also present in some form or other.[69] The DPD, too, established the foundational conceptual categories, discussed further in Part II, of "data controllers" and "data processors."[70]

The DPD was binding on all EU Member States but required implementation through national law.[71] This gave rise to significant variation between both national laws and national enforcement policies, allowing regulatory arbitrage by companies that chose more lax jurisdictions.[72] In contrast to the DPD, the GDPR was intended to be a harmonizing regulation that applies directly to each Member State.[73] It nonetheless contains many opportunities for Member State derogation—that is,

---

65. The Hessische Datenschutzgesetz (Data Protection Act of Hesse) from 1970 defined Datensuchtz (Data Protection). GONZALEZ FUSTER, *supra* note 15, at 56. Sweden enacted the first national data protection law in 1973 (Datalag). *Id.* at 58. Germany enacted its Federal Data Protection Law (Bundesdatenschutzgesetz) in 1977. *Id.* at 60. Austria adopted its law in 1978. *Id.* at 71. France adopted its law in 1978 as well (loi informatique et libertés). *Id.* at 77; *see also* González Fuster & Gutwirth, *supra* note 34, at 533–34.

66. GONZÁLEZ FUSTER, *supra* note 14, at 91; *see also* González Fuster & Gutwirth, *supra* note 34, at 535; *Modernisation of the Data Protection "Convention 108"*, COUNCIL OF EUR., https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet (last visited Nov. 5, 2020).

67. Directive 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, 1995 O.J. (L 281) 31, 50.

68. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317, ¶ 91 (May 13, 2014).

69. *Id.* ¶¶ 70–84.

70. Directive 95/46/EC, supra note 67, at art. 2(d)–(e).

71. Like a non-self-executing treaty.

72. TJ MCINTYRE, *Regulating the Information Society: Data Protection and Ireland's Internet Industry*, *in* THE OXFORD HANDBOOK OF IRISH POLITICS 1, 2 (Farrell & Hardiman eds., forthcoming 2020).

73. *Compare* Directive 95/46/EC, *supra* note 67, *with* GDPR, *supra* note 2.

places where Member States are explicitly contemplated as creating, and sometimes are even required to create, variations through national legislation.[74] Thus, despite the fact that the GDPR is directly applicable as an EU regulation rather than a directive, many Member States have nonetheless passed implementing laws with potentially significant variations.[75]

The biggest change to the EU's pre-existing approach to data protection is that the GDPR is harder law than the DPD. It applies directly to the Member States without enacting legislation, it toughens EU-wide harmonization mechanisms, and it potentially imposes much larger fines on violators.[76] The combination of these features with the GDPR's explicit extraterritorial reach made more companies around the world take note of EU law. That is, many of the GDPR's requirements existed under the DPD in some form, but many companies, particularly global companies, took note of them only when the potential penalties and likelihood of enforcement increased.

C. Basic Misconceptions About the GDPR: Understanding Lawfulness and Corporate Accountability

We close this Part by discussing other misconceptions about the GDPR's content. Despite what a number of Americans appear to think and despite cosmetic similarities to U.S. laws, the GDPR is neither primarily a consent-based regime nor primarily based on notice-and-choice. Understanding this is important because these particular mischaracterizations often lead American critics to readily dismiss the GDPR as too similar to U.S. privacy laws that have failed or been ineffective.[77]

We mentioned above that there are similarities between some U.S. laws and the EU's data protection approach.[78] The bulk of the U.S. approaches to information or data privacy, however, differ from European-style data protection in several important ways. First, the U.S. federal statutory approach is sectoral rather than omnibus (that is, comprehensive) like the GDPR—federal U.S. privacy statutes do not cover all per-

74. GDPR, *supra* note 2, *passim*.

75. The IAPP provides a derogation tracker to members. *See* Emily Leach, *Tracking GDPR Derogations and Implementations* (Dec. 11, 2018), https://iapp.org/news/a/tracking-gdpr-derogations-and-implementations/.

76. European Commission, *Article 29 Data Protection Working Party: Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679*, 17/EN WP 253 (Oct. 2017) [hereinafter *Article 29 Data Protection Working Party*].

77. *See The 10 Problems of the GDPR: Hearing on the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation Before the S. Judiciary Comm.*, 116th Cong. 2 (2019) [hereinafter *Layton Statement*] (statement of Roslyn Layton, Visiting Scholar, American Enterprise Institute).

78. McGeveran, *supra* note 27, at 1025.

sonal data, but only data in particular sectors, or held by particular entities.[79]

Second, where the United States takes a more comprehensive (or nonsectoral) approach to personal data, it employs what some scholars have identified as a consumer protection approach to data privacy, focusing on protecting individuals in direct relationships with companies.[80] The consumer protection approach to information privacy is taken by the Federal Trade Commission and by state attorneys general around the country, which each enforce versions of "unfair and deceptive trade . . . practices" (UDAP) laws.[81] When applied to data privacy, deceptive practices usually include false promises made by companies to individuals in privacy policies or public statements; unfairness applies to flaws such as unilateral changes to privacy policies or inadequate data security.

This creates the problem one of us has termed the "Internet of Other Peoples' Things"—that data privacy protections in the United States largely extend only so far as direct consumer relationships and not to the growing variety of both surveillance systems and data processing conducted by third-parties that have no direct relationships to consumers.[82] In the United States, in others words, data privacy protection focuses on the relationship and does not follow the data.[83] This leaves an increasingly vast ecosystem of third-party data brokers largely unregulated.[84] By contrast, true EU-style data protection follows personal data regardless of who holds it.[85] Third-party data brokers are not only subject to the GDPR, but are systematically disfavored by it.[86]

The U.S. approach to data privacy is often criticized, too, for an excessive focus on individual notice and choice.[87] That is, U.S. privacy laws focus on providing individuals with information and respecting their purportedly autonomous decisions to opt in or out of a particular set of information practices. The U.S. version of individual control and consent is understood to be a paper regime, based on long, elaborate privacy

---

79. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 905 (2009).

80. *See* 15 U.S.C. § 45(a)(1) (2018) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."); *see also* McGeveran, *supra* note 27, at 965.

81. Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 750, 754 (2016).

82. *See* Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 639–40 (2015).

83. McGeveran, *supra* note 27, at 965–67. *But see* Chander et al., *supra* note 11 (manuscript at 3–5) (describing the CCPA as breaking from previous U.S. privacy laws).

84. VT. STAT. ANN. tit. 9, § 2447 (2020); *see also* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100–.199 (West 2018).

85. McGeveran, *supra* note 27, at 965–67.

86. Hoofnagle et al., *supra* note 4, at 69.

87. *See, e.g.*, Ian Kerr, *Devil is in the Defaults*, 4 CRITICAL ANALYSIS LAW 91, 98–99 (2017); Ian Kerr et al., *Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 1, 2, 6 (Ian Kerr et al. eds., 2009).

policies—that often go unread—and surveillance that is impossible to opt out of in practice.[88] Thus, "consent" and "notice and choice" have become somewhat dirty words in data privacy conversations, standing for the exploitation of individuals under the fictional banner of respecting their autonomy.[89]

The GDPR is not primarily based on consent. Let us say it again: the GDPR is not primarily based on individual consent, at least not in the sense that U.S. practitioners and academics understand consent.[90] The GDPR has its problems and pathologies, but they are resolutely different from those of a primarily notice-and-choice-based regime.[91] Consent is potentially more substantive under the GDPR than it is in the U.S. context[92] and is not core to the GDPR in the way it is to the U.S. approach to data privacy.

The GDPR requires that personal data is "processed lawfully,"[93] which is often confusing to U.S. readers. Lawfulness is a component not just of EU data protection law but of European and international constitutional analysis.[94] Technically, for an action to be lawful it must be done according to a law. But the GDPR concept of lawfulness, and the concept of lawfulness in prior EU data protection law, is far more specific.[95]

Data protection starts with a ban: one cannot process personal data unless a lawful condition applies.[96] Article 6 of the GDPR outlines these lawful conditions: individual consent; necessity for performance of a contract; necessity for compliance with a legal obligation; necessity to protect the vital interests of the data subject or another person; necessity for a task carried out in the public interest; or necessity for the "legitimate interest" of the data controller.[97] One cannot process personal data under the GDPR unless one of these conditions applies. For certain kinds of data and certain kinds of data processing, the grounds for lawfulness are more limited.[98]

---

88. *See, e.g.*, McGeveran, *supra* note 27, at 973–74.

89. *See, e.g.*, Edwards, *supra* note 4, at 24–27.

90. *See* Hoofnagle et al., *supra* note 4, at 79; Gabriela Zanfir-Fortuna, *Forgetting About Consent: Why the Focus Should be on "Suitable Safeguards" in Data Protection Law* 4 (Univ. of Craiova Fac. of L. & Admin. Scis., Working Paper, 2013) [hereinafter *Forgetting About Consent*], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2261973; *see also* GABRIELA ZANFIR-FORTUNA & TERESA TROESTER-FALK, FUTURE OF PRIV. F. AND NYMITY, PROCESSING PERSONAL DATA ON THE BASIS OF LEGITIMATE INTERESTS UNDER THE GDPR: PRACTICAL CASES 3–4 (2018) [hereinafter PROCESSING PERSONAL DATA]; *Notice and Consent*, *supra* note 7.

91. *See Notice and Consent*, *supra* note 7; *see also Layton Statement*, *supra* note 77, at 12–13.

92. Elizabeth Edenberg & Meg Leta Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, 21 NEW MEDIA & SOC'Y 1804, 1808–10 (2019).

93. GDPR, *supra* note 2, at art. 5.

94. *See, e.g.*, Sweet & Mathews, *supra* note 33, at 85.

95. *See* PROCESSING PERSONAL DATA, *supra* note 90, at 3–4.

96. *See* McGeveran, *supra* note 27, at 966; *see also* PROCESSING PERSONAL DATA, *supra* note 90, at 3 (citing GDPR, *supra* note 2, at art. 5(1)(a)).

97. GDPR, *supra* note 2, at art. 6(1).

98. *See id.* at art. 22.

When Americans characterize the GDPR as a solely consent-based law, they are wrong. Most businesses subject to the GDPR process personal data either under the individual consent ground or the legitimate interest ground.[99] Under the GDPR, when businesses process personal data under individual consent, obtaining consent does not mean businesses can do whatever they want. There are still protections that remain in place, and individuals continue to have rights they can invoke with respect to that data.[100] Moreover, there are significant risks to processing personal data solely based on consent. First, due to the GDPR's more robust approach to both notice and consent, a regulator may find that the consent is not valid.[101] Second, individuals can withdraw consent.[102] A number of companies publicly indicated a preference for processing under the legitimate interest ground, which does allow individuals to later object to processing, but relies on various balancing tests companies may be more confident they can control.[103]

Another fiction making its way around American circles is that the GDPR is primarily centered on individual control.[104] Americans who characterize the GDPR in this way often then reject it as too stringent of a privacy regime to survive in the U.S. legal context.[105] The GDPR does not in any sense give individuals absolute control of their data. Nearly nothing in the GDPR is absolute. Rights have exceptions and are almost always constituted through balancing tests as discussed above.[106]

Furthermore, to the extent the GDPR is about individual control, it is not only about individual control. That is, the GDPR's approach to data protection does not solely rely on individuals actively exercising their rights.[107] The second half—perhaps the more important half—of the GDPR is about the accountability of companies, even in absence of people actively exercising their individual rights.

One of the core principles of the GDPR is the principle of accountability.[108] In some ways, accountability is familiar to those U.S. lawyers accustomed to U.S. data privacy laws. The FIPs are based on accountability and implemented through individualized transparency and partici-

---

99. *See* Edwards, *supra* note 4, at 23; *see also Notice and Consent*, *supra* note 7.
100. JEF AUSLOOS, THE RIGHT TO ERASURE IN EU DATA PROTECTION LAW 154 (2020).
101. *Id.* at 217.
102. Hoofnagle et al., *supra* note 4, at 90.
103. *See* GDPR, *supra* note 2, at art. 6(1)(f); *Article 29 Data Protection Working Party*, *supra* note 76, at 9.
104. However, note Jef Ausloos's important explanation of how control is at the core of the fundamental right to data protection in the Charter of Fundamental Rights of the EU and therefore different from the core of the GDPR, which is all about fair balancing different rights, freedoms and interests. AUSLOOS, *supra* note 100, at 52, 71.
105. *See, e.g.*, Patrick, *supra* note 5.
106. GDPR, *supra* note 2, at Recital 4; *see also* sources cited *supra* note 103.
107. AUSLOOS, *supra* note 100, at 72.
108. GDPR, *supra* note 2, at art. 5(2).

pation rights.[109] However, one can understand the GDPR's principle of accountability as focusing on companies "be[ing] able to demonstrate *compliance* with" the regime.[110]

That is, the GDPR is not just a system of individual rights. It is, at its core, also a compliance regime, focused on company duties, infrastructure, heuristics, and record-keeping—in short, corporate governance.[111] Even the GDPR's individual rights can entail a substantial amount of corporate accountability. Companies and government entities go through internal processes and legal analysis to assess when they must comply with individual rights and when they might legitimately invoke an exception, not to mention assess and mitigate risk when individual rights might be threatened on a larger scale.[112]

The GDPR's emphasis on corporate compliance is, in our view, responsible for the more significant practical export of GDPR-influenced principles and practices. While companies might not provide for individual data protection rights to individuals in non-EU countries around the world, they may be more likely to extend internal compliance patterns to non-EU data. Changes to company infrastructure and decision-making for GDPR compliance, in other words, can have positive externalities for non-EU persons. Once companies internalize compliance costs, they are more likely to try to impose similar costs on their competitors in other jurisdictions by joining efforts to enact new data privacy laws.[113]

This is not to say that GDPR compliance is or will be perfect.[114] Companies will assess how likely they are to be subject to GDPR enforcement and how costly it will be to increase compliance. The law is written in many places in broad, almost aspirational terms—the kind of language that gives U.S. compliance lawyers serious heartburn.[115] But that vagueness is at least partially intentional. The GDPR is often vague because it tasks companies with figuring out how to best implement its aspirations.[116]

One of us identified this dynamic as what regulatory theory terms "collaborative governance": the formation of public–private partnerships

109. Hartzog, *supra* note 25, at 952–53.

110. GDPR, *supra* note 2, at art. 5(2) (emphasis added).

111. *See* Hoofnagle et al., *supra* note 4, at 67–68; *see also* Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1560, 1602, 1611 (2019).

112. *See* Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations* 4–5 (Univ. of Colo. L. Legal Stud. Rsch. Paper, Paper No. 19-28, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3456224.

113. Chander et al., *supra* note 11 (manuscript at 10); *see also* Schwartz & Peifer, *supra* note 4, at 121.

114. *See, e.g.*, Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 792–95 (2020) (discussing legal endogeneity in U.S. privacy practices).

115. *See* Hoofnagle et al., *supra* note 4, at 67 (describing GDPR's language as vague and aspirational).

116. *See* Kaminski, *supra* note 111, at 1598.

around both the substance and enforcement of the law.[117] The GDPR, in effect, often entrusts companies with coming up with what compliance should look like. This is backed by regulators who leave some room for error.[118] In the context of data protection, European regulators are often more interested in cooperation and good faith efforts than in perfect compliance.[119]

A similar approach to addressing privacy through public–private partnerships has been proposed in the United States.[120] While evaluating these proposals in detail is beyond the scope of this Guide, we note that the backdrop of the GDPR is different than the backdrop of such a regime in the United States. In Europe, delegation to the private sector may work.[121] Not only does the GDPR establish significant penalties with which regulators can threaten companies, but data protection and privacy are fundamental rights in Europe.[122] This changes the dynamic between free speech and privacy interests. It also encourages companies to take government enforcement more seriously, even with friendly regulators, because courts can overrule those regulators based on violations of fundamental rights.

That is, even if EU regulators might act cooperatively towards companies, there is no guarantee that European courts will do the same. Because human rights protections in the EU constrain not just government actors but also companies, this creates a very different setting for delegated corporate compliance.[123] For every vague balancing test that a company conducts under the GDPR, there is the possibility that a court will find that balancing inadequate as a matter of fundamental rights.

II. WHAT THE GDPR COVERS AND REQUIRES: A SHORT OVERVIEW

An American attorney with experience practicing U.S. data privacy law may find the GDPR in some ways familiar, and in others, quite foreign. Yet, American attorneys are increasingly called upon to provide GDPR analysis for domestic U.S. companies.[124] Combining the potential for large fines with extended extraterritorial reach, the GDPR has effec-

117. *Id.* at 1595. See discussion *infra* Part III, for explanation of how to read and interpret the GDPR.

118. Kaminski, *supra* note 111, at 1599 ("If the GDPR's regulators are too command-and-control minded, they may override the collaborative nature of the system and eliminate envisioned benefits from private sector involvement.").

119. Hoofnagle et al., *supra* note 4, at 67 (discussing imperfect compliance and cooperation with regulators); McGeveran, *supra* note 27, at 983.

120. Dennis D. Hirsch, *Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons it Holds for U.S. Privacy Law*, 2013 MICH. ST. L. REV. 83, 96 (2013); McGeveran, *supra* note 27, at 980.

121. *See* Kaminski, *supra* note 111, at 1564.

122. Charter of Fundamental Rights, *supra* note 28, at arts. 7–8; *see also* Schwartz & Peifer, *supra* note 4, at 142; Hoofnagle et al., *supra* note 4, at 92–93.

123. Charter of Fundamental Rights, *supra* note 28, at art. 51.

124. Sean McGuinness & Katie Fillmore, *The Impact of GDPR on Attorneys and Law Firms in the United States*, AM. GAMING LAW., Autumn 2018, at 17, 17–19.

tively scared many domestic U.S. companies into contemplation of its requirements, if not into compliance.

This Part provides an overview of GDPR coverage and requirements, with references to more detailed resources. It is not intended to be a step-by-step compliance guide. In fact, American attorneys should maintain a healthy skepticism of GDPR compliance checklists and automated compliance programs. Filled with broad standards, the GDPR as a document does not naturally lend itself to a checklist approach.

It may make more sense to understand the GDPR as a process rather than as law. We do not mean to undermine how seriously companies should be taking the regulation. But to read the law as if the text itself contains all the answers, and as if perfect checklist compliance is the goal, misunderstands the nature of the GDPR and its goals.[125] Many of the GDPR's requirements take the form of mandatory, clear enough rules. But the GDPR's simultaneous focus on collaborative governance means that, where its requirements are fuzzier, companies might approach its obligations as a continuous, ongoing process of risk assessment—albeit, risk assessment with a floor of real human rights protection.[126]

The core of the GDPR is housed in a set of principles outlined in Article 5.[127] These principles build on the familiar FIPs, but also indicate two concepts U.S. readers may find unfamiliar. Article 5 requires transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality—all principles drawn from the FIPs and echoed to various degrees in U.S. sectoral data privacy laws.[128] But U.S. readers often misunderstand the core GDPR principle of "lawfulness," discussed in detail above, as requiring individual consent. The principle of "accountability," also discussed above, is often misunderstood by Americans, who think of it as being about accountability to individuals, where in the context of the GDPR, it is equally about corporate compliance.[129]

A. Where, What, and Whom: The GDPR's Coverage

The GDPR is on the radar of many American companies because of the breadth of what it covers, its extraterritorial reach, and its potential threat of large fines. We start with the aspect likely of most interest to Americans: where in the world the GDPR covers.

---

125. Hoofnagle et al., *supra* note 4, at 67.

126. Claudia Quelle, *The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat it, Too* 5 (Tilburg L. Sch., Research Paper No. 17, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000382.

127. GDPR, *supra* note 2, at art. 5.

128. *Id.*

129. Kaminski, *supra* note 111, at 1560, 1602, 1611.

The GDPR has an explicitly extraterritorial reach.[130] It applies to the processing of personal data where a company is established in the EU, regardless of whether it exports the data elsewhere for processing.[131] It also applies to data processing by non-EU-based companies where those companies (a) offer goods or services to individuals in the EU, or (b) monitor the behavior of individuals in the EU.[132] To fall under the GDPR, a company must do something more than merely having an internationally accessible website.[133] But offering goods or services in the language of an EU Member State—or otherwise implying an EU audience—may indicate that a company is targeting EU persons.[134]

Like the DPD, the GDPR restricts companies from exporting personal data to regions that lack adequate data protection law.[135] Both past and current EU data protection laws established a system for assessing whether another country's laws are "adequate" for such exports to occur.[136] If the European Commission (Commission) makes an adequacy decision, then transfer of personal data to that country does not require any additional authorization.[137] If, however, no adequacy decision exists, then companies cannot transfer data except "subject to appropriate safeguards," a limited list of options that includes establishing binding corporate rules and standard contract clauses.[138] Binding corporate rules, however, are limited to international transfers within the same company or "group of enterprises engaged in a joint economic activity."[139]

The United States has occupied a somewhat unique position with respect to the EU's adequacy determinations. The United States has never sought an adequacy decision, most likely because it would be sure to fail.[140] Instead, the EU and United States negotiated a compromise, the 2000 Safe Harbor framework, under the DPD.[141] Under the Safe Harbor,

---

130. Art. 3(1) can be understood as codifying the jurisdiction holding in the 2014 CJEU *Google Spain* opinion, which held that Google could be covered by European law even though it was processing data in the United States. Case C-131/12, Google Spain SL v. González, ECLI:EU:C:2014:317, ¶¶ 45–60 (May 13, 2014).

131. GDPR, *supra* note 2, at art. 3(1).

132. *Id.* at art. 3(2)(a)–(b).

133. *Id.* at Recital 23.

134. Recital 23 explains that regulators will assess a number of factors, including language, currency, possibility of ordering goods or services from the EU, or mentioning customers or users in the EU. *Id.*

135. "The European Commission has so far recognised Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland . . . Uruguay" and the United States of America (limited to the Privacy Shield framework) "as providing adequate protection." *Adequacy Decisions*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Nov. 4, 2020).

136. Schwartz & Peifer, *supra* note 4, at 118; GDPR, *supra* note 2, at Recitals 103–07, art. 45.

137. GDPR, *supra* note 2, at art. 45.

138. *Id.* at art. 46–47, 93.

139. *Id.* at Recital 110.

140. Schwartz & Peifer, *supra* note 4, at 118.

141. U.S. DEP'T OF COM., SAFE HARBOR PRIVACY PRINCIPLES AND RELATED FREQUENTLY ASKED QUESTIONS (2000); Commission Decision 2000/520, art. 1, 2000 O.J. (L 215) 7, 8 (EC).

the Commission agreed that U.S. companies that self-certified to the voluntary Safe Harbor principles could export EU persons' data.[142] In 2015, however, the Grand Chamber of the CJEU (which is basically the CJEU sitting en masse) invalidated the Safe Harbor in *Schrems v. Data Protection Commissioner*[143] (*Schrems I*), finding that the United States failed to protect EU persons from extensive national security surveillance.[144]

In place of the Safe Harbor, the United States and the Commission established the similar Privacy Shield, again a self-certification mechanism to a set of privacy principles.[145] Once again, a legal challenge to the arrangement—again made by Max Schrems and known as *Schrems II*—made its way up to the CJEU.[146] In July 2020, the CJEU invalidated the U.S.–EU arrangement for a second time.[147] While the court generally upheld another mechanism for international data transfers, standard contractual clauses, its reasoning about the scope of national security surveillance and the lack of judicial recourse for EU persons in the United States threatens the use of this transfer mechanism in the U.S. context.[148] *Schrems II* thus will greatly affect the business practices of many transnational companies that process EU persons' data in the United States, causing them either to reevaluate the contractual clauses used or to house data for processing in Europe.

Next, we turn to the question of what the GDPR covers. Unlike most U.S. data privacy laws, which take a sectoral approach to privacy, the GDPR represents an omnibus data protection regime.[149] It covers the processing of personal data, with both "processing" and "personal data" defined broadly. Personal data includes not just personally identifying data but personally *identifiable* data, reaching broader than U.S. laws that focus on discrete categories of information such as names or Social Security Numbers.[150] Processing, too, is defined broadly to include nearly

142. Commission Decision 2000/520, *supra* note 141, at Recital 5.

143. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015).

144. *Id.* ¶ 7.

145. *Privacy Shield Overview*, PRIV. SHIELD, https://www.privacyshield.gov/Program-Overview (last visited Nov. 5, 2020).

146. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd., ECLI:EU:C:2020:559 (July 16, 2020).

147. *Id.* ¶¶ 199–202.

148. *Id.* ¶¶ 8, 14, 199–202.

149. Schwartz & Peifer, *supra* note 4, at 128.

150. *See* GDPR, *supra* note 2, at art. 4(1).

> "[P]ersonal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[.]

Id.; *see also id.* at Recitals 26, 28, 29, 30; Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1887–93 (2011).

anything one could do with data.[151] There are exceptions to the GDPR's broad coverage, such as the household activity exception,[152] Member State-enacted exceptions for freedom of expression and journalism,[153] and areas such as national security and policing.[154] The default scope of the GDPR's coverage, however, is extremely broad.

Finally, we turn to the "whom." Unlike U.S. laws like the Health Insurance Portability and Accountability Act[155] (HIPAA) or even the recently effective California Consumer Privacy Act[156] (CCPA) that apply to only specific entities, the GDPR applies to all entities that process personal data—with the significant exceptions of law enforcement and national security.[157] However, the GDPR divides entities into different categories that are subject to different requirements.[158]

The GDPR governs the behavior of two categories of entities: "data controllers" and "data processors."[159] These entities are defined by the extent to which they directly control data processing (a controller) versus perform the processing on behalf of another company (a processor). Both government and private entities can be controllers or processors under the GDPR.[160] This terminology is taken from the GDPR's predecessor, the DPD.[161] Interpretative guidance and legal decisions under the DPD can be helpful for understanding the distinction between the two types of entities.[162]

The GDPR diverges from the DPD on its treatment of these entities, however, in two important ways: (1) it assigns obligations to both con-

---

151. *See* GDPR, *supra* note 2, at art. 4(2).

> "[P]rocessing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Id.

152. *Id.* at Recital 18, art. 2(2)(c).

153. *Id.* at Recital 153, art. 85.

154. *Id.* at art. 23.

155. Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

156. CAL. CIV. CODE § 1798.145(c)(1) (West 2020).

157. GDPR, *supra* note 2, at art. 2(2)(d).

158. *See, e.g.*, *id.* at art. 24 (establishing what is the "responsibility of the controller," a category of entity).

159. *Id.* at art. 4(7)–(8); *see id.* at arts. 24–43.

> "[C]ontroller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law . . . .

Id. at art. 4(7). "'[P]rocessor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller . . . ." *Id.* at art. 4(8).

160. *See id.* at arts. 4(7)–(8), 24–43.

161. Directive 95/46/EC, *supra* note 67, at art. 2(d)–(e).

162. *See, e.g.*, Peter Blume, *An Alternative Model for Data Protection Law: Changing the Roles of Controller and Processor*, 5 INT'L DATA PRIV. L. 292, 293 (2015).

trollers and processors; and (2) it introduces the concept of the "joint controller," or a second controller equally responsible for controller obligations.[163] Even with the added obligations imposed on processors, one of the most significant decisions a lawyer applying the GDPR must make is whether their client is a controller or a processor.

B. The GDPR's Requirements: Individual Rights and Company Obligations

In sum, the GDPR consists of two approaches to data protection: a set of individual rights and a set of company obligations.[164] These two approaches overlap. A number of individual rights are also obligations on companies, and a number of company obligations serve as systemic protections for individual rights.[165] Many U.S. readers, however, focus on the GDPR's individual rights and either miss or downplay the substantial obligations on companies.[166] This is a mistake. Much of the work the GDPR aspires to do is beneath the surface, changing corporate infrastructure and processes and reprioritizing decision-making around data protection rights and values.[167]

Those who are familiar with the FIPs are likely aware of the GDPR's individual rights. These rights are understood as founded on the Charter's protection of personal data, which requires both a right of access and right of rectification.[168] The GDPR establishes notification rights, a right of access, a right to rectification, a right to erasure (or "right to be forgotten"), a right to restriction of processing, a right to data portability, a right to object to processing, and several rights with respect to automated decision-making.[169]

The detailed substance of these rights is beyond the scope of this Guide. However, we note two overarching observations. First, as is typical of a true data protection regime, the GDPR's individual rights do not hinge on whether a person has a direct consumer relationship with a company. They attach to the personal data, regardless of who holds that

---

163. Edwards, *supra* note 4, at 6.

164. GDPR, *supra* note 2, at arts. 12–23 (explaining the rights of the data subject); *id.* at arts. 24–43 (explaining the duties of a controller and processor); *id.* at arts. 44–50 (explaining transfers to third countries).

165. *See, e.g.*, *id.* at arts. 13–14 (explaining the notification obligations); *see also* Kaminski & Malgieri, *supra* note 112, at 3.

166. *See* Kaminski, *supra* note 111, at 1560 (providing a discussion on the impact the GDPR has on company infrastructure and heuristics); *see also* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377 (2006).

167. Kaminski, *supra* note 111, at 1585.

168. Charter of Fundamental Rights, *supra* note 28, at art. 8.

169. GDPR, *supra* note 2, at arts. 13–18, 20–22. The FIPs principles of data security and data breach notifications are also present in the GDPR but are listed among company responsibilities rather than individual rights. *Id.* at arts. 32–34.

data.[170] A third-party data broker has obligations to notify individuals, to enable them to access data, to correct data, and so on.[171]

Second, the GDPR's individual rights are replete with both specific rules on the one hand, and broader standards and balancing tests on the other.[172] The GDPR's balancing tests may seem particularly strange to a U.S.-based reader. Take, for example, the right to object to processing.[173] An individual may object to data processing done on "legitimate interest" grounds.[174] To continue processing the data, a company must "demonstrate[] compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject."[175] To a U.S. lawyer accustomed to various levels of constitutional scrutiny, including strict scrutiny, it may be strange to think of fundamental rights as something that can be balanced against other interests.[176] Even stranger is the notion that a company, rather than a court, might be tasked with doing the balancing.

This brings us to the other side of the GDPR: corporate governance. The GDPR imposes significant obligations on companies, aimed at creating compliance infrastructure, pushing companies to make rights-based engineering decisions, and performing rights-based risk assessments.[177] In general, the GDPR's company obligations try to force corporate culture to take data protection seriously.

As discussed above, a core principle of the GDPR is accountability.[178] A data controller is both "responsible for[] and [must] be able to demonstrate compliance with" the requirements of the GDPR.[179] International internet-policy scholar Lilian Edwards has pointed out that this accountability principle replaces the old requirement under the DPD that companies notify their local authority before data processing.[180] Instead of requiring that companies first check in with the government, the GDPR tasks companies with significant compliance responsibilities.[181]

Thus, each data controller must maintain records of data processing activities.[182] Data protection authorities (DPAs) have the power to order

---

170. *Id.* at arts. 2–3.
171. *See, e.g.*, *id.* at art. 14.
172. *Id.* at Recitals 4, 47.
173. *Id.* at art. 21.
174. *Id.* For more information about legitimate interests, see PROCESSING PERSONAL DATA, *supra* note 90, at 5–8.
175. GDPR, *supra* note 2, at art. 21(1).
176. *See* Sweet & Mathews, *supra* note 33, at 78–79.
177. *See* Edwards, *supra* note 4.
178. GDPR, *supra* note 2, at art. 5(2).
179. *Id.*; *see also The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data* (July 13, 2010), https://www.dataprotection.ro/servlet/ViewDocument?id=720.
180. Edwards, *supra* note 4, at 21; Directive 95/46/EC, *supra* note 67, at art. 18.
181. Edwards, *supra* note 4, at 19–21.
182. GDPR, *supra* note 2, at art. 30.

companies to "provide any information [they] require[] for the performance of [their] tasks," and to conduct data protection audits.[183] Companies that conduct data processing that "is likely to result in a high risk to the rights and freedoms of natural persons" must further conduct data protection impact assessments.[184] High-risk data processing includes large-scale processing of sensitive data (special category data[185]) and large-scale systematic monitoring of public places.[186] For particularly risky processing, companies must share the impact assessment with, and consult with, regulators.[187] While the GDPR's risk assessment process is not perfect, it represents an attempt to saddle companies with responsibilities for protecting individual rights on a systemic level and can meaningfully feed back into, or even help constitute, a number of individual rights.[188]

The GDPR explicitly attempts to influence both technological development and organizational infrastructure. For example, the requirement of "data protection by design and by default" requires companies to integrate data protection values into the technologies they build and use and into their organizational processes and infrastructure.[189] As another example of the focus on organizational infrastructure, the GDPR requires many companies to establish an internal Data Protection Officer (DPO).[190] That person must be an independent expert who reports to the highest level of management.[191] The DPO is tasked with monitoring compliance (including staff training and audits), providing advice, and acting as the go-between with regulators.[192] The DPO must be provided with both resources and access to information.[193]

One of us has argued that the GDPR's approach to corporate governance contains the hallmarks of collaborative governance.[194] Often, the

---

183. *Id.* at art. 58(1)(a)–(b).

184. *Id.* at art. 35.

185. *Id.* at art. 9(1).

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Id.

186. *Id.* at art. 35. Data protection authorities are also tasked with making publicly available lists of the kinds of data processing that require impact assessments. *Id.*

187. *Id.* at art. 36.

188. See Kaminski & Malgieri, *supra* note 112, at 4–5, for discussion of impact assessments.

189. GDPR, *supra* note 2, at art. 25.

190. *Id.* at art. 37. A DPO is required where "core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale," or core activities are large-scale processing of sensitive data. *Id.* at art. 37(1)(b).

191. *Id.* at art. 38.

192. *Id.* at art. 39.

193. *Id.* at art. 38.

194. *See* Kaminski, *supra* note 111, at 1537.

regulation implicitly or explicitly tasks private companies with self-monitoring and determining the substance of the regulation.[195] This approach should not, however, be confused with self-regulation. The GDPR's enforcement and oversight mechanisms, extensive rules and guidance, and the backing of an active human rights court make it clear that this is not a hands-off, self-regulatory regime.[196] It is rather an attempt to make a complex general regulation both sector specific and iterative, so that substantive standards produced now will affect technologies and practices of the future.

Finally, the GDPR provides a novel form of enforcement through Article 80. Data subject rights may be exercised by the individual or through "collective redress," outlined in Article 80.[197] Collective redress is similar to U.S. class action claims. This approach to compliance has traditionally carried less policy prominence in Europe,[198] but reports and studies developed as part of drafting the GDPR outlined the challenges to enforcement and argued for more options.[199] Article 80 states that Non-Governmental Organizations (NGOs) represent data subjects across the spectrum of enforcement actions including lodging complaints with the DPA, challenging a DPA determination, or seeking redress against a controller or processor in court.[200] But collective redress rules have not been established, and whether an NGO can exercise certain rights and perform certain functions depends on the laws of the Member States, which vary greatly.[201]

C. Complementary Data Protection Laws

It may surprise many Americans to learn that the GDPR is not the only EU-wide privacy law. The GDPR is a general regime, but there are a number of what might be characterized as sector-specific regimes that exist as well.[202] The GDPR is referred to as a *lex generalis*: a general law

---

195. *See, e.g.*, GDPR, *supra* note 2, at arts. 40–43.

196. *See generally* Kaminski, *supra* note 111, at 1596–99.

197. GDPR, *supra* note 2, at art. 80.

198. Or perhaps even traditional hostility. *See* S.I. Strong, *Cross-Border Collective Redress in the European Union: Constitutional Rights in the Face of the Brussels I Regulation*, 45 ARIZ. ST. L.J. 233, 233 (2013) (Europe as a region has been "hostile to the provision of large-scale private litigation"). European collective action policy has developed slowly and inconsistently due in large part to reliance on public enforcement and administrative measures used to regulate markets and market actors. *See* Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMPAR. L. 411, 417 (2011).

199. EUR. UNION AGENCY FOR FUNDAMENTAL RTS., ACCESS TO DATA PROTECTION REMEDIES IN EU MEMBER STATES 11–12 (2014); *Action Needed to Better Reinforce Data Protection Rights*, EUR. UNION AGENCY FOR FUNDAMENTAL RTS. (Aug. 7, 2014), http://fra.europa.eu/en/news/2014/action-needed-better-reinforce-data-protection-rights.

200. GDPR, *supra* note 2, at art. 80.

201. *See* Laima Jančiūtė, *Data Protection and the Construction of Collective Redress in Europe: Exploring Challenges and Opportunities*, 9 INT'L DATA PRIV. L. 2, 8–9 (2019).

202. *See, e.g.*, Waltraut Kotschy, *The Proposal for a new General Data Protection Regulation—Problems Solved?* 4 INT'L DATA PRIV. L. 274, 275–76 (2014).

that creates restrictions and requirements for personal data.[203] A *lex specialis*—or a law that particularizes and complements the general rules—takes precedence over the general law.[204]

The most well-known non-GDPR EU digital privacy laws are those that apply to cookies. These were introduced by the 2002 ePrivacy Directive (ePD), amended in 2009.[205] As an EU directive, the ePD required harmonization but was not directly binding on Member States.[206] Thus, Member States enacted national laws implementing the ePD that remain in effect and govern communication privacy and cookie practices.[207] But because the ePD references the DPD—now the GDPR—interpretation of these laws requires multiple documents. Currently, the Council and Parliament of the EU are negotiating a directly binding update: the ePrivacy Regulation.[208] If passed, this regulation would cover the storage and accessing of communication, not personal data (though the two are often one and the same), and, at least in draft form, is primarily a consent-based regime.[209]

There are multiple other EU-wide laws that potentially overlap with the GDPR's coverage. For example, the GDPR does not speak to entering contracts. The 2000 e-Commerce Directive removes legal obstacles to electronic contracting.[210] The e-Commerce Directive also governs intermediary liability—that is, the liability online platforms have for content that appears on them.[211] The Consumer Rights Directive governs business-to-consumer markets, aligning national consumer laws that detail, for example, the information a consumer needs to be given prior to

---

203. *See id.* at 276.

204. *See id.*

205. Directive 2009/136, of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No. 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11 [hereinafter Directive 2009/136/EC]; *see* Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sectior, 2002 O.J. (L 201) 37.

206. *See* Directive 2009/136/EC, *supra* note 205.

207. *Opinion 5/2019 on the Interplay Between the ePrivacy Directive and the GPR, in Particular Regarding Competence, Tasks and Powers of Data Protection Authorities*, European Data Protection Board (12 March 2019).

208. *EU Council Presidency Releases Progress Report on Draft ePrivacy Regulation*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (June 4, 2020), https://www.huntonprivacyblog.com/2020/06/04/eu-council-presidency-releases-progress-report-on-draft-eprivacy-regulation/.

209. Meg Leta Jones & Jenny Lee, *Comparing Consent to Cookies: A Case for Protecting Non-Use*, CORNELL INT'L L.J. (forthcoming 2020).

210. Directive 2000/31/EC, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on electronic commerce'), 2000 O.J. (L 178) 1, 11.

211. *Id.*

purchasing something and the rights and means to cancel online purchases.[212]

Another important form of parallel protection comes from the Data Protection Law Enforcement Directive (LED), which provides protections when personal data is processed in connection with criminal offenses or through the execution of criminal penalties.[213] The LED applies when the processing of personal data is performed by a data controller with "competent authority" and for "law enforcement purposes."[214] If a law enforcement agency processes personal data for non-law enforcement purposes (e.g., human resources), other laws like the GDPR may apply.

These are only a few examples of the "sectoral" EU rules that exist alongside, or in addition to, the GDPR. U.S. lawyers who advise their clients on GDPR obligations should remain aware of the thicket of other possibly applicable EU regulatory regimes.

III. HOW TO READ THE GDPR

Despite its length, the GDPR is not often detailed or precise. It states its requirements in vague or aspirational language.[215] In this Part, we explain how to read the GDPR and point to several helpful resources not immediately apparent from the GDPR's text. Many practitioners and academics use the online version of the GDPR available at https://gdpr-info.eu/, which links each Article of the GDPR to the corresponding Recital or Recitals. This website is also searchable and contains a subsection on commonly used keywords.

The GDPR frequently, though not always, contains broad language that requires interpretation. For example, the duty of Data Protection by Design and by Default in Article 25 requires data controllers to "implement appropriate technical and organisational measures . . . which are designed to implement data-protection principles . . . in an effective manner . . . in order to meet the requirements of this Regulation and protect the rights of data subjects."[216]

How is one to interpret this provision in a way that helps a company comply with it? First, the GDPR's text itself contains a few examples:

212. Directive 2011/83/EU, of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, Amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and Repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, 2011 O.J. (L 304) 7, 20, 24, 47, 48, 49.

213. Directive 2016/680, 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 by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 4, 7, 11 (EU).

214. *Id.*

215. Hoofnagle et al., *supra* note 4, at 67.

216. GDPR, *supra* note 2, at art. 25(1).

pseudonymization is provided as an example of an appropriate technical measure, and data minimization is given as an example of a data protection principle.[217] Often, the GDPR's text provides an open list of examples to illustrate broader principles.

Second, the GDPR's text is accompanied by a long preamble, known as the Recitals.[218] The 173 GDPR Recitals are not, strictly speaking, the law. Instead, they serve as interpretative instruments through which courts and DPAs may, and usually do, interpret the GDPR's text.[219] Often, political compromises that did not make it into the GDPR's text itself made it into the Recitals, which can confuse things as Recitals are not supposed to create new law. That said, when the GDPR's text is vague, companies would be well-advised to look to the Recitals for further clarity, since this is what the GDPR's other interpreters (including regulators) will be doing.

In the case of Data Protection by Design, Recital 78 on "Appropriate Technical and Organisational Measures" may help fill in some of the text's vagueness.[220] The Recital provides additional examples of technical and organizational measures beyond the GDPR's text.[221]

Often, the combination of GDPR text and Recitals itself is not enough. This is where what were formerly known as Article 29 Working Party Guidelines (Guidelines) come into play. The Article 29 Working Party was a coordinating group of DPAs from each EU Member State that operated under the GDPR's predecessor, the DPD, to issue guidelines on key provisions of European data protection law.[222]

Under the GDPR, the European Data Protection Board (EDPB) replaced the Article 29 Working Party.[223] The EDPB has endorsed the Article 29 Working Party Guidelines on the GDPR.[224] Thus, these Guidelines represent the opinion of a coordinated group of data protection regulators from across the EU, tasked with helping to harmonize data protection law under the GDPR.[225] The Guidelines are not hard law, but given the deference they will likely receive from national regulators, companies ignore them at their peril.

---

217. *Id.*

218. *See id.* at Recitals 1–173.

219. For a discussion of the limited role played by Recitals in EU law as interpreted by the CJEU, see Roberto Baratta, *Complexity of EU Law in the Domestic Implementing Process*, 2 THEORY & PRAC. LEGIS. 293 (2014) ("Recitals can help to explain the purpose and intent behind a normative instrument. They can also be taken into account to resolve ambiguities in the legislative provisions to which they relate, but they do not have any autonomous legal effect.").

220. GDPR, *supra* note 2, at Recital 78.

221. *Id.*

222. *Article 29 Working Party Archives 1997 – 2016*, EUR. COMM'N, https://ec.europa.eu/justice/article-29/documentation/index_en.htm (last visited Nov. 5, 2020).

223. GDPR, *supra* note 2, at art. 68.

224. European Data Protection Board, *Endorsement 1/2008 of GDPR WP29 Guidelines* (May 25, 2018).

225. *Id.*

While not comprehensive, the Guidelines address a wide variety of topics. These include data breach notification, the right to data portability, Data Protection Impact Assessments, consent, transparency, and automated decision-making.[226] The EDPB continues to issue guidelines, first as drafts for public consultation and then as final versions.[227] The Guidelines are available at https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.[228]

But what if, as is the case with data protection by design, there is no set of guidelines yet available from the EDPB? Then practitioners may want to turn to interpretations offered by individual Member State authorities. At least until Brexit happens, the United Kingdom's (UK) Information Commissioner's Office (ICO) is a steady source of relatively clear GDPR interpretation. For example, the ICO has a fairly extensive webpage on data protection by design, which refers in turn to the seven "privacy by design" principles that originated with the Information and Privacy Commissioner of Ontario, and to other resources.[229] The ICO's Guide to the GDPR is available online at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.[230] It is important to note, however, that the UK implemented the GDPR in the Data Protection Act 2018, and thus technically, the ICO's advice is for businesses attempting to comply, not with the GDPR, but with the UK's Act.[231] There is no guarantee that the UK's implementation in fact fully embodies the GDPR's requirements, and in other Member States with other implementing laws, the ICO's advice may be inapplicable.

A number of other national DPAs have issued guidelines on a variety of issues. Many national DPAs have a "guidelines" section on their websites. France produced guidelines on online tracking[232] and facial

---

226. *Id.*

227. *GDPR: Guidelines, Recommendations, Best Practices*, EUR. DATA PROT. BD., https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (last visited Nov. 5, 2020).

228. *Id.*

229. *Guide to Data Protection Regulation (GDPR): Data protection by design and default*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (last visited Nov. 5, 2020).

230. *Id.*

231. *Id.*

232. Press Release, Comm'n nationale de l'informatique et des libertés (CNIL), Cookies and Other Tracking Devices: the CNIL Publishes New Guidelines (July 23, 2019) (on file with authors); Commission nationale de l'informatique et des libertés,"Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) (rectificatif)," Guidelines (in French) (July 4, 2019), https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337.

recognition;[233] the Irish DPA issued guidelines on data breaches, impact assessments, and Brexit;[234] and the Dutch DPA recently issued guidelines on privacy policies.[235]

The GDPR is ultimately interpreted by courts, as are the underlying fundamental rights to privacy and data protection established in the Charter.[236] The Charter applies to EU lawmakers and to national authorities implementing EU law.[237] This means that when the GDPR is applied, the CJEU may ultimately end up hearing a case either on the interpretation of the GDPR or on its compatibility or incompatibility with the Charter rights—effectively, its constitutionality.[238]

CJEU cases can be searched at https://europa.eu/european-union/law/find-case-law_en or at https://eur-lex.europa.eu/collection/eu-law/eu-case-law.html.[239] Additionally, CJEU cases can be found according to a classification scheme, which includes case listings organized by fundamental right.[240]

The CJEU is made up of one judge from each EU country and eleven Advocates General.[241] The Advocate General's role may be novel to U.S. lawyers, as an Advocate General is neither a party to the case nor a judge.[242] If the CJEU determines that there is a novel legal issue, an Advocate General will be asked to issue an opinion prior to the CJEU's opinion. That opinion is advisory rather than binding, though Advocates Generals' opinions are influential and usually followed by the CJEU.[243] The opinions are written more broadly and comprehensively than the final CJEU opinion, in which there are no dissents.

---

233. COMM'N NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, FACIAL RECOGNITION: FOR A DEBATE LIVING UP TO THE CHALLENGES GUIDELINES 1 (unofficial English trans., 2019).

234. *Data Protection Commissioner Guidance*, IR. DATA PROT. COMM'N, https://www.dataprotection.ie/en/dpc-guidance (last visited Nov. 5, 2020).

235. *Rapportage Verkennend onderzoek Gegevensbeschermingsbeleid*, AUTORITEIT PERSOONSGEGEVENS (Apr. 17, 2019), https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_verkennend_onderzoek_gegevenschermingsbeleid.pdf.

236. Charter of Fundamental Rights, *supra* note 28, at art. 52(5).

237. *Id.* at art. 5(7).

238. *Court of Justice of the European Union (CJEU)*, *supra* note 40 (National courts interpret EU law, but can ask or refer a question about EU law (or about whether a national law or practice complies with EU law) to the CJEU to gain clarification. Private individuals and an EU government (EU Council, Commission, or Parliament) can also ask the CJEU to annul an EU act that violates EU treaties or fundamental rights).

239. *Find Case-Law*, EUR. UNION, https://europa.eu/european-union/law/find-case-law_en (last visited Nov. 5, 2020); *Case Law*, EUR-LEX, https://eur-lex.europa.eu/collection/eu-law/eu-case-law.html (last visited Nov. 5, 2020).

240. *See Directory of Case-Law*, EUR-LEX, https://eur-lex.europa.eu/browse/directories/new-case-law.html?root_default=RJ_NEW_1_CODED%3D1 (last visited Nov. 5, 2020).

241. *See Court of Justice of the European Union (CJEU)*, *supra* note 40.

242. *Role of Advocates General at the CJEU*, EUR. PARLIAMENT (Oct. 10, 2019), https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)642237.

243. *Id.*

In other ways, too, CJEU cases look a bit different than U.S. and other common law cases. They begin with party and procedural details and then state excerpts from the relevant law or laws, listing the applicable legal language verbatim without commentary. The facts are then presented and are followed by analysis, including the previously mentioned law and references to other cases.

As discussed in Part I, the right to data protection is not absolute and can be limited by general interest or the protection of rights and freedoms of others.[244] Article 8 of the Convention and Article 52 of the Charter contain the conditions for limiting privacy and data protection rights.[245] Under EU law, limitations to any fundamental right, including data protection, are lawful only if they are done in accordance with the law, respect the essence of the right, are subject to the principle of proportionality, and are performed in pursuit of a general objective recognized by the EU or the need to protect the rights of others.[246] As such, it is important to read the GDPR keeping in mind what it does not govern—e.g., national security and issues related to the press—because the EU does not have legislative competence deriving from any relevant treaty.

Few cases have been decided since the GDPR went into effect, but a number of recent, high-profile cases reveal the complicated nature of EU law. For instance, in September 2019, the CJEU further defined the bounds of the right to be forgotten it had recognized in 2014,[247] as well as the explicit right to erasure more recently granted by the GDPR.[248] The case arose because in 2015, the French data protection agency (CNIL) called for Google, Inc. to implement the 2014 right-to-be-forgotten ruling limiting access to search results globally.[249] In 2016, Google used geoblocking to prevent those within the EU from retrieving results that were deindexed as a result of a right to be forgotten request.[250] The CNIL imposed a fine and Google appealed.[251] The Advocate General produced an opinion in January 2019, stating that search engines should only have to prevent access to personal data within the EU, not globally.[252] The CJEU agreed, explaining, "[t]he right to the protection of personal data is not an absolute right; it must be considered

244. Sweet & Mathews, *supra* note 33, at 78.

245. Convention on Human Rights, *supra* note 30, at art. 8; Charter of Fundamental Rights, *supra* note 28, at art. 52(5).

246. Charter of Fundamental Rights, *supra* note 28, at art. 52(1).

247. Case C-131/12, Google Spain SL v. AEPD, ECLI:EU:C:2014:317, ¶ 3 (May 13, 2014) (note, that in this case the CJEU did not follow the advocate general's opinion. ECLI:EU:C:2014:317 – Opinion Advocate-General Jääskinen of June 25, 2013).

248. GDPR, *supra* note 2, at art. 17.

249. Case C-507/17, Google LLC v. CNIL, ECLI:EU:C:2019:772, ¶ 2, 30-33 (Sept. 24, 2019).

250. *Id.* at 32.

251. *Id.* at 33–34.

252. Case C-507/17, Google LLC v. CNIL, ECLI:EU:C:2019:15 – Opinion Advocate General Szpunar, ¶¶ 47-50 (Jan. 10, 2019).

in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[253] The court, however, did not declare global removal impossible.[254] Instead, it found extra-territorial application of the right to be forgotten to be a matter of country-specific assessment of their own international jurisdiction law.[255]

National courts are starting to issue interpretations of the GDPR as well. In February 2020, a French court intervened in the use of facial recognition at schools. A regional test of the technology had been planned for the gates of one high school located in Nice and another in Marseille and conditioned access to the school grounds on facial recognition.[256] Three nonprofits challenged the decision in the Administrative Court of Marseille, but while the court considered the case, CNIL issued a notice clarifying its position against the tests[257] and later another notice further emphasizing its opposition[258] to political criticism from local leaders.[259] The court agreed with CNIL's interpretation.[260] The tests used the legal basis of consent for processing, but the court found that the signature of students or guardians on a form was insufficient for the type of biometric data at issue.[261] Additionally, the court found the region failed in terms of proportionality because it had not articulated why less intrusive measures would not achieve the purposes for processing.[262]

---

253. Case C-507/17, Google LLC v. CNIL, ECLI:EU:C:2019:772, ¶ 13 (Sept. 24, 2019).

254. *Id.* at ¶¶ 60–61.

255. *Id.* ¶ 72.

> A supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights (see, to that effect, judgments of 26 February 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, paragraph 29, and of 26 February 2013, Melloni, C-399/11, EU:C:2013:107, paragraph 60), a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine.

Id.

256. Press Release, Comm'n nationale de l'informatique et des libertés, Experimentation with Facial Recognition in Two High Schools: the CNIL Clarifies its Position (Oct. 29, 2019) (unofficial English trans.) (on file with authors).

257. *Id.*

258. CNIL, FACIAL RECOGNITION: FOR A DEBATE LIVING UP TO THE CHALLENGES 2 (2019) (unofficial English trans.).

259. @RenaudMuselier, TWITTER (Oct. 29, 2019, 8:10 AM), https://twitter.com/RenaudMuselier/status/1189182719239999491?s=20 (Renaud Muselier, president of the region at issue, tweeted that the CNIL was out of date and that facial recognition promoted safety and educational goals); *see also* Christian Estrosi & Bertrand Ringo, *Criminalité, Délinquance: Les Choix Dogmatiques de la Cnil*, L'OPINION (Dec. 24, 2019), https://www.lopinion.fr/edition/politique/criminalite-delinquance-choix-dogmatiques-cnil-tribune-christian-206816 (Mayors of Nice and Gravelines were also openly critical of the CNIL).

260. Tribunal administratif de Marseille du 27 février 2020, n° 1901249, La Quadrature du Net et autres, https://forum.technopolice.fr/assets/uploads/files/1582802422930-1090394890_1901249.pdf.

261. *Id.*

262. *Id.*

We close with some source recommendations that should be useful for those trying to keep track of changes and understand the law in greater depth. In order to keep up with the changing landscape of data protection law, we recommend the International Association of Privacy Professionals' website (www.IAPP.org)[263] and daily email subscription (https://iapp.org/news/daily-dashboard/).[264] For updated analysis coming out of Europe, we recommend the *European Data Protection Law Review* and the journal *International Data Privacy Law*.[265] To build a strong foundation, we recommend the *Handbook of European Data Protection Law*, updated annually and published by the European Union Agency for Fundamental Rights and free to download.[266] For reference materials, we recommend *The EU General Data Protection Regulation (GDPR): A Commentary*, which is a carefully and richly annotated version of the GDPR edited by Christopher Kuner, Lee Bygrave, Christopher Docksey, and Laura Dreschsler.[267] We also recommend Lilian Edwards's book *Law, Policy, & the Internet* (2018)[268] and Orla Lynskey's book *The Foundations of EU Data Protection Law* (2015).[269]

CONCLUSION

It is challenging for American lawyers starting from scratch to understand the complex system that is the GDPR, or the legal context in which the law exists. American lawyers representing clients affected by the GDPR, academics who plan to write about or teach the GDPR, and policymakers attempting to draft new data privacy law all need an easier entry point for understanding this vast regulation. It is our hope that this Article provides that entry point.

The GDPR is based on the European fundamental right to data protection, a positive right distinct from privacy.[270] The GDPR is made up of 99 Articles and a 173-section Preamble with guiding Recitals.[271] It includes both individual rights and data controller/processor obligations.[272] While individual rights are important to meaningful individual control and European data protection, the GDPR is not a consent-based piece of legislation.

---

263. IAPP, https://iapp.org/ (last visited Nov. 5, 2020).

264. *Daily Dashboard*, IAPP, https://iapp.org/news/daily-dashboard/ (last visited Nov. 5, 2020).

265. *European Data Protection Law Review*, LEXXION, https://edpl.lexxion.eu/ (last visited Nov. 5, 2020); *About: International Data Privacy Law (IDPL) Journal*, OXFORD ACAD., https://academic.oup.com/idpl/pages/About (last visited Nov. 5, 2020).

266. EUROPEAN DATA HANDBOOK, *supra* note 58.

267. The EU General Data Protection Regulation (GDPR): A Commentary (Christopher Kuner et al. eds., 2020).

268. Edwards, *supra* note 4.

269. ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW (2015).

270. GDPR, *supra* note 2, at art. 1.

271. *See id.*

272. *Id.*

There are a number of sources beyond the GDPR itself that are relevant to understanding the evolving state of European data protection law. The CJEU interprets the Charter and hears data protection cases referred to it by Member States' courts.[273] The EDPB actively produces guiding opinions on timely issues to help harmonize data protection law under the GDPR.[274] Member States' national interpretations of the GDPR may be particularly important to those advising clients and require knowledge of the data protection agency culture and communications, national law either passed or amended to adhere to GDPR, and the court structure of the Member State. Most areas of U.S. law have a corresponding area of EU law, but what Americans refer to as information privacy could be addressed in the GDPR or may more specifically be addressed in European consumer protection, e-commerce, law enforcement, or privacy directives.

Finally, as the conversation around enacting U.S. data privacy law continues, understanding the GDPR becomes only more important.[275] Whether the goal of new U.S. laws is to harmonize with the GDPR or depart from it, the only way to do either is to know what the GDPR is to begin with.

273. *See, e.g.*, *Court of Justice of the European Union (CJEU)*, *supra* note 40.

274. *Opinions*, EUR. DATA PROT. BD., https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en (last visited Nov. 5, 2020).

275. *See* Chander et al., *supra* note 11 (manuscript at 3–4).