Privacy Statements Under the GDPR

*Mike Hintze**

INTRODUCTION

The European General Data Protection Regulation (GDPR)[1] imposes many onerous compliance obligations that affect companies worldwide. Those subject to the GDPR must evaluate the risk of all their data processing obligations and prepare formal data protection impact assessments (DPIAs) on those that are higher risk.[2] They must ensure that contracts with vendors and service providers contain specific data protection terms set out by the Regulation.[3] They must implement systems and processes capable of responding to requests from individuals exercising their rights under the GDPR, including rights to access, correct, port, delete, or restrict the processing of personal data.[4] They must implement product development processes and policies to meet the law's new "data protection by design" requirements.[5] And there are many others.

The need to include specific types of information in a privacy statement is a GDPR compliance obligation that does not get as much attention as some other GDPR requirements.[6] Perhaps that is because

* Partner, Hintze Law PLLC; Affiliate Instructor of Law, University of Washington School of Law; and Senior Fellow, Future of Privacy Forum. The views expressed in this Article are my own and do not necessarily reflect the positions of any current or former employer or client.

1. Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 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].

2. *Id.* art. 35, at 53.

3. *Id.* art. 28(3), at 49.

4. *Id.* arts. 15–20, at 43–45.

5. *Id.* art. 25, at 48.

6. This Article uses the term "privacy statement," rather than "privacy policy" or "privacy notice" to refer to the public-facing document describing an organization's privacy-related practices. While all three terms are commonly used to describe this type of document, the terms "privacy policy" and "privacy notice" are less specific and can lead to confusion. For instance, the term "privacy policy" is also frequently used to refer to an organization's set of internal policies and guidelines that govern personal data. This internal policy is typically focused on principles and rules that internal personnel use to guide product design and data management practices. By contrast, the external "privacy statement" is in large part a factual document that describes in detail how that internal policy has been

privacy statements have been much maligned in recent years. They are too long and full of legalese. Nobody reads them. They are part of a notice and consent approach to privacy that puts an unrealistic burden on consumers to make informed choices. But despite these well-known criticisms, the GDPR doubles down on privacy statements. In fact, gauging by the roughly fourfold increase in privacy statement requirements compared to the previous law, the GDPR quadruples down.

As a result, ensuring that a privacy statement is GDPR-compliant is one of the more important obligations that companies must navigate. And meeting the privacy statement requirements effectively is not as simple as it might first appear. This Article discusses how companies should approach and craft their privacy statements to meet these new GDPR requirements, thereby reducing their risk.

Part I describes the new obligations to provide notice under the GDPR, including what kinds of organizations must have a privacy statement and the contents of that privacy statement. Part II discusses several important stylistic and design decisions that go into creating a privacy statement, which are an important part of meeting the GDPR obligations. The Article concludes with a brief consideration of the need to address these privacy statement requirements in the context of the many additional compliance obligations under the GDPR and the importance of prioritizing the privacy statement.

I. GDPR OBLIGATIONS TO PROVIDE NOTICE

GDPR Articles 13, 14, and 15(1) provide a lengthy and detailed list of information that must be provided to data subjects. These notice obligations do not specify a particular format for providing this information, but common practice and the expectation of customers, regulators, and others is that this information will be included in a privacy statement.

---

applied to specific products or activities. For example, an organization's internal policy may state it should not collect more personal data than it needs to operate its business and provide its services. The policy may further require internal teams to document and justify their data collection practices, and to escalate questions to the legal department in cases of doubt. But the public-facing privacy statement will describe the facts regarding what data types are collected and how they are used. In other words, a privacy statement reflects the organization's internal policy, but it also provides a detailed factual statement of how those policies are applied in practice. Thus, using the term "privacy statement" more accurately reflects what the document is, and it avoids the confusion inherent in using the same term to describe both internal and external documents. Likewise, the term "privacy notice" can be used to refer to many types of notices. Products or services may provide specific privacy-related details to consumers in a piecemeal way in the user interface. Thus, users may see many privacy notices as they interact with a product or service. By contrast, the privacy statement is the comprehensive document that gathers all the essential privacy-related information in a single place.

A. What Organizations Must Have a Privacy Statement?

Under the GDPR, the notice obligations apply to "data controllers"—those organizations that determine "the purposes and means of the processing of personal data."[7] By contrast, they do not apply directly to "data processors"—those organizations that process personal data on behalf of a data controller—such as vendors or service providers handling personal data at the direction of an organization.[8]

Processors do have an obligation to provide information or other assistance to a controller as necessary for the controller to meet its obligations, including its notice obligations.[9] So, for example, a controller's privacy statement may need to describe the types of data processing carried out by the controller's service providers—and if the controller cannot adequately include such a description without input from the processor, the processor must provide that input.

Further, while processors do not necessarily have an obligation to post a public-facing privacy statement, many nevertheless choose to do so. Such a document can serve as a self-help resource for controllers that are drafting their own privacy statements and need to describe some aspect of the processor's activities. And the presence of a privacy statement can help the processor demonstrate the steps it takes to protect the privacy and security of the data it handles, which can be useful for both commercial and regulatory objectives. For example, companies may be reluctant to purchase data processing services if there is any doubt about a processor's privacy and security practices. Thus, a well-written privacy statement containing strong commitments can be seen as a competitive differentiator that can help drive sales.

B. What Must Be Included in a Privacy Statement?

The previous privacy law in Europe, the 1995 Data Protection Directive, required companies to provide notice to consumers, and it specified six categories of information that must be included. Organizations were required to inform consumers of:

- The identity of the data controller (typically the organization);
- Where the personal data is obtained from a source other than the data subject, the categories of data processed;

---

7. *See* GDPR, *supra* note 1, art. 4(7), at 33 (defining "controller"); *see also id.* arts. 12–15, at 39–43 (notice obligations as they apply to controllers).

8. *Id.* art. 4(8), at 33.

9. *Id.* art. 28(3), at 49.

- Where the personal data is obtained from the data subject, whether providing the data is mandatory, and any possible consequences of a failure to provide such data;
- The recipients or categories of recipients of the data;
- The purposes for which personal data about them is being processed; and
- The existence of a right to access and correct the data.[10]

By comparison, the GDPR requires organizations to provide a much more extensive range of information to individuals. The following discussion lists and describes each type of information that must be included in a privacy statement to meet GDPR obligations.

1. The identity of the data controller.[11]

Under the GDPR, the privacy statement must identify the data controller, which is the entity or entities that ultimately determine how the data will be used.[12] For example, if a vendor hosts a website on behalf of an organization, the organization will be the data controller and the vendor will be a data processor. Thus, the privacy statement for that website must identify the organization as the controller (although it may also state that the vendor is hosting the website on behalf of the organization).

Within a corporate family of a parent corporation and a number of controlled subsidiaries and affiliates, the parent will typically be the data controller. However, there are some cases in which a subsidiary will be the data controller and the corporate parent will be a data processor. Regardless, the privacy statement should describe those relationships and clarify the role that each plays. As a related example, in the context of an acquisition, the acquired company's privacy statement(s) should be updated promptly to disclose the identity of the new corporate parent.

Typically, a privacy statement will identify the organization or organizations up front, in the introductory paragraph. For instance, it could start with something like: "This privacy statement applies to [Company] and its controlled affiliates and subsidiaries." If the company offers products and services under several brands that are intended to be covered by the privacy statement, listing those as part of identifying the controller is advisable. If an EU subsidiary or affiliate is operating as a data controller for data from the EU, that role should be specified somewhere in the privacy statement, such as where other EU-specific topics are addressed.

---

10. Council Directive 95/46, arts. 10–11, 1995 O.J. (L 281) 41–42 (EU).

11. GDPR, *supra* note 1, art. 13(1)(a), at 40; *id.* art. 14(1)(a), at 41.

12. *Id.* art. 13(1)(a), at 40; *id.* art. 14(1)(a), at 41; *see also id.* art. 4(7), at 33 (defining "controller").

2. The contact details of the data controller.[13]

While the 1995 Directive only required the privacy statement to disclose the identity of the data controller, the GDPR additionally requires that the controller's contact information be included.[14] This information is typically included in a "contact us" section at or near the end of the privacy statement. Listing contact details is a seemingly straightforward and simple requirement, but it can be surprisingly fraught with challenges.

Many companies have found that publishing an email address in a privacy statement often results in that address receiving large amounts of spam and other non-privacy-related messages, which can overwhelm the organization's ability to respond expeditiously to legitimate privacy concerns and inquiries. One approach to address this challenge is to implement a web form that can route the inquiries to the appropriate recipient and help prevent spam.

Another important consideration is ensuring that the company is capable of effectively responding to customers or other individuals with privacy questions, concerns, or complaints. Thus, it is important to be sure that those inquiries are received by those with the capability and expertise to respond to them quickly and appropriately. It is also a best practice to have processes in place to track those inquires in order to maintain appropriate records, flag and fix instances of non-compliance, and identify trends that may reflect the emergence of reputational or other risks.

3. Where the GDPR requires the organization to appoint a European representative, the identity and contact details of that representative.[15]

The GDPR requires non-European data controllers to appoint a European representative under certain circumstances.[16] In such cases, the privacy statement must also include the identity and contact information of that representative.[17]

---

13. *Id.* art. 13(1)(b), at 40; *id.* art. 14(1)(b), at 41.

14. *Id.* art. 13(1)(b), at 40; *id.* art. 14(1)(b), at 41.

15. *Id.* art. 13(1)(b), at 40; *id.* art. 14(1)(b), at 41.

16. Where a data controller or processor is not established in the EU, but offers goods or services to EU residents or monitors the behavior of data subjects located in the EU, it must designate an EU representative unless the data processing is

> occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing.

Id. art. 27, at 48.

17. *Id.* art. 13(1)(a), at 40; *id.* art. 14(1)(a), at 41.

4. Where the GDPR requires the organization to appoint a data protection officer (DPO), the contact details of the DPO.[18]

Similarly, the GDPR requires certain organizations to appoint a data protection officer (DPO).[19] Where a DPO is appointed, that person's contact information must also be included in the privacy statement.[20] However, unlike the European representative, the DPO's identity need not be disclosed.

For both the representative and the DPO contact information, such details can be included in either the general "contact us" section of the statement, or in a EU-specific section.

5. The types of personal data obtained.[21]

A privacy statement must disclose the categories of personal data that the organization collects.[22] This does not mean a granular list of every data point collected, but rather a list of categories. There is some flexibility in terms of the level of granularity, but it should be sufficiently specific and descriptive to provide the reader with a fair understanding of the scope and nature of data collection.

Obviously, for an organization that collects many different types of data, such a disclosure could be quite lengthy. Often, a long list of data collected, by itself and without context, can appear overly invasive. Thus, it may be better to combine the disclosures of *what* data is collected with descriptions of *why* it is collected and *how* it will be used.

Under the GDPR, this requirement applies to personal data that is obtained from a source other than the data subject.[23] But as a practical matter, most companies will list all the categories of personal data they collect, without making that distinction.

---

18. *Id.*

19. Private sector organizations must appoint a DPO where the "core activities" of the organization 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 "processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10." *Id.* art. 37(b)–(c), at 55.

20. *Id.* art. 13(1)(a), at 40; *id.* art. 14(1)(a), at 41.

21. *Id.* art. 14(1)(d), at 41; *id.* art. 15(1)(b), at 43.

22. *Id.* art. 14(1)(d), at 41; *id.* art. 15(1)(b), at 43. "Personal data" is defined as

> 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. art. 4(1), at 33.

23. *Id.* art. 14(1)(d), 41; *id.* art. 15(1)(b), at 43.

6. The source(s) from which the personal data originate, other than from the data subjects themselves, and if any such data came from publicly accessible sources, specifying that fact.[24]

When data is requested from an individual and is explicitly provided, such as in a web form, the means of data collection is self-evident. But increasingly, the bulk of the data gathered about individuals is collected through a variety of passive means, or is acquired from third parties, and these sources must be disclosed.

As an example, many privacy statements that cover websites or online services need to include a detailed discussion of how data is collected passively through the use of cookies.[25]

Where data is acquired from third parties, it remains unclear whether European regulators will interpret this provision to require the disclosure of every individual third-party source of data. But at the very least, organizations need to list categories of third-party data sources (such as data brokers, social networks, other partners, and public sources), and should perhaps illustrate with key examples for each category.[26]

7. Where the personal data is collected from the data subject, whether providing the data is required, including: (a) whether it is a requirement necessary to enter into a contract; (b) whether it is otherwise required by

24. *Id.* art. 14(2)(f), at 42; *id.* art. 15(1)(g), at 43; *see also id.* Recital 61, at 12 ("Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.").

25. Cookies are small text files that websites and online services can store on the computer or other device that connects to the site or service. They are used for a variety of purposes. For more detailed information about cookies, see ALL ABOUT COOKIES.ORG, http://www.allaboutcookies.org/, [https://perma.cc/K3P9-XRG9]. The EU ePrivacy Directive, a body of law separate from the GDPR, requires consent for cookies and similar technologies, and consent requires clear notice regarding use of cookies. *See* Council Directive 2002/58, art. 5(3), 2002 O.J. (L 108) 60 (EC) (as amended by Council Directive 2009/136, 2009 O.J. (L 337) 30 (EC)) ("[T]he storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information . . . ."). Some organizations have chosen to maintain a separate "cookie policy" that their cookie banners or cookie consent experiences can point to. However, because a privacy statement would typically need to contain some discussion of cookies, and several references to cookies throughout, it will frequently be more efficient for the organization and easier for the customer to have all privacy-related cookie disclosures in the privacy statement. Plus, having cookie disclosures in multiple documents creates the risk of real or perceived inconsistencies.

26. *See* GDPR, *supra* note 1, Recital 61, 2016 O.J. (L 119) 12 (EU) ("Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.").

> statute or contract; and (c) the possible consequences if the data subject fails or declines to provide such data.[27]

The previous European privacy law required privacy statements to include whether providing data is mandatory, as well as the consequences of not providing data.[28] The GDPR expanded this obligation by also requiring that the privacy statement specify if a requirement to provide data is based on a statute or a contract.[29]

In practice, these disclosures tend to be quite general. For example, a privacy statement might declare that some services require a certain amount of data to function correctly and that refusal to provide that data means that the person will not be able to use the service. Where providing certain information is required so that the organization can meet a legal requirement, such as where age is collected in order to determine whether parental consent is required,[30] the privacy statement should describe that requirement.

8. The intended purposes of processing the personal data.[31]

Another basic element of a privacy statement is a description of how the data is used. As with the descriptions of the data collected, organizations must include a description of how collected data is used. As with other aspects of the privacy statement, organizations must decide what level of specificity to use for these descriptions. Often, privacy statements will describe categories or types of uses. Common uses include:

- Operating and providing the product(s) or service(s);
- Improving the product(s) and service(s);
- General business operations (such as accounting, auditing, etc.);
- Security (including fraud detection, keeping the product(s) safe and secure, and securing the organization's systems and infrastructure);
- Personalization (either within the particular product or service, or across products and services);
- Direct marketing; and
- Advertising (including online behaviorally targeted advertising).

---

27. *Id.* art. 13(2)(e), at 41.

28. Council Directive 95/49, art. 10(c), 1995 O.J. (L 281) 41 (EC).

29. GDPR, *supra* note 1, art. 13(2)(e), at 41.

30. For example, the GDPR provides that where the legal basis of data processing is consent, parental consent is required if the data subject is under the age of 16 (although individual EU member states can lower that threshold age as low as 13). *Id.* art. 8, at 40–41.

31. *Id.* art. 13(1)(c), at 40; *id.* art. 14(1)(c), at 41; *id.* art. 15(1)(a), at 43.

If the privacy statement lists categories of uses, it is best to illustrate each category with some key examples. In structuring these descriptions, it can help add clarity if the organization distinguishes "primary purposes" over which the organization does not offer choice (such as providing the services, business operations, and security) from secondary uses over which users have some choice (such as direct marketing and ad targeting).

Some purposes of processing may require considerable detail due to a high level of regulatory scrutiny, as well as the direct or indirect applicability of certain self-regulatory obligations. In particular, if personal data is processed for online behavioral advertising, such use should be described in detail.[32] Further, most companies that provide online behavioral advertising services participate in one or more self-regulatory programs, such as those offered by the Network Advertising Initiative (NAI),[33] Digital Advertising Alliance (DAA),[34] and European Interactive Digital Advertising Alliance (EDAA).[35] Each of these programs requires that participants include specific elements in their privacy statements and contractually pass through certain privacy notice requirements to website publishers and other customers or partners of the participant.[36]

---

32. For example, the Article 29 Working Party has stated that ad networks and publishers should ensure that individuals are told, at a minimum, who (i.e., which entity) is responsible for serving the cookie and collecting the related information. In addition, they should be informed in simple ways that (a) the cookie will be used to create profiles; (b) what type of information will be collected to build such profiles; (c) the fact that the profiles will be used to deliver targeted advertising; and (d) the fact that the cookie will enable the user's identification across multiple web sites.

Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioural Advertising*, WP 171, at 24 (June 22, 2010).

33. *See* NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/ [https://perma.cc/Z59Y-NNBT].

34. *See* DIGITAL ADVERTISING ALLIANCE SELF-REGULATORY PROGRAM, http://www.aboutads.info/ [https://perma.cc/Y542-Z2TT].

35. *See* YOUR ONLINE CHOICES, http://www.youronlinechoices.com/ [https://perma.cc/ZQ2L-UGVP].

36. The NAI obligates members to contractually bind the websites where they collect data for ad targeting to clearly and conspicuously post a notice that includes:

(a) a statement of the fact that data may be collected for Personalized Advertising purposes on the website; (b) a description of types of data, including any PII, Precise Location Data, or Personal Directory Data, that are collected for Personalized Advertising purposes on the website; (c) an explanation of the purposes for which data is collected by, or will be transferred to third parties, including Cross-Device Linking if applicable; and (d) a conspicuous link to an Opt-Out Mechanism for Interest-Based Advertising and Retargeting.

NETWORK ADVERT. INITIATIVE, NAI SELF-REGULATORY CODE OF CONDUCT § II.B.3, at 8–9 (2018), https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf [https://perma.cc/59U7-FJ67].

9. Where personal data is used for automated decision making, including profiling, the existence of such processing, as well as a description of the logic involved, the significance of the processing, and any anticipated consequences for the data subject.[37]

This privacy statement requirement calls out one particular use, or purpose of processing, of personal data. If personal data is used for automated decision-making or profiling, that use should be described in greater detail. Thus, the privacy statement must describe such processing, which must include "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[38]

10. The legal basis for processing the personal data.[39]

The GDPR also requires organizations to describe in their privacy statements the "legal basis" or bases for processing personal data.[40] A basic requirement of European data protection law is that any processing of personal data must have a "legal basis."[41] The more common legal bases are (1) consent of the data subject, (2) necessary for the performance of a contract with the data subject, or (3) the "legitimate interests" of the data controller or a third party. Determining the appropriate legal basis for data processing often involves a careful and detailed evaluation of the facts, the details of which are beyond the scope of this Article; but once the legal bases have been determined, the bases must be described in the privacy statement.

The need to describe the legal bases for processing and determine the level of granularity of such description raises an important issue. The GDPR does not provide clear guidance on the required level of specificity for descriptions of the legal bases. As a result, some organizations choose to keep the description very general. For example, a privacy statement might say something like: "When we process personal data about you for the purposes described in this statement, we do so with your consent, to fulfil our contractual or legal obligations, or to fulfill our other legitimate interests."

However, the GDPR text can be read to suggest a more granular and specific description is needed. In listing the items to be included in a privacy statement, GDPR pairs this obligation to describe the legal bases

37. GDPR, *supra* note 1, art. 13(2)(f), at 41; *id.* art. 14(2)(g), at 42; *id.* art. 15(1)(h), at 43.
38. *Id.* art. 13(2)(f), at 41; *id.* art. 14(2)(g), at 42; *id.* art. 15(1)(h), at 43.
39. *Id.* art. 13(1)(c), at 41; *id.* art. 14(1)(c), at 41.
40. *Id.* art. 13(1)(c), at 41; *id.* art. 14(1)(c), at 41.
41. *See id.* art. 6, at 36–37 (listing the available legal bases for processing personal data).

with the obligation to describe the purposes of processing.[42] This pairing could be read as suggesting that the legal basis should be described separately for each purpose of processing.[43] Thus, a more detailed and conservative approach to this requirement would list every use or category of use and note the legal basis or bases for each.

11. Where the legal basis is "legitimate interests," a description of those interests.[44]

As noted above, one legal basis for processing personal data under the GDPR is "the legitimate interests pursued by the controller or by a third party" under Article 6(1)(f).[45] When relying on that basis, the privacy statement must include a description of those interests. This information may be partially provided as part of privacy statement language about "purposes of processing"—i.e., how data is used and shared with third parties. But in most cases, it is advisable to add language specifically calling out the use of legitimate interests as the legal basis for processing. For example:

> In those cases where we rely on our legitimate interests, those interests include providing products you use, operating our business, meeting legal obligations, protect the security of our systems and our customers, and meeting other essential business and operational needs.

Here too, the appropriate level of specificity will need to be determined by the organization.

12. The recipients (or categories of recipients) of the personal data.[46]

A privacy statement must disclose the categories of third parties to which personal data may be shared.[47]

Some privacy statements make the implausible claim that "we never share your data with anyone." But every organization either discloses data to at least some third parties, or is likely to at some point. For example:

---

42. *See id.* art. 13(1)(c), at 41; *id.* art. 14(1)(c), at 41 ("the purposes of the processing for which the personal data are intended as well as the legal basis for the processing").

43. As described above, the appropriate level of specificity in listing the purposes of processing is another area of uncertainty under the GDPR.

44. GDPR, *supra* note 1, art. 13(1)(d), at 41; *id.* art. 14(2)(b), at 42.

45. *Id.* art. 13(1)(d), at 41; *id.* art. 14(2)(b), at 42.

46. *Id.* art. 13(1)(e), at 41; *id.* art. 14(1)(e), at 41; *id.* art. 15(1)(c), at 43.

47. *Id*. art. 13(1)(e), at 41; *id.* art. 14(1)(e), at 41; *id.* art. 15(1)(c), at 43.

- Any organization could be compelled to turn over data to law enforcement.[48]
- Virtually every organization is likely at some point to use a vendor or service provider that will need some access to personal data (accountants, payment processors, IT support providers, customer service vendors, etc.).
- Nearly any company could be involved in a merger, acquisition, divestiture, or similar transaction that would require sharing some personal data with the other company or companies involved.
- Many organizations have ongoing commercial relationships with other parties that involve some sharing of data—ad service providers, social networks, etc.

All of these categories of third-party data sharing or potential data sharing should be described in the privacy statement.

Another category that should be noted in many cases is sharing within a corporate family—among affiliates and subsidiaries. But it is advisable to avoid characterizing controlled affiliates and subsidiaries as "third parties" because in some cases it may be possible and advantageous to characterize such entities as first parties.[49] Thus, it may be beneficial to differentiate (a) transfers of, or access to, data within a corporate family of controlled affiliates and subsidiaries from (b) disclosures of data to unrelated third parties.

13. The right to request access to personal data held by the organization.[50]

Like the previous EU privacy law, the GDPR provides for a right for data subjects to access personal data, subject to certain exceptions.[51] And like the previous law, the GDPR requires that data subjects be given notice

48. Some legal standards require the potential disclosure of data to law enforcement to be specifically called out. For instance, the EU-U.S. Privacy Shield Framework requires a privacy statement to include a description of "the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements." *See* EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce § II.1.a.xii [hereinafter EU-U.S. Privacy Shield Framework Principles].

49. For example, a company may consist of several different legal entities, but operates as a single, integrated enterprise with shared infrastructure and data systems, under common control, and represented by a common brand. In such cases, it could be misleading or confusing to describe mere collection and storage of data in that shared infrastructure as third-party sharing, despite the fact that more than one legal entity may have access to the data.

50. GDPR, *supra* note 1, art. 13(2)(b), at 41; *id.* art. 14(2)(c), at 42; *id.* art. 15(1)(e), at 43.

51. *Id.* art. 15, at 43.

of this right.[52] However, it is important to note that the GDPR states the notice requirement related to data access in terms of an individual's right to *request* from the controller access to personal data.[53] Drafting the privacy statement to state this right as a "right to request" rather than an absolute right to access such data will avoid overstating the right and will preserve the organization's ability to deny such a request where there is an applicable exception or another legal basis for doing so.

14. The right to request that personal data be corrected or amended if such data is inaccurate or incomplete.[54]

Like the right to access, a data subject's right to rectification and an organization's obligation to provide notice of that right is not new.[55] But the GDPR also permits the right to rectification to be stated in terms of a "right to request." For the reasons stated above, it is important to draft the privacy statement so as to state this as a right to request, rather than an absolute right to correct or amend personal data.

15. The right to request erasure of personal data under certain circumstances.[56]

In contrast, the right of erasure (also referred to as the right to be forgotten) is a new right under the GDPR.[57] But the right only applies under certain circumstances.[58] And like other rights, there are a number of exceptions.[59] The notice provisions of the GDPR allow the right of erasure

---

52. *Id.*

53. *Id.*

54. *Id.* art. 13(2)(b), at 41; *id.* art. 14(2)(c), at 42; *id.* art. 15(1)(e), at 43.

55. *Id.* art. 16, at 66 (describing the right of correction ("right to rectification")).

56. *Id.* art. 13(2)(b), at 41; *id.* art. 14(2)(c), at 42; *id.* art. 15(1)(e), at 43.

57. *See id*. art. 17, at 43–44 (describing the right to erasure, its applicability, and its exceptions).

58. The right of erasure applies where:

> (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based . . . and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing [of the data for direct marketing purposes]; (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; [or] (f) the personal data have been collected in [the context of services offered directly to children].

Id. art. 17(1), at 43–44.

59. The right of erasure does not apply were the processing of the data is necessary:

> (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health . . .; (d) for archiving purposes in the public interest, scientific

to be described as a right to *request* deletion of personal information. It may be prudent for the privacy statement to go into detail regarding the applicability of the right.

The benefit of including such detail is that it may cut down on the number of baseless requests to delete data—requests which would require the organization to spend resources to process and are likely to lead to unhappy customers when they are denied. The downside of including such detail is, of course, that it will make the privacy statement longer.

16. A limited right to data portability.[60]

Another new right introduced in the GDPR is the right of data portability (i.e., the right to receive any personal data he or she has provided in a structured, commonly used, and machine-readable format, and to transmit that data to another organization).[61] Specifically, the Regulation states that the privacy statement must disclose the existence of the right of a data subject to receive data "he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller."[62] Note that, unlike the notice requirements related to the rights to access, correction, and erasure, this language does not phrase the requirement in terms of a "right to request." However, the right to data portability only applies under certain circumstances,[63] so it may be prudent to describe the limited applicability of the right in the privacy statement, or at least convey that it is not an absolute right.

17. Where the legal basis for processing is the consent of the data subject, the existence of the right to withdraw such consent at any time.[64]

Where an organization processes personal data based on the consent of the data subject under GDPR Article 6(1)(a) or 9(2)(a), the Regulation requires that the privacy statement state the existence of the right to withdraw consent at any time ("without affecting the lawfulness of

---

> or historical research purposes or statistical purposes . . . in so far as [erasure] is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.

Id. art. 17(3), at 44.

60. *See id.* art. 13(2)(b), at 41; *id.* art. 14(2)(c), at 42; *id.* art. 15(1)(e), at 43.

61. *See id.* art. 20(1), at 45 (scope of the data portability obligations).

62. *See id.*; *see also id.* art. 13(2)(b), at 41; *id.* art. 14(2)(c), at 42; *id.* art. 15(1)(e), at 43.

63. The right of data portability applies only where the legal basis for processing is consent or the performance of a contract *and* the processing is carried out by automated means. *See id.* art. 20(1), at 45.

64. *See id.* art. 13(2)(c), at 41; *id.* art. 14(2)(d), at 41.

processing based on consent before its withdrawal").[65] In addition to stating that the data subject can withdraw consent, stating the condition included in the parenthetical above is also advisable. That condition makes it clear that even if the data subject withdraws consent, any data processing based on consent before the withdrawal remains lawful. This disclosure can occur either where the privacy statement discusses the legal bases for processing (in particular, where processing relies on the consent of the data subject), or it can occur as part of a list of data subject rights (further described below).

18. The right to object to the processing of personal data or obtain a restriction of such processing under certain circumstances.[66]

Additional GDPR rights that must be disclosed in the privacy statement are the rights of a data subject to object to the processing of personal data and the right to obtain a restriction of such processing under certain circumstances. The right to object applies to processing for marketing purposes,[67] where the legal basis is "legitimate interests,"[68] or where a much narrower basis for certain tasks in public interest and/or on behalf of a government agency applies.[69] The right to obtain a restriction on processing applies under four narrow circumstances described in Article 18(1).[70] As with other data subject rights described above, organizations may choose to include detail on the limitations of these rights so as to discourage individuals from asserting them in circumstances when they do not apply.

---

65. *Id.*

66. *Id.* arts. 13–15, at 41–43.

67. *Id.* art. 21(2)–(3), at 45.

68. *Id.* art. 21(1), at 45 (referencing Article 6(1)(f): "necessary for the purposes of the legitimate interests pursued by the controller or by a third party").

69. *Id*. (referencing Article 6(1)(e): "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller").

70. *Id.* art. 18(1), at 44. The circumstances under which the right to obtain a restriction on processing may apply are:

> (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; [and] (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Id.

19. The right to lodge a complaint with a supervisory authority.[71]

The GDPR requires organizations to specifically state in their privacy statements that individuals have a right to lodge a complaint with a supervisory authority.[72] Most organizations will want to encourage users to first contact the organization itself, rather than lodge a complaint with a regulator, so this information should either reference, or be placed in conjunction with, the organization's contact information. For example, the "contact us" section of the privacy statement might include a sentence such as:

> You have the right to lodge a complaint with a supervisory authority, but we encourage you to first contact us with any questions or concerns at the address provided below.

Alternatively, a description of this right could be included along with the descriptions of the individual rights required to be disclosed under the GDPR.

20. Transfers of data out of Europe.[73]

The GDPR requires detailed disclosures about data transfers outside of the European Economic Area (EEA). Specifically, where a data controller intends to transfer personal data to a third country or international organization, the privacy notice must describe the fact of such transfer and either:

- the existence or absence of an adequacy decision by the European Commission, or
- in the case of transfers based on "suitable safeguards" (such as contractual provisions or binding corporate rules), a description of such safeguards and how to obtain a copy of them.[74]

If there are only a few jurisdictions to which the organization typically transfers data, it may be possible to list them. But often, companies want to maintain some flexibility and future-proof a privacy statement by leaving it more general and saying that data may be processed in any country where the company or its service providers maintain personnel or facilities. An organization may also want to maintain similar flexibility regarding the "suitable safeguards" it relies on under the GDPR. For example, an organization that has several bases for transferring data from Europe, including the use of standard contractual clauses as approved

71. *Id.* art. 13(2)(d), at 41; *id.* art. 14(2)(e), at 42; *id.* art. 15(1)(f), at 43.

72. *Id*. art. 13(2)(d), at 41; *id.* art. 14(2)(e), at 42; *id*. art. 15(1)(f), at 43.

73. *Id.* art. 13(1)(f), at 41; *id.* art. 14(1)(f), at 42; *see also id.* art. 15(2), at 43.

74. *Id.* art. 13(1)(f), at 41; *id.* art. 14(1)(f), at 42; *id.* art. 15(2), at 43 (referencing the permissible bases and safeguards for cross-border data transfers set out by Articles 46, 47, and 49(1)(b)).

by the European commission, might have a paragraph in its privacy statement that says something like:

> We store and process personal data in the United States and other countries where we or our service providers maintain personnel or facilities. With respect to personal data from the European Economic Area and Switzerland, some destinations have not been determined by the European Commission to have an adequate level of data protection. When we transfer data from the EEA and Switzerland, we use a variety of legal mechanisms, including contracts, to help ensure personal data remains protected. You can request a copy of the relevant contractual clauses by contacting us as described at the end of this statement.

If an organization participates in the EU–U.S. Privacy Shield as a basis for such data transfers, a much more extensive and explicit set of notice requirements also apply.[75] Some Privacy Shield notice requirements are redundant of GDPR requirements (e.g., describing the types of personal data collected and the purposes of processing), but others are unique to the Privacy Shield and go beyond what must be included under the GDPR generally. These include:

- a statement of the organization's participation in the Privacy Shield[76] and its adherence to the Privacy Shield Principles with respect to all personal data received from the EU in reliance on the Privacy Shield;[77]
- a link to, or the web address for, the Privacy Shield List maintained by the Department of Commerce (https://www.privacyshield.gov);[78]
- a statement regarding the organization being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation, or any other U.S. authorized statutory body;[79]

75. *See* EU-U.S. Privacy Shield Framework Principles, *supra* note 48; *see also* Commission Implementing Decisions (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 48 (EU). Most companies that participate in the EU-U.S. Privacy Shield also participate in the Swiss-U.S. Privacy Shield.

76. EU-U.S. Privacy Shield Framework Principles, *supra* note 48, § II.1.a.i.

77. *Id.* § II.1.a.iii.

78. *Id.* § II.1.a.i.

79. *Id.* § II.1.a.x.

- an organization must inform individuals about the entities or subsidiaries of the organization also adhering to the Principles, where applicable;[80]
- a description of when exceptions to the organization's adherence to the Principles "will apply on a regular basis" based on statute, government regulation, or case law that creates conflicting obligations or explicit authorizations";[81]
- the organization's liability for damage in cases of onward transfers to third parties;[82]
- the independent dispute resolution body designated by the organization to address unresolved complaints and provide appropriate recourse, free of charge to the individual, related to the organization's adherence to the Privacy Shield Principles—the description of which must provide a link to the website or complaint submission form of such body[83] and specify whether it is: (1) the panel established by European data protection authorities, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States;[84] and
- a statement of the possibility, under certain conditions, for the individual to invoke binding arbitration for claimed violations of the Principles.[85]

Typically, an organization will attempt to pack the specific Privacy Shield disclosures into one or two brief paragraphs. For example:

> [Company] and our controlled U.S. subsidiaries participate in the EU–U.S. and Swiss–U.S. Privacy Shield frameworks, as set forth by

80. *Id.* § II.1.a.ii.

81. *Id.* § I.5.

82. *Id.* § II.1.a.xiii. Under the Privacy Shield, the organization's liability in the case of onward transfers does not apply when "the organization proves that it is not responsible for the event giving rise to the damage." *Id.* § II.7.d. An organization will likely wish to include a description of this limitation in its privacy statement to avoid creating strict liability for damage resulting from onward transfers.

83. *See id.* § III.6.d. The UK Information Commissioner's Office (ICO) provides a Privacy Shield complaint form that can be used to submit a complaint to the data subject's data protection authority (DPA) for consideration by the DPA panel. *See EU-US Privacy Shield Complaint Form for Submitting Commercial-Related Complaints to the EU DPAs*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/make-a-complaint/eu-us-privacy-shield/ [https://perma.cc/V73V-QLQT].

84. EU-U.S. Privacy Shield Framework Principles, *supra* note 48, § II.1.a.ix.

85. *Id.* § II.1.a.ix. The right of the individual to invoke binding arbitration applies to only to those "residual" claims that remain unresolved after pursuing the other available means of recourse under the Privacy Shield. *Id.* § III.11.d.iv. Organizations wishing to avoid creating a broader right to arbitration than exists under the Privacy Shield will likely choose to describe this limitation and/or otherwise qualify the privacy statement language regarding the right to arbitration.

> the U.S. Department of Commerce. We adhere to the Privacy Shield principles with respect to personal data transferred from the European Economic Area or Switzerland to the United States in reliance on the Privacy Shield. If third-party agents process personal data on our behalf in a manner inconsistent with the Privacy Shield Principles, we remain liable unless we prove we are not responsible for the event giving rise to the damage. To learn more about the Privacy Shield, and to view our certification which includes a list of our subsidiaries also adhering to the principles, see the Privacy Shield website at https://privacyshield.gov.
>
> Our compliance with the Privacy Shield principles is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC). If you have a question or complaint related to our participation in the Privacy Shield, we encourage you to contact us as described at the end of this statement. For any complaints related to the Privacy Shield that cannot be resolved with us directly, we have chosen to cooperate with a panel established by the European data protection authorities (DPAs) for resolving disputes. A form for submitting a complaint to your local DPA is available at [link to complaint form website].[86] As further explained in the Privacy Shield Principles, binding arbitration is available under certain circumstances to address residual complaints not resolved by other means.

Finally, the Commerce Department has asked companies applying for the Privacy Shield to include language regarding the Privacy Shield "above the fold" (i.e., in the top layer of a layered notice or near the top of a long statement). This does not mean that all language required under the Privacy Shield Framework should be at the top of the statement, but it does mean that some brief statement regarding the Privacy Shield should be near the top, which can then be linked to more information deeper in the statement.

21. Retention of personal data.[87]

The GDPR requires the privacy notice to describe "the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period."[88] The flexibility to describe the retention "criteria" rather than the specific retention time periods is helpful,

---

86. See *EU-US Privacy Shield Complaint Form for Submitting Commercial-Related Complaints to the EU DPAs*, *supra* note 83, for an example of such a form published by the UK Information Commissioner's Office.

87. The GDPR has various articles regarding the storage of personal data. GDPR, *supra* note 1, art. 13(2)(a), at 41; *id.* art. 14(2)(a), at 42; *see also id.* art. 15(1)(d), at 43.

88. *Id.* art. 13(2)(a), at 41; *id.* art. 14(2)(a), at 42; *see also id.* art. 15(1)(d), at 43.

particularly in cases where there are many different data types with variable retention periods. Examples of criteria are:

- The time needed to keep data for essential business operations, such as financial accounting and auditing, protecting the security of the organization's systems and detecting fraud, maintaining appropriate business and financial records, and dispute resolution.
- Customer expectations regarding retention. For example, in many cases where a customer creates an account, there is an expectation that certain data will be retained in that account unless the customer actively deletes it or closes the account.
- Sensitivity of the data. In general, where sensitive data types are collected, retention timeframes should be shorter.
- Legal obligations to retain data. In some cases, applicable laws require that certain data be retained. Examples include laws requiring certain recordkeeping or other data retention, government orders to retain data during an investigation, or data that must be retained for the purpose of litigation.

Often, a hybrid approach is advisable where some specific timeframes are listed, but various criteria are described to cover the remaining cases where listing actual retention times is impractical or impossible.

II. STYLE AND STRUCTURE MATTER

In addition to the lengthy enumeration of specific items that must be included in a privacy statement, the GDPR also states that this information must be presented in a "concise, transparent, intelligible and easily accessible form."[89]

A. Privacy Statements Must Be Concise

The fact that the GDPR dramatically increased the number of subjects that must be included in a privacy statement, at the same time as adding a requirement that the privacy statement be "concise," creates an obvious tension and a difficult challenge.

While some of the items to be included in a privacy statement can be covered with relatively few words, a number of the required items necessitate lengthy factual descriptions of what the organization does. Such descriptions might include: what data it collects and how, how that data is used, whether and with whom the data is shared, and how long the data is retained. Developing a complete and accurate understanding of the

89. *Id.* art. 12(1), at 39.

relevant facts may be the most important and challenging aspect of creating a privacy statement. A privacy statement that contains factual inaccuracies provides an easy target for regulators, plaintiffs' lawyers, and privacy advocates.

Nevertheless, the requirement to keep information provided in a privacy statement "concise" should be taken seriously. Writers should take great care in drafting statements so the essential information is provided as concisely as possible. But a desire to make the statement shorter should not trump the need to include all the required elements and provide full and accurate information for each element. The result may be a fairly lengthy document. A privacy statement should be as long as it needs to be to meet all the applicable legal requirements and provide full descriptions of all the relevant data practices.[90] Some of the structure and design elements discussed below can provide easier navigation and readability for long privacy statements.

B. Privacy Statements Must Be Clear and Easy to Read

Part of making a privacy statement "transparent" and "intelligible," as required by the GDPR, requires the drafter to be thoughtful about the language used. The use of technical or legal jargon reduces the clarity of a privacy statement for the average reader. Instead, drafters of privacy statements should use plain language to describe data practices in the clearest possible way.[91] There are excellent resources and guidance available on plain language writing that can be utilized for privacy statement drafting.[92]

C. Privacy Statements Should Be Structured to Be Easily Navigable

A well-structured privacy statement helps the reader find relevant information quickly and easily. It makes it unnecessary to read the entire

---

90. For a longer description of how long privacy statements should be, see Michael Hintze, *In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044 (2017).

91. For a comparison of several companies' privacy statements using criteria for plain language writing, see Katy Steinmetz, *These Companies Have the Best (And Worst) Privacy Policies*, TIME (Aug. 6, 2015), http://time.com/3986016/google-facebook-twitter-privacy-policies/ [https://perma.cc/S6U4-YHLM]. One can also access the full report: CTR. FOR PLAIN LANGUAGE, PRIVACY POLICY ANALYSIS, http://centerforplainlanguage.org/wp-content/uploads/2015/09/TIME-privacy-policy-analysis-report.pdf [https://perma.cc/6H92-TNLC].

92. *See* CENTER FOR PLAIN LANGUAGE, http://centerforplainlanguage.org/ [https://perma.cc/K6FG-JF6M] (provides resources for the use of plain language and serves as a watchdog for unclear writing by the government and private sector); PLAINLANGUAGE, http://www.plainlanguage.gov/ [https://perma.cc/24W7-RKVY] (U.S. federal government site focused on fostering plain language writing in U.S. government documents and publications); *Various Plain English Statutes*, LANGUAGEANDLAW, www.languageandlaw.org/texts/stats/plaineng.htm [https://perma.cc/75S7-72UN] (texts of plain language laws that have been adopted in various U.S. states).

statement in order to locate the information that is relevant to a particular reader or to find the answer to a particular question. A well-organized and structured privacy statement will reduce redundancies, which will in turn reduce overall length. Using clear headings will help the reader find the relevant information quickly. If the privacy statement is long, the use of a table of contents with hyperlinks, or similar navigation aids, will also increase usability.

Likewise, adopting a layered format can provide quick summaries and a roadmap for finding more detail in the full statement. A typical layered privacy statement will have a short "top layer" that provides a brief summary, often designed to fit on one page or one screen, of a privacy statement's key points and a roadmap for navigating the full statement. Layered privacy statements have been used successfully for over a decade and are regularly encouraged by privacy regulators and others.[93]

The design should also take into account the different form factors on which the privacy statement may be read so that it will render correctly on both large and small screens.

D. Privacy Statements Should Be Easy to Find

Making the statement "easily accessible" requires that it be easy to find in the first place. Links to the privacy statement should be provided in prominent locations and in consistent ways across the different points at which an individual data subject interacts with an organization. For example, every web page should have the link to the statement in the same conspicuous location and use the same words. The link should contain the word "privacy." The link should be even more prominent where users are asked to provide personal data, are asked to make a choice regarding personal data, or are asked for more sensitive personal data.

An important question related to how a privacy statement is presented and referenced involves whether and how it should be accepted as a condition of using a product or service. Should a user be required to agree to the privacy statement when registering for a service? Should the privacy statement be incorporated by reference into the terms of service, end user license agreement (EULA), or other terms that the user agrees to? Some organizations have done so, presumably based on the belief that the incorporation by reference might bolster a consent argument: that the

93. For example, the Article 29 Working Party's recommendations to Google on its 2012 privacy statement included a recommendation that Google adopt a layered privacy statement. Letter from Isabelle Falque-Pierrotin, Chairman, Article 29 Working Party, to Larry Page, Chief Exec. Officer, Google, Inc. (Oct. 16, 2012), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf [https://perma.cc/BC6J-U6YS].

individual consented to the data collection and use described in the privacy statement.

One disadvantage of the incorporation by reference approach is that it suggests that the consent of the data subject provides the legal basis under the GDPR for all the data processing described in the privacy statement. This approach has significant legal implications. Where the legal basis is consent, the data subject has the right to revoke consent, and relying on consent as a legal basis triggers additional data subject rights and other obligations that might not otherwise exist.[94] More importantly, such an approach will not constitute valid consent under the GDPR, which requires that consent be "freely given, specific, informed and unambiguous."[95] In fact, language that requires broad consent to data use practices as a condition of use has been criticized as violating consumer protection rules. Criticism has been particularly harsh in Germany where consumer groups have successfully brought actions against companies that have required consumers to accept a broad range of data processing as part of agreeing to a service's terms of use.[96]

E. The Privacy Statement Should Be Accessible for All Users

Another aspect of making sure the privacy statement is easily accessible is ensuring it is compatible with screen readers and other assistive technologies. If those with disabilities are unable to effectively access and read the privacy statement, the statement is not fulfilling its purpose and the organization is not complying with its obligations. Resources to help website and software developers meet accessibility standards are available from a number of sources and vendors.[97]

---

94. *See* GDPR, *supra* note 1, art. 7(3), at 37 (regarding the right to withdraw consent); *see also id.* art. 20(1)(a), at 38–39 (the right to data portability, which applies only where the legal basis for processing is the consent of the data subject or the performance of a contract with the data subject); *id.* art. 8, at 37–38 (the requirement to obtain the parental consent where consent if the legal basis for processing of personal data regarding children).

95. *Id.* art. 4(11), at 34.

96. *See, e.g.*, Loek Essers, *Berlin Court Rules Google Privacy Policy Violates Data Protection Law*, PCWORLD (Nov. 20, 2013), http://www.pcworld.com/article/2065320/berlin-court-rules-google-privacy-policy-violates-data-protection-law.html [https://perma.cc/9N2A-22EE].

97. The Web Content Accessibility Guidelines 2.0 Level AA is a standard, approved by the World Wide Web Consortium (W3C) and the International Organization for Standardization (ISO), that developers can use in addressing accessibility issues. *See* WEB ACCESSIBILITY INITIATIVE, http://www.w3.org/WAI/ (last visited Feb. 13, 2019). Engineering resources for how to comply are available at: Michael Cooper, Andrew Kirkpatrick & Joshue O Connor, *Understanding WCAG 2.0: A Guide to Understanding and Implementing Web Content Accessibility Guidelines 2.0*, WORLD WIDE WEB CONSORTIUM (Oct. 7, 2016), http://www.w3.org/TR/UNDERSTANDING-WCAG20/Overview.html [https://perma.cc/HT2N-9ALS].

F. Should the Privacy Statement Be Global or Europe-Only?

Another design consideration that will affect the length and usability of the privacy statement is whether the privacy statement is localized for Europe only, or whether the organization maintains a global privacy statement that remains consistent across jurisdictions. Companies that operate globally or that collect personal information from consumers globally (which could involve as little as operating a globally-available website) must consider the privacy statement requirements across multiple jurisdictions. And these questions about localization are difficult ones.

Privacy statements should be translated into the languages in which the products and services it covers are presented. For example, if an online service is made available in ten languages, the privacy statement for that service should also be available in those languages. But beyond that, how much variation should there be by market?

One reason an organization's privacy statement might vary by jurisdiction is that certain services or product features discussed in the privacy statement are not available in every local market, so there is a desire to remove those references that are inapplicable. However, another approach would be to simply state near the beginning of the privacy statement that not all products or features mentioned in the privacy statement are available in all markets.

More significantly, under the GDPR, European residents are given a number of privacy rights that are not legally required in most markets outside of Europe. Organizations may be reluctant to convey those rights to customers or others where not required by law to do so, thereby effectively extending those rights globally. The descriptions of those rights might be included in a European version of the privacy statement but omitted from other versions. Another way to address that dilemma is to include those descriptions in a dedicated section called "European Privacy Rights." The section could contain language making clear the section applies only to residents of Europe.

But there are several factors weighing in favor of keeping a privacy statement as consistent as possible worldwide. Having different privacy statements in different jurisdictions can raise questions from customers, advocates, and regulators—especially if it appears to some readers as if they are being provided with less information or fewer privacy protections than customers in other jurisdictions. Further, making different privacy commitments in different markets creates compliance challenges for global services. If the organization has to track different processes or different data usage disclosures for different markets, the resulting complexity would be difficult and costly to manage, could lead to incompatibilities, and would increase the likelihood of error, thereby

creating additional legal risk. By contrast, maintaining one global version of a privacy statement not only simplifies compliance, it dramatically increases the ease of maintaining the statement itself.

CONCLUSION: PRIVACY STATEMENTS AS A TOP GDPR COMPLIANCE PRIORITY

Companies facing the daunting challenges of complying with the GDPR must plan for tackling its numerous requirements. A few of those compliance obligations are listed in the introduction of this Article, but a complete discussion is well beyond this Article's scope. Suffice it to say there are many such obligations. As a result, part of any organization's planning inevitably must include an assessment of risks and prioritization of its compliance investments. Based on such an assessment, meeting the GDPR privacy statement requirements should nearly always rise to the top of the list.

One reason for that conclusion is the simple fact that a company's privacy statement is public-facing. As such, it is a highly visible indicator of the steps the company has taken to comply with the GDPR. As described in Part I above, the GDPR requires a number of specific elements that must be included in a privacy statement. It is a relatively simple matter to check a company's privacy statement to see if those elements are included. If they are not, it is a very strong indicator that the company has not taken the steps it should to comply, which is a red flag that the company is likely to have other—and bigger—compliance problems. Those are not messages that companies want to broadcast to regulators or customers.

Another factor is that the work done to create a privacy statement can be leveraged for other compliance tasks. For instance, drafting a privacy statement requires an understanding of the underlying facts of the company's data collection and use practices. Many, or most, of these same facts will typically need to be discovered and recorded to meet obligations such as the documentation requirements under Article 30 and the DPIA requirements under Article 35.[98]

98. For example, GDPR, *supra* note 1, art. 30(1), at 50–51, requires data controllers to document, *inter alia*, (1) the name and contact details of the controller and, if applicable, the controller's representative and the data protection officer, (2) the purposes of processing, (3) the categories of personal data, (4) the categories of recipients of personal data, (5) transfers of data outside of the EU, and (6) data retention timeframes—all items that should also be included in the privacy statement. Compare, *id.* art. 35, at 53–54, which requires that controllers conduct a data protection impact assessment for high-risk data processing activities, which must include documentation of, *inter alia*, the purposes of processing and, where the legal basis is "legitimate interests," a description of those interests, which are also items that must be included in the privacy statement.

Finally, as demonstrated in this Article, drafting a well-crafted and legally sufficient privacy statement is not a simple matter. But it does not require the kind of engineering investments necessitated by certain elements of the GDPR—such as ensuring data systems are capable of responding, at scale, to individual erasure or data portability requests. It typically does not require developing entirely new business processes, such as building "data protection by design" into product development or "data protection impact assessments" into product release. And in most cases, companies already have privacy statements, so making them GDPR-compliant involves updating and adding detail to an existing document. Thus, in many organizations, updating the privacy statement may be seen as part of the GDPR "low hanging fruit" where the effort and cost required is easily outweighed by the compliance and risk-reduction benefit.