NOTES

A CONTEXTUAL EXTRATERRITORIALITY ANALYSIS OF THE DPIA AND DPO PROVISIONS IN THE GDPR

JOSHUA BLUME*

ABSTRACT

Consumer demands, breaches, and a shifting regulatory landscape are causing companies to rethink privacy. Due in large part to heavy fines that could range into the billions of euros, the GDPR will be the first law to set a global privacy standard, and though companies otherwise seeking to be GDPR-compliant may not apply all the law's provisions globally, there are at least two provisions those companies are likely to begin implementing now that the law is enforceable. Those two provisions relate to Data Protection Impact Assessments and Data Protection Officers. The first will require companies to methodically sketch out how their business practices affect consumers' personally identifiable information, and the second will install an unencumbered privacy professional that will ensure the company will do all it can to protect and restrict the use of personally identifiable information. Because these provisions are relatively untested anywhere outside of the EU, parallels can be drawn between these provisions and other laws with global reach such as the Foreign Corrupt Practices Act. Those comparisons indicate that the enforcement and fines provisions in the GDPR, along with growing consumer demands, will cause many companies seeking to be GDPR-compliant to go beyond the law's requirements and create new privacy protections around the globe. Because the Data Protection Impact Assessment and the Data Protection Officer provisions are necessarily structural changes, the changes they bring to multinational companies are likely to increase privacy protections for data subjects around the globe.

---

* Joshua D. Blume currently holds the position of Manager, Tax & Trade at Panasonic Corporation of North America. All views and opinions expressed herein are those of the author alone. Joshua holds a Juris Doctor from Georgetown University Law Center with a Certificate in WTO Studies. Joshua also holds a B.A. with double majors in Economics and International Studies with minors in Classical Studies and Political Science from Utah State University. He would like to thank his wife, Kolbie, for all her love and support, the editors and staff of the Georgetown Journal of International Law for their time and assistance, and all of the other friends, family, and coworkers who helped him with both the genesis of this note and life generally—especially during the travails of the evening law program and passing the Bar. © 2019, Joshua Blume.

I. Introduction

In May 2018, the European Union's (EU) newest law on privacy, the Global Data Protection Regulation (GDPR), went into effect.[1] It brought sweeping changes to privacy protections, included extraterritorial reach, and prescribed fines large enough to make any financial officer blush. The evident goal of the EU has been not only to provide protections for its own citizens but also to establish a new baseline of privacy protections worldwide. Some organizations around the globe are beginning to decide if they should comply with this regulation at all, and if so, to what extent. Those that are contemplating compliance, however, are now in an arduous process of analyzing which provisions to apply to EU data subjects alone versus other global users. With dozens of provisions and exponentially more recitals, companies seeking compliance will remain hard at work for months to come, but two specific provisions, namely the Data Protection Impact Assessment and the Data Protection Officer requirements appear to be requirements that will increase corporate accountability and elevate privacy concerns for multinational corporations for all global data subjects.

The human right to privacy, as specifically outlined in the Universal Declaration of Human Rights,[2] has greatly informed the historical precedents for privacy protections in the EU. A renewed vigor in search of those protections in the digital age helps explain why the EU has adopted a new privacy law. Informed companies will continue to determine exactly how to proceed with compliance for EU data subjects and will bucket their options for global data subjects into three categories: global applicability; a fragmented approach, applying the provision only in the EU while a different set of policies elsewhere; or wait and see how different member states will apply and enforce the law against other companies before taking action. Two provisions of the law, the Data Protection Impact Assessment and the Data Protection Officer requirements, are constructed in such a way that many companies will feel strongly incentivized to adopt them globally. Other laws, such as the U.K. Modern Slavery Act,[3] provide similar though imperfect

1. Parliament and Council Regulation 2016/679 of April 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 [hereinafter GDPR], http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

2. G.A. Res. 217 (III) A; Universal Declaration of Human Rights (Dec. 10, 1948), available at http://www.un.org/en/universal-declaration-human-rights/ [hereinafter UDHR].

3. Modern Slavery Act 2015, c. 30 (Eng.), http://www.legislation.gov.uk/ukpga/2015/30/pdfs/ukpga_20150030_en.pdf.

analogies for why companies will apply the GDPR standards globally for these two provisions. As just two provisions of a massive and complex law, further research is necessary to determine how companies are likely to continue responding to the dozens of other requirements set forth in the EU's newest and the world's most daunting privacy law.

II. Background

A. *The Human Right to Privacy*

In the aftermath of World War II, many countries and human rights activists felt that the need to preserve privacy was paramount, and as such, it was included in the Universal Declaration of Human Rights; specifically, Article 12 reads:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[4]

Though this right to privacy is clearly outlined in the Universal Declaration of Human Rights, states have chosen to apply it in different ways.[5] The EU has long been considered one of the most vocal defenders of this principle of privacy.[6] European Commission (EC) President Jean-Claude Juncker elaborated on the EU view of mandatory privacy protections in his 2016 State of the Union by stating:

> Europeans do not like drones overhead recording their every move, or companies stockpiling their every mouse click. In Europe, privacy matters. This is a question of human dignity.[7]

---

4. UDHR, *supra* note 2, art. 12.

5. *Compare, e.g.*, U.S. Const. amend. I *with* Charter of Fundamental Rights of the European Union, Dec. 7, 2000, O.J. (C 364) 1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf/.

6. For one example of this is the controversial "right to be forgotten," see, e.g., Michael Geist, *Did a Canadian court just establish a new right to be forgotten online?*, Globe & Mail (Feb. 6, 2017), http://www.theglobeandmail.com/report-on-business/rob-commentary/did-a-canadian-court-just-establish-a-new-right-to-be-forgotten-online/article33915916/?utm_source=twitter.com&utm_medium=Referrer:+Social+Network+/+Media&utm_campaign=Shared+Web+Article+Links/.

7. European Commission Press Release IP/16/3042, The State of the Union 2016: Towards a Better Europe – A Europe that Protects, Empowers and Defends (Sept. 14, 2016), europa.eu/rapid/press-release_IP-16-3042_en.htm.

More telling, however, is the EC webpage dedicated to the protection of personal data that specifies "everyone has the right to the protection of personal data."[8]

These views are not, however, confined to EU citizens.[9] In a world with self-driving cars, electronic payment via watches, blood pressure tracking implants, and so much more, consumers are demanding that companies start to think more seriously about privacy protections.[10] The competition for consumers' time and information is now also starting to wax and wane according to the protections given to information, because, whether natively or not, companies with large numbers of returning users are improving privacy disclosures and protections.[11] Microsoft, for example, has updated its detailed privacy statement to be more readable and now includes a specific human rights page that cites the need for privacy and data protection for consumers.[12] How that information is protected and shared, and what consumers can do to limit that sharing, delete their information, or seek enhanced security or restrictions for their data is further explained on a separate page dedicated solely to the human right of privacy.[13]

Protections and disclosures regarding the use of personally identifiable information (PII) are all but uniform, with different industries and companies still trying to find their own sweet spot for collecting and using PII while permitting explicit opt-out options for consumers.[14] All the while, tensions and stakes are high in Europe, and they will likely

8. *Protection of Personal Data*, EUR. COMM'N, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data (last visited Jan. 2, 2019).

9. *See generally* Bellman et al., *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, 20 INFO. SOC'Y 313 (2004), https://www8.gsb.columbia.edu/sites/decisionsciences/files/files/1172.pdf.

10. Omri Ben-Shahar, *Privacy Protection Without Law: How Data Privacy Is Shaped by Market Forces*, FORBES (Jan. 30, 2017), https://www.forbes.com/sites/omribenshahar/2017/01/30/privacy-protection-without-law-how-data-privacy-is-shaped-by-market-forces/#17e2bd6b7800/.

11. *But see* Leslie K. John, *We Say We Want Privacy Online, But Our Actions Say Otherwise*, HARV. BUS. REV. (Oct. 16, 2015), https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise/ (detailing how, in 2015, consumers complained about the lack of privacy protections but did not do much to change their habits or opt-out of data collection).

12. *Human rights*, MICROSOFT, https://www.microsoft.com/en-us/about/corporate-responsibility/human-rights/ (last updated Nov. 2016).

13. *Privacy at Microsoft*, MICROSOFT, https://privacy.microsoft.com/en-US/ (last visited Apr. 26, 2017).

14. *See generally* Florencia Marotta-Wurgler, *Self-Regulation and Competition in Privacy Policies*, 45 J. LEGAL STUD. S13 (June 2016) (finding that adult sites are more likely to make "concise and clear notice of privacy practices" including limiting data sharing with third parties while could-computing sites are more "likely to follow stringent data security standards").

continue to be so for some time; in late 2016, Oracle Corp. went so far as to brief European antitrust regulators about the deceptive consent mechanisms used by Alphabet Inc.'s Google to collect consumer PII in exchange for services.[15] On the other side of the pond, the U.S. Federal Trade Commission (FTC) has been given the power to enforce privacy promises under Section 5 of the FTC Act for false claims.[16] This enforcement is, however, limited in the sense that the FTC can only bring a case against a company for acting with deception or in contradiction of the company's public privacy statement.[17] Furthermore, the consumer must be able to show "substantial injury" by the company that was not "reasonably avoidable" and not "outweighed by countervailing benefits."[18] Therefore, if a company elects to utilize different privacy statements in the EU and the United States, it can effectively apply different standards of collection and protections to consumers.[19]

B. *The DPD and Subsequent Evolution of Digital Privacy in the EU*

In October 1995, the European Parliament and Council passed Directive 95/45/EC, also known as the Data Protection Directive

15. Natalia Drozdiak & Jack Nicas, *Google Privacy-Policy Change Faces New Scrutiny in EU*, WALL ST. J. (Jan. 24, 2017, 6:51 PM), https://www.wsj.com/articles/oracle-expresses-concern-to-eu-over-google-privacy-policy-1485263548/.

16. Federal Trade Commission Act, § 5, 15 U.S.C. § 45 (2012). *See also Enforcing Privacy Promises*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises/ (last visited Apr. 26, 2017).

17. *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FTC, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority/ (last revised July 1, 2008).

18. *Id. But see, e.g.*, *Vizio to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Smart Televisions without Users' Consent*, FTC (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it/ (fining Vizio $2.2 million for improper use of PII outside the scope of the privacy notice provided to consumers).

19. However, EU citizen data must be transferred using an adequacy agreement that supplies "essentially equivalent" protections. This is what had previously invalidated the U.S.-EU Safe Harbor program and recently gave rise to the EU-U.S Privacy Shield program.

Court of Justice of the European Union Press Release No. 117/15, The Court of Justice declares that the Commission's US Safe harbor Decisions is invalid (Oct. 6, 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf/. This has given rise to the EU-U.S. Privacy Shield agreement. *See Privacy Shield Overview*, INT'L TRADE ADMIN., https://www.privacyshield.gov/Program-Overview (last accessed Apr. 26, 2017). *But see* Jacques Bourgeois et al., Sidley Austin LLP, Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States (2016), http://www.sidley.com/~/media/publications/essentially-equivalent—final.pdf/ (arguing that the U.S. and EU systems provide "essentially equivalent" protections for privacy).

(DPD).[20] This law has governed EU data privacy over the past two decades, throughout the invention of the Internet, smartphones, and the quickly evolving Internet of things. Many of the DPD's definitions have naturally become ambiguous in the age of social media, networking, viral videos, virtual shopping, and e-mail. Sensing inadequacy in this older law and recognizing the impact of globalization and the Internet, the EU has opted to update its more than twenty-year-old law in response to the current marketplace.[21]

While beyond the scope of this paper, the DPD was successful at creating the modern understanding of controllers, processors, and subprocessors of data.[22] This distinction between these different groups was key because the DPD only regulated controllers, which were defined as "the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[23] Many provisions have been updated, including the GDPR's coverage of processors, but the definitions remain the same.[24] Essentially, this means that while only original recipients of data would be responsible for their safety, security, and clear consent for usage of that PII, now entities, individuals, organizations, or public authorities that receive PII from a third party must also provide the required protections for the human right of privacy, at least as far as the EU interprets the law.[25]

---

20. 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML/ [hereinafter Directive 95/46/EC].

21. It should be noted that while directives merely set "goal[s] that all EU countries must achieve," regulations are "binding legislative act[s]." *Regulations, Directives and other acts*, EUR. UNION, https://europa.eu/european-union/eu-law/legal-acts_en/ (last visited Apr. 26, 2017). This is a fundamental difference that will provide greater uniformity of enforcement throughout the EU for privacy protections established in the GDPR. *See id.*

22. For an in-depth analysis, see, e.g., Candidate 8016, The Relations of Controllers, Processors and Sub-processors under the DPD and GDPR (Dec. 1, 2016) (unpublished manuscript), https://www.duo.uio.no/bitstream/handle/10852/54570/ICTLTHESIS_8016.pdf?sequence=1&isAllowed=y/.

23. Directive 95/46/EC, *supra* note 20, art. 2. *See also* SEEUNITY, THE MAIN DIFFERENCES BETWEEN THE DPD AND THE GDPR AND HOW TO ADDRESS THOSE MOVING FORWARD (2017), https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf.

24. *Compare* Directive 95/46/EC, supra note 20, art. 2 *with* GDPR, *supra* note 1, art. 4.

25. *See* Bridget Treacy, *Working Party confirms 'controller' and 'processor' distinction*, 10 PRIVACY & DATA PROTECTION 3, 3-5 (2010), https://www.hunton.com/files/Publication/8fe272d1-d29c-4abd-85ae-17843d084da3/Presentation/PublicationAttachment/6d1be60b-be7d-413c-bd6f-6ee37c02c631/Treacy_controller-processor_distinctions.pdf.

C. *The EU Revisits Privacy with the GDPR*

1. Background on Changes

In January 2012, the EC proposed a reformation of the EU data protection rules.[26] In coordination with the Digital Single Market initiative, the EC's goal was to provide an answer to the ninety percent of EU citizens requesting the same data protection rights and rules across the EU.[27] Over the next four years, the EC provided factsheets,[28] questions and answers,[29] polls,[30] and an impact assessment[31] on the need for an enhanced data protection law.[32] Then, on April 27, 2016, the EU Parliament and Council passed Regulation (EU) 2016/679, also known as the GDPR.[33] According to the EC, the eighty-eight-page document is "an essential step to strengthen citizens' fundamental rights in the digital age."[34] In pursuit of a smooth transition, the EU member states had until May 2018 to transpose it into national law when the regulation took effect.[35]

Despite having months to prepare, the EU's announcement of "heavy fines" enhanced anxiety for many companies.[36] Those fines are set at "€20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater" for serious derogations from the law, while lessor derogations will be fined 2% of global revenues, or €10

---

26. *Reform of EU data protection rules*, EUR. UNION, http://ec.europa.eu/justice/data-protection/reform/index_en.htm/ (last visited Apr. 26, 2017).

27. *Digital Single Market*, EUR. UNION, https://ec.europa.eu/commission/priorities/digital-single-market/ (last visited Apr. 24, 2017).

28. *See, e.g.*, Ve±ra Jourová, *Data protection Eurobarometer*, EUR. UNION (June 24, 2015), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf.

29. *See, e.g.*, European Commission Press Release MEMO/15/6385, Questions and Answers – Data protection reform (Dec. 21, 2015), http://europa.eu/rapid/press-release_MEMO-15-6385_en.pdf.

30. *See, e.g.*, EUR. COMM'N, SPECIAL EUROBAROMETER 359: ATTITUDES ON DATA PROTECTION AND ELECTRONIC IDENTITY IN THE EUROPEAN UNION (2011), http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

31. *See Impact Assessment*, SEC (2012) 72 final (Jan. 25, 2012), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN.

32. *See Digital Single Market*, *supra* note 27.

33. Commission Regulation 2016/679, 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN/.

34. *Reform of EU data protection rules*, EUR. UNION, http://ec.europa.eu/justice/data-protection/reform/index_en.htm/ (last visited Apr. 26, 2017).

35. *Id.*

36. EU GDPR.ORG, http://www.eugdpr.org/ (last visited Apr. 26, 2017) (also note the stress-inducing countdown clock).

million, whichever is greater.[37] As if the fines were not sufficient, the gravity of the law has been further increased as the GDPR also includes new rules about the territorial scope.[38] According to Article 3, the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the EU, regardless of whether the processing takes place in the EU or not.[39] It continues to include "the processing of personal data of data subjects who are in the EU by a controller not established in the EU, where the processing activities" that are "related to" the monitoring of a data subject's behavior within the EU or of goods and services, "irrespective of whether"[40] payment is required.[41] This application to controllers as well as processors has widely broadened the scope of the EU's privacy protections. Now organizations that have not previously worried about data protection rules in the EU are being strongly encouraged to start.

2. Overview of Provisions

As noted above, the law specifically includes an "increased territorial scope" that allows the EU to sue "all companies processing the personal data of data subjects residing in the EU, regardless of the company's location."[42] Thus, the law applies to all transnational companies and organizations, regardless of where they are based.[43] With this broad

37. GDPR, *supra* note 1, art. 83(4-5). *See also* Kuan Hon, *GDPR: Potential fines for data security breaches more severe for data controllers than processor*, REG. (May 12, 2016, 08:33 AM), http://www.theregister.co.uk/2016/05/12/gdpr_potential_fines_for_data_security_breaches_more_severe_for_data_controllers_than_processors_says_expert/.

38. *See* Allison Callahan-Slaughter, Comment, *Lipstick on a Pig: The Future of Transnational Data Flow Between the EU and the United States*, 25 TUL. J. INT'L & COMP. L. 239, 252 (2016).

39. GDPR, *supra* note 1, art. 3(1).

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

41. *See GDPR FAQs*, EU GDPR.ORG, http://www.eugdpr.org/gdpr-faqs.html/ (last visited Apr. 27, 2017) (stating that the "GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects," and that it "applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location"). *See also* E. Bougiakiotis, *The enforcement of the Google Spain ruling*, 24 INT. J. LAW INFO. TECH. 311 (2016) (explaining the implications of the *Google Spain* case on the EU's extraterritorial enforcement of privacy protections).

42. *GDPR Key Changes*, EU GDPR.ORG, http://www.eugdpr.org/key-changes.html/ (last visited Apr. 27, 2017). *See also GDPR FAQs*, *supra* note 41.

43. Warwick Ashford, *EU data protection rules affect everyone, say legal experts*, COMPUTER WEEKLY (Jan. 11, 2016, 5:00 PM), http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts (quoting Stewart Room, cyber security and data protection partner at PricewaterhouseCoopers, "This will impact every entity that holds or uses European personal data both inside and outside of Europe").

reach comes dozens of new rules and regulations that each of these companies will need to weigh as they contemplate the risk of fines posed by the GDPR.[44] Some of these mandated rights for data subjects include breach notification within a grueling seventy-two-hour window, the right for all data subjects to access their personal information, and the "right to be forgotten."[45] The structure of some of the rules means that this combination of fines, requirements, and the strong response of multinational companies[46] to the regulation is likely to set a new floor for data privacy protections around the world.[47] There are two provisions that are likely to have the most immediate effect, namely, the Data Protection Impact Assessment and the Data Protection Officer requirements. [48]

a. Data Protection Impact Assessment

As required by Section 3 of the GDPR, for the first time, data controllers are required by law to conduct a Data Protection Impact Assessment (DPIA) with the assistance of a data protection officer (DPO).[49] The idea is to facilitate a better understanding of what is being done with EU data subjects' PII; as one consulting firm suggests, this is likely to yield "more uniform assessments."[50] These impact assessments are to be conducted before the collection of PII and directly

44. *See, e.g.*, *Pulse Survey: US Companies ramping up General Data Protection Regulation (GDPR) budgets*, PwC, http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf/ (last visited Apr. 27, 2017), for an analysis of company views.

45. *GDPR Key Changes*, *supra* note 42.

46. *See* PwC, *supra* note 44.

47. *See, e.g.*, Tiffany Curtiss, *Privacy Harmonization and the Developing World: The impact of the EU's General Data Protection Regulation on developing economies*, 12 Wash. J.L. Tech. & Arts 95, 95-96 (2016) (further assessing the impact of the GDPR on other countries).

48. Though interesting and worth research unto themselves, the entirety of the GDPR provisions and their likelihood of adoption are beyond the scope of this paper. To read more on some of these provisions, including data portability, limitations on profiling, documentations and recordkeeping, privacy by design and by default, right to object to processing, and data breach notifications please see, e.g., Alex van der Wolk & Sotirios Petrovas, The EU General Data Protection Regulation: A Primer for International Business, Morrison Foerster (2016), https://www.mofo.com/resources/publications/the-eu-general-data-protection-regulation-a-primer-for-international-business.pdf.

49. GDPR, *supra* note 1, art. 35(1-2). *See also* Felix Bieker et al., *A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation*, 4 Privacy Tech & Pol'y 21, 24-36 (2016), http://www.springer.com/cda/content/document/cda_downloaddocument/9783319447599-c2.pdf?SGWID=0-0-45-1587701-p180200777/.

50. *The General Data Protection Regulation: Long awaited EU wide data protection law finalised*, Deloitte, https://www2.deloitte.com/nl/nl/pages/risk/articles/the-general-data-protection-regulation.html/ (last visited Apr. 27, 2017).

published by the supervising Data Protection Authority (DPA).[51] DPIAs are compulsory "where a type of processing . . . is likely to result in high risk to the rights and freedoms of natural persons."[52] Each data controller must analyze the type of data they are collecting, as well as "assess privacy risks to individuals" and the nature, "use and disclosure of their personal data."[53] At a minimum, the DPIA must include:

> a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
> b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
> c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
> d) the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.[54]

Due to the required depth and breadth of the DPIA, organizations have been encouraged for months now to analyze the impact their actions have on PII.[55] This has forced companies to begin contemplating how they will continue work with the DPAs (or start if they have not yet begun to do so), integrate their DPO, and tailor the fundamental rights proclaimed in the GDPR to their own business.[56] Much like the U.K. Modern Slavery Act and other impact assessment requirements, companies will be strongly encouraged to begin thinking about how they disclose their business processes; the GDPR may also prove to

51. GDPR, *supra* note 1, art. 35(5-6).

52. GDPR, *supra* note 1, art. 35(1). *See also id.* art. 35(3) (providing explicit language also encouraging DPIAs in particular scenarios).

53. *Sample DPIA Template*, IAPP, https://iapp.org/resources/article/sample-dpia-template/ (last visited Nov. 18, 2018).

54. GDPR, *supra* note 1, art. 35(7).

55. Monique Magalhaes, *GDPR: Data Protection Impact Assessment*, TECHGENIX (Feb. 13, 2017), http://techgenix.com/gdpr-data-protection-impact-assessment/.

56. *See* Bieker, *supra* note 49, at 24-36.

nudge companies to utilize broader assessment frameworks such as the U.N. Guiding Principles Reporting Framework.[57]

b. Data Protection Officers (DPO)

The GDPR also requires a designated Data Protection Officer to ensure compliance with the GDPR; DPOs are "the cornerstone of the GDPR's accountability regime."[58] Before the GDPR went live in May 2018, one study anticipated that the regulation would require 75,000 organizations to have active DPOs.[59] Chapter IV, Section 4 of the GDPR is dedicated to explaining the designation process, position, and responsibilities of the DPOs.[60] As one firm has put it, a key change the GDPR brings is that DPOs now "have direct obligations for the first time."[61] They must also have "expert knowledge of data protection law and practices."[62] DPOs may also "insist upon company resources" to accomplish their required duties, as well as have "significant independence," including a "direct reporting line 'to the highest level of management.'"[63] Furthermore, Article 38(3) prohibits the firing of DPOs for "performing [their] tasks" and demands that organizations must ensure that other tasks assigned to DPOs "do not result in a conflict of interests," further guidance for which suggests they cannot be located in the C-suite of the organization.[64]

57. SHIFT PROJECT & MAZARS, UN GUIDING PRINCIPLES REPORT FRAMEWORK (2015), https://www.ungpreporting.org/database-analysis/.

58. Fiona Maclean & Calum Docherty, *GDPR Guidance: DPOs, Data Portability & the One-Stop-Shop*, LATHAM & WATKINS GLOBAL PRIVACY & SECURITY COMPLIANCE: L. BLOG (Dec. 20, 2016), http://www.globalprivacyblog.com/privacy/gdpr-guidance-dpos-data-portability-the-one-stop-shop/.

59. Rita Heimes & Sam Pfeifle, *Study: GDPR's global reach to require at least 75,000 DPOs worldwide*, IAPP (Nov. 9, 2016), https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.

60. GDPR, *supra* note 1, art. 37-39.

61. *Preparing for the General Data Protection Regulation*, ALLEN & OVERY (January 2018), http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf.

62. GDPR, *supra* note 1, at pmbl. ¶ 97.

63. Rita Heimes, *Top 10 operation impacts of the GDPR: Part 2 – The mandatory DPO*, IAPP (Jan. 7, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-the-mandatory-dpo/ (citing GDPR, *supra* note 1, art. 38(3)).

64. GDPR, *supra* note 1, art. 38(3), 38(6); EU Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs')*, 15-16, WP 243 (revised Apr. 5, 2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=44100/.

Though many companies may choose to outsource this role, a study by the International Association of Privacy Professionals (IAPP) estimates that, on the low end, it costs twenty-one hours of training to achieve "baseline competence" for DPOs.[65] These training and preparation costs will likely be most prohibitive to smaller businesses, but many are looking to how Germany has provided flexibility for outsourcing this role as the best potential example for how the GDPR will work in practice.[66] While there are few laws' impacts that are fully analogous to the impact this requirement will have on the thousands of businesses affected by this requirement, as discussed more below in Section IV(B)(ii)(1), Sarbanes-Oxley's (SOX) requirement that the CEO and CFO directly certify financial statements may be a close analogy and provide valuable lessons for companies to apply in the GDPR context.[67]

D. *Extraterritoriality and the Effect on Business Decisions*

Of all the provisions in the GDPR, one of the most monumental is the explication of its extraterritoriality. Article 3 explains that the "regulation applies to the processing of data"[68] for subjects residing in the EU, regardless of where in the world the processor or controller is located.[69] This dramatic change from the DPD has caused myriad firms

65. *From Here to DPO: Building a Data Protection Officer*, IAPP, 1, https://iapp.org/media/pdf/resource_center/From_Here_to_DPO_FINAL.pdf (last visited Apr. 27, 2017) ("baseline competence" construed as a basic understanding of GDPR itself).

66. David Meyer, *What will mandatory DPOs look like under the GDPR? Germany could tell you*, IAPP (June 6, 2016), https://iapp.org/news/a/what-will-mandatory-dpos-look-like-under-the-gdpr-germany-could-tell-you/. *See also Guidelines on Data Protection Officers ('DPOs')*, *supra* note 64, at 15-16 (describing the WP29's DPO guidelines).

67. *Sarbanes Oxley FAQ*, Sarbanes-Oxley-101.com, http://www.sarbanes-oxley-101.com/sarbanes-oxley-faq.htm/ (last visited Apr. 27, 2017).

68. GDPR, *supra* note 1, art. 3. *See also Recital 22: Processing by an establishment*, INTERSOFT CONSULTING, https://gdpr-info.eu/recitals/no-22/ (last visited Oct. 3, 2018); *Recital 23: Applicable to processors not established in the Union if data subjects wihtin [sic] the Union are targeted*, INTERSOFT CONSULTING, https://gdpr-info.eu/recitals/no-23/ (last visited Oct 3. 2018); *Recital 24: Applicable to processors not established in the Union if data subjects within the Union are profiled*, INTERSOFT CONSULTING, https://gdpr-info.eu/recitals/no-24/ (last visited Oct. 3, 2018); *Recital 25: Applicable to processors due to international law*, INTERSOFT CONSULTING, https://gdpr-info.eu/recitals/no-25/ (last visited Oct. 3, 2018).

69. *See generally Material and territorial scope*, BIRD & BIRD LLP, https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/11–guide-to-the-gdpr–material-and-territorial-scope.pdf?la=en (last visited Apr. 27, 2017) (noting GDPR also includes the "monitor[ing]" of EU individuals' behavior with very limited exclusions); *New rules, wider reach: the extra-territorial scope of the GDPR*, 1-2, Slaughter & May (June 2016), https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf (noting that the recent *Google Spain* case had portended this shift toward extraterritoriality).

and businesses to respond with business solutions and outreach to businesses domiciled outside of the EU.[70] Many firms that did not previously feel the need to provide access to remedies such as the right to be forgotten must now recalibrate their privacy notices and reframe their approaches to privacy if they do not want to roll the dice on millions of euros in fines.

The question many firms will consider, however, is the likelihood that a throw of the dice will yield a massive judgement against them. One author has argued that while extraterritoriality's broad power may be checked by continued roadblocks for EU evidence requests, the ability of the EU to obtain necessary evidence is likely to expand greatly.[71] This will provide the EU with the necessary tools to fully prosecute foreign-based subsidiaries, especially in the United States.[72] However, evidence requests are just a small part of the puzzle (see Appendix I for an introductory analysis of the effect of the growth of Data Protection Authorities on one example).[73] Unfortunately, it will be impossible to know exactly how much sway the GDPR will have over companies domiciled within and outside of the EU before actions start to be brought, but other laws with strong extraterritorial power, such as the U.S. Foreign Corrupt Practices Act, could provide some helpful perspective.

1. Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act of 1977 (FCPA) was originally enacted to discourage bribery and kickbacks.[74] Nearly thirty-five years

---

70. *See, e.g.*, *Tips for U.S. Companies in the Age of EU GDPR and Privacy Shield: A collection of expertly crafted articles and guidance*, BUREAU OF NATIONAL AFFAIRS, INC., https://www.bna.com/uploadedFiles/BNA_V2/Legal/Pages/Custom_Trials/BLPV/Tips_for_US_Companies_EU_GDPR_Privacy_Shield_final.pdf (last visited Apr. 27, 2017) (hosting a collection of articles providing tips to U.S. companies on the GDPR).

71. *GDPR will result in significant increase in litigation*, PWC (Feb. 4, 2017), available at http://www.privacyrisksadvisors.com/news/gdpr-will-result-in-significant-increase-in-litigation-pwc/.

72. *Id.*

73. *Id. See also, e.g.*, Jonathan Millard & Tyler Newby, *EU's General Data Protection Regulation: Sweeping Changes Coming to European and U.S. Companies*, AMERICAN BAR ASS'N: PRIVACY AND DATA SECURITY (May 23, 2016), http://apps.americanbar.org/litigation/committees/technology/articles/spring2016-0516-eu-general-data-protection-regulation.html/; David Moncure, John Del Piero & Jeffrey McKenna, *The General Data Protection Regulation's Key Implication for E-Discovery*, INSIDE COUNSEL (Nov. 23, 2016), http://www.insidecounsel.com/2016/11/23/the-general-data-protection-regulations-key-implic/ (describing how "awareness" of growing E-Discovery powers in the EU can be connected with "jaw-dropping financial penalties" to hold foreign-based entities accountable to the GDPR).

74. *Foreign Corrupt Practices Act: An Overview*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act/ (last visited Apr. 27, 2017).

after its passage, the New York Bar Association penned an impact report detailing the worry the FCPA was causing U.S. companies currently subject to the law and contrasting that worry with the law's effects on companies not subject to the FCPA.[75] The report argues that worry and fear often preclude companies from acquiring foreign entities in jurisdictions where anti-corruption laws are not stringently enforced or require a lower reporting threshold.[76] This burden has prohibited companies subject to the FCPA from being as competitive as they would like to be. On the other hand, companies that are not currently subject to the law tend to avoid coming under the law's jurisdiction as much as possible.

Much like violations of the GDPR, violations of the FCPA are no laughing matter, and besides the naming and shaming entailed in posting violators on the Securities and Exchange Commission (SEC) website, the associated fees frequently run in the millions of dollars, averaging $156.6 million in 2014.[77] In 2016 alone there were twenty-six enforcement actions totaling $2.3 billion.[78] Because the GDPR allows for fines based on topline revenue, these numbers are not beyond the pale of possibility, and for some companies, the annual representations could act as a starting benchmark.[79] The simple power behind each of these laws is that they allow for enforcement of crimes committed halfway across the world to be prosecuted in either the United States (FCPA) or Europe (GDPR).[80] While there are some limitations to foreign "issuers," under the FCPA, a vast amount of correspondence and

75. *See generally* The FCPA and its Impact on International Business Transactions: Should Anything be Done to Minimize the Consequences of the U.S.'s Unique Position on Combating Offshore Corruption? (2011), NEW YORK CITY BAR, http://www2.nycbar.org/pdf/report/uploads/FCPAImpactonInternationalBusinessTransactions.pdf/.

76. *Id.*

77. *See SEC Enforcement Actions: FCPA Cases*, Securities and Exchange Comm'n, https://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml (last visited Apr. 27, 2017). S*ee also*, Baker Hostetler, *Top 10 SEC Enforcement Highlights of 2016*, JDSUPRA (Jan. 26, 2017), http://www.jdsupra.com/legalnews/top-10-sec-enforcement-highlights-of-42964/ (including in the list the September ruling against Och-Ziff for bribes to government officials in Africa).

78. Nicole H. Sprinzen, *US anti-bribery law set to remain in place under Trump*, FINANCIAL TIMES (Dec. 29, 2016) https://www.ft.com/content/a5b6d5e8-c951-11e6-8f29-9445cac8966f/.

79. For example, Apple, Inc. had posted more than $82 billion in revenue for just Q3 and Q4 in 2016; thus, if they were to be fined at the lower two-percent threshold, it would result in fines greater than $1.6 billion. *See* Apple Inc., Q4 2016 Unaudited Summary Data, https://images.apple.com/newsroom/pdfs/Q4FY16DataSummary.pdf (last visited Apr. 27, 2017).

80. Sean Hecker & Margot Laporte, *Should FCPA "Territorial" Jurisdiction Reach Extraterritorial Proportions?*, 42 INT'L L. NEWS, (Winter 2013), http://www.americanbar.org/publications/international_law_news/2013/winter/should_fcpa_territorial_jurisdiction_reach_extraterritorial_eproportions.html/.

interstate commerce around the world finds its way home to the United States.[81] Though the laws do not provide perfect parallels, past precedent seems to indicate that when a powerful country or group of countries decides to crack down on ethical compliance, they can do so with reasonably strong effect. Thus, all else being equal, the GDPR's requirements will likely set a new global standard for compliance that may still take time to catch on, but, if appropriately enforced, will set a new floor for privacy protections.[82]

E. *The Current State of Play and Enforceability of the GDPR*

1. A Shift in Focus from Government to Business Use of Data

As data continues to evolve and expand, so too has the definition of PII.[83] In recent years, a common debate in different countries has been whether IP addresses can be defined as PII.[84] The nature and business of any organization is most likely to differentiate how individual PII is captured, utilized, retained, and disposed of; as one example, the Electronic Frontier Foundation uses five categories to rate organizational transparency of data usage centering mainly on responses to

81. Mike Koehler, *Into the FCPA's Jurisdiction Thicket*, FCPA PROFESSOR L. BLOG (Apr. 28, 2015), http://fcpaprofessor.com/into-the-fcpas-jurisdictional-thicket/ (referencing a May 2014 FBI affidavit for wire fraud signaled foreign-sent e-mails that were received and stored on Google's servers in Northern California as basis for their jurisdiction; a move that should echo the shivers created by the jurisdiction ruling in the *Google Spain* case for privacy). *Cf.* Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (holding that jurisdiction over Google Inc. applied because the nature of data transfers between the subsidiary and parent company gave the government with controlling authority over the subsidiary jurisdiction over the information transferred to the parent company in another jurisdiction).

82. *See, e.g.*, Wim Nauwelaerts & Anna Pateraki, *2017-1 GTDT: Data Protection & Privacy EU overview*, 1 DATA PROTECTION & PRIVACY (2017) (summarizing the new GDPR compliance standards).

83. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New concept of Personally Identifiable Information*, BERKELEY L. SCHOLARSHIP REPOSITORY, 1814, 1815-19 (Jan. 1, 2011), http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs/ (introducing divergent views on PII). Though beyond the scope of this paper, there are dozens of studies, analyses and far more opinions about the varying types of treatment of PII. *See, e.g.*, Alexander Southwell et al., *Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy*, CLS BLUE SKY BLOG (Feb. 3, 2017), http://clsbluesky.law.columbia.edu/2017/02/03/gibson-dunn-reviews-u-s-cybersecurity-and-data-privacy/.

84. Frederick Lah, *Are IP Addresses "Personally Identifiable Information"?*, 4 J.L. & POL'Y INFO. SOC'Y, 676, 679-83 (2008), http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Lah_Formatted_Final.pdf.

government requests for data.[85] Much of the focus on telecom, social media, cloud computing, and other platforms has centered on government disclosure requests in the United States.[86] The GDPR, however, is likely to usher in a new age of consumer protections; some have argued that the use of DPIAs, as just one example, will make it easier for outside organizations to review the use and treatment of consumer data for marketing and business purposes.[87]

2. Shortfalls in Current Protections and Overall Readiness for the GDPR

Now that the GDPR is in effect, it is likely that more companies will begin to rework their compliance procedures. That said, one survey of U.S. CIOs in 2016 found that eighty percent of U.S. companies that house data for subjects in the EU under the protection of the GDPR were not at that time securing the required consent from those individuals.[88] A separate independent study by the British Standards Institution (BSI) just one month before GDPR went into effect found that, of 1,800 firms surveyed, ninety-seven percent agreed that GDPR would affect them, but only five percent felt "fully prepared" and only thirty-three percent were "halfway to complying."[89] In the wake of their "GDPR Preparedness Pulse Survey" back in December 2016, PricewaterhouseCooper's (PwC) U.S. privacy leader, Jay Cline, announced that while ninety-two percent of respondents have reported GDPR compliance among their business' top priorities for 2017,

85. Nate Cardozo, Kurt Opsahl & Rainey Reitman, *Who Has Your Back?: Protecting your data from government requests*, ELECTRONIC FRONTIER FOUNDATION (June 17, 2015), https://www.eff.org/files/2015/06/18/who_has_your_back_2015_protecting_your_data_from_government_requests_20150618.pdf (including five categories: "Follows industry-accepted best practices," "Tells users about government data demands," "Discloses policies on data retention," "Discloses government content removal requests," and "Pro-user public policy: opposes backdoors").

86. For a sample of surveys focused on the responses to privacy practices in the United States, see, e.g., *Public Opinion on Privacy*, EPIC.ORG, https://epic.org/privacy/survey (last visited Apr. 27, 2017).

87. *See generally* Warwick Ashford, *European data protection law to give consumers more control*, COMPUTER WEEKLY (Mar. 6, 2017), http://www.computerweekly.com/news/450414345/European-data-protection-law-to-give-consumers-more-control/ (analyzing how the GDPR is likely to "give consumers more control").

88. Marcin Grabinski, *Survey Shows US CIOs Getting a GDPR Headache*, INFORMATION WEEK (Feb. 21, 2017), http://www.informationweek.com/strategic-cio/survey-shows-us-cios-getting-a-gdpr-headache/a/d-id/1328219/.

89. Zach Emmanuel, *Most Organizations Unprepared for GDPR, survey finds*, COMPUTER WEEKLY, https://www.computerweekly.com/news/252440114/Most-organisations-unprepared-for-GDPR-survey-finds/ (last visited Oct. 4, 2018).

"American multinationals" that had not already taken "significant steps" to adequately prepare for the GDPR were quickly falling behind.[90] Considering there was so little change in preparedness in the intervening eighteen months seems to indicate that many companies continue to lag behind. That said, there are likely far more businesses and other organizations that are either unaware of or currently lack the necessary resources to even start addressing the new requirements under the GDPR.

On the consumer side, other surveys have found that consumers are becoming more aware of privacy protections and are beginning to demand greater control over their personal information. An International Data Corporation survey found eighty-four percent of consumers are "concerned about" their privacy, with seventy percent stating they were more worried now than in the past.[91] Another study found that nine in ten consumers "worried about online privacy," yet eight out of ten want personalization to their needs that typically "necessitates" collection of personal information.[92] However, another study by Auckland University of Technology found that forty-five percent of 1,377 respondents felt that online privacy does not exist, though only eleven percent reported their privacy had been violated in the past.[93] Thus, despite consumers currently yielding their data up in exchange for services and products, such as personalization that requires data collection, they are becoming more aware of measures that might prevent or limit their disclosure of personal information.

This consumer awareness of data collection has also shown a direct connection to perceptions and trust in certain brands and products; as one example, a Morning Consult Brand Intelligence survey of 22,000 Americans found that favorability of Yahoo dropped ten percent in the

90. PwC, *supra* note 44.

91. *New IDC Survey Finds Widespread Privacy Concerns Among U.S. Consumers*, INTERNATIONAL DATA CORPORATION (Jan. 24, 2017), http://www.idc.com/getdoc.jsp?containerId=prUS42253017/. *See also* Matt Hamblen, *Privacy worries are on the rise, new poll of U.S. consumers shows*, COMPUTERWORLD, (Jan. 30, 2017, 1:01 PM), http://www.computerworld.com/article/3163207/data-privacy/privacy-worries-are-on-the-rise-new-poll-of-u-s-consumers-shows.html/ (finding that younger consumers, an important target market for many companies, are more worried about their privacy).

92. *9 in 10 consumers worried about online privacy (but most want personalization too)*, NET IMPERATIVE (Mar. 9, 2017), http://www.netimperative.com/2017/03/9-10-consumers-worried-online-privacy-want-personalisation/.

93. Shane Cowlishaw & Alexandra Nelson, *Many New Zealand internet users have no expectation of privacy online*, STUFF, (updated Dec. 14, 2016, 12:11 PM), http://www.stuff.co.nz/technology/87541035/many-new-zealand-internet-users-have-no-expectation-of-privacy-online/.

wake of its December 2016 breach notification.[94] Separately, a Cisco Institute study found that almost a quarter of businesses reported lost business opportunities from a "hack or a breach," while nearly a third stated a loss of revenue as a result of a "security incident."[95] Thus, consumers want the freedom and tailor-made experiences the Internet can bring, but they are also wary, even without personal experience of privacy loss, to allow access to their PII. This consumer wariness is, in turn, affecting the bottom line for organizations that operationalize use of PII. As more consumers become aware of the GDPR, and as more investors become aware of the potential fines that are applicable, the market pressure on companies to adopt the EU's new standards is likely only to increase. In fact, as just one example, a coalition of U.S. and EU consumer and privacy rights groups urged Facebook to apply the GDPR principles globally just a month before the law went into effect.[96] As such, it is likely that the more agile and informed a corporation is with regard to privacy issues, the more likely it is to thrive in this new privacy-aware environment.[97]

3. Enforcement Provisions

Before deciding the level of compliance with GDPR's standards, companies are likely to ask: How enforceable is the GDPR? As one firm has pointed out, the GDPR provides new investigatory and corrective powers, in addition to the two-tiered fines.[98] The firm continues to suggest that businesses prioritize "their implementation actions" because Article 79 suggests a broad jurisdiction and right to remedy under the law. Essentially, this provision allows for an individual to raise a complaint wherever the business "has an establishment" or where the "data

94. Amir Nasr, *Consumer's Views of Yahoo Dropped After Latest Data Breach Disclosure*, Morning Consult (Mar. 6, 2017, 4:22 PM), https://morningconsult.com/2017/03/06/consumers-views-yahoo-dropped-latest-data-breach-disclosure/ (representing a drop from 73 percent to 63 percent favorability).

95. Sean Michael Kerner, *Cisco Report Reveals Business Impact of Data Security*, eWeek (Jan. 31, 2017), http://www.eweek.com/security/cisco-report-reveals-business-impact-of-data-security/.

96. Natasha Lomas, *Facebook Urged to Make GDPR Its "Baseline Standard" Globally*, TechCrunch (Apr. 9, 2018), https://techcrunch.com/2018/04/09/facebook-urged-to-make-gdpr-its-baseline-standard-globally/.

97. *Businesses still confused about GDPR*, Help Net Security, Mar. 1, 2017, https://www.helpnetsecurity.com/2017/03/01/gdpr-confusion/.

98. Nuria Pastor & Georgia Lawrence, *Getting to know the GDPR, Part 10 – Enforcement under the GDPR – What happens if you get it wrong*, Field Fisher: Privacy, SECURITY and Info. L. BLOG (Mar. 5, 2016, 4:45 PM), http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-10-enforcement-under-the-gdpr-what-happens-if-you-get-it-wrong/.

subject has his or her habitual residence."[99] Connected with the "one stop shop" provision detailed in Appendix I, this will essentially provide data subjects the opportunity to forum shop, finding the DPA with the most bandwidth, availability, and aggressive stance.[100]

This uniformity of law does not necessarily translate to uniform enforcement, though, because each member state maintains control of its own supervisory authority.[101] Because the GDPR is a regulation, it is "applied in its entirety" in all EU member states simultaneously as of May 2018.[102] In contrast, directives such as the DPD allow individual member states to devise their own laws aimed at achieving a common goal.[103] One example of this is the EU consumer rights directive, which encouraged member states with different judicial systems to enact legislation that would best achieve the goals of the directive.[104] Though there are some provisions in the GDPR that will allow member states to use their own thresholds, such as the age of consent for children, the fundamental protections are the same.[105] Germany is in the process of amending and updating its data protection law to do just this, reiterating many of the pieces of the GDPR while taking advantage of the law's flexible provisions.[106]

---

99. GDPR, *supra* note 1, art. 79(1)-(2).

100. *See infra* Appendix I (detailing growth of DPA enforcement powers and capacity).

101. See infra Appendix I for a description of the interplay between supervisory authorities and their growth in the years since the passage of the GDPR.

102. *Regulations, Directives and other acts, supra* note 21. For one example of another EU regulation with similar international impact, see generally Regulation 2015/478, 2015 O.J. (L 83) 16, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0478&from=EN/ (regulating common rules for imports, a high-priority issue that requires simultaneously and virtually identical enforcement to achieve its true aim).

103. *Regulations, Directives and other acts, supra* note 21.

104. Directive 2011/83/EU, of the European Parliament and of the Council of 25 October 2011, 2011 O.J. (L 304) 64, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&from=EN/.

105. GDPR, *supra* note 1, art. 8. *See also* James Titcomb, *Britain opts out of EU law setting social media age of consent at 16*, Telegraph (Dec. 16, 2015 2:42 PM), http://www.telegraph.co.uk/technology/internet/12053858/Britain-opts-out-of-EU-law-raising-social-media-age-of-consent-to-16.html/ (discussing UK's push for the flexibility to revert to age 13 for online consent); *Briefing Note: Age of Consent in the General Data Protection Regulation*, ICT Coalition, http://ictcoalition.org/gallery/96/Briefing-Note-Age-of-Consent-in-the-General-Data-Protection-Regulation[3].pdf/ (last visited Apr. 27, 2017) (requesting the age of consent be reverted to 13 to create true conformity of law throughout the EU).

106. Tim Wybitul, *German Government Presents Revised Draft GDPR Implementation Bill*, Chronicle of Data Protection L. Blog : International/EU Privacy (Jan. 30, 2017), http://www.hldataprotection.com/2017/01/articles/international-eu-privacy/german-government-presents-revised-draft-gdpr-implementation-bill/.

However, as one author has put it, there are great questions about the efficacy of applying equal standards to controllers and processors and the effects that may have on cross-border data flows and business.[107] As cross-border data flows is still a relatively young issue, international taxation in the EU may prove a helpful comparison for how member states may view GDPR enforcement.[108] Due to its breadth and depth, there is a major question about the ability of the enforcement bodies to control the thousands of global businesses to which the GDPR applies.[109] Thus, many companies are now in a position where they will be debating whether or not the cost of compliance is worth the proportional risk of having actions brought against them.[110]

Despite fines and extraterritoriality provisions eclipsing even the FCPA, many companies may still elect to deprioritize GDPR compliance for now.[111] This may be because the firm is willing to take the compliance risk, remains unaware of or does not understand the law, or simply reasons it will be less likely than other organizations to be among the first targets of DPA investigations. Regardless of the reason, the choice is at least a several million euro toss of the dice.[112] The risk does not end there; as one organization has pointed out, the GDPR provides additional protections and disclosure requirements to encourage

107. Lokke Moerel, *GDPR conundrums: Data transfer*, IAPP: PRIVACY TRACKER (June 9, 2016), https://iapp.org/news/a/gdpr-conundrums-data-transfer/.

108. For a discussion on ease of paying taxes correlated with statutory and effective tax rates, see, e.g., Andrew Packman & Neville Howlett, *Paying Taxes 2017: In-depth analysis on tax systems in 190 economies*, PWC, https://www.pwc.com/gx/en/services/tax/paying-taxes-2017.html (last visited Apr. 27, 2017). *See also* Kyle Pomerleau & Emily Potosky, *Corporate Income Tax Rates around the World, 2016*, TAX FOUNDATION (Aug. 18, 2016), https://taxfoundation.org/corporate-income-tax-rates-around-world-2016/ (comparing tax rate attractiveness across nearly all countries, globally).

109. Rita Heimes & Sam Pfeifle, *supra* note 59 (estimating that 75,000 companies will require a DPO, a standard requirement for businesses that utilize or harbor EU data subject information compared with only 28,000 between the EU and the U.S. combined).

110. Appendix I further describes the growth and improved power of the EU DPAs, including exponential growth in funding since the passage of the GDPR in 2014, the new powers granted to the EC and the individual DPAs, as well as the impact of the "one stop shop" provisions.

111. Monica McDonnell, *Deprioritising GDPR: Is it a Risk Worth Taking*, Informatica Blog (Feb. 9, 2017), https://blogs.informatica.com/2017/02/09/deprioritising-gdpr-risk-worth-taking/#fbid=x0v8jp5RP7P.

112. *Id.* That gamble is not just limited to the fines leveraged by the EU DPAs. Shareholders would very likely bring derivative suits against the company for failing to get in compliance during a multi-year ramp up to enforcement. *See, e.g.*, Seth Aronson et al., *United States: Shareholder Derivative Actions: From Cradle to Grave*, MONDAQ: CORP./COMMERCIAL L. BLOG http://www.mondaq.com/unitedstates/x/87654/Directors+Officers/Shareholder+Derivative+Actions+From+Cradle+To+Grave/ (last updated Jan. 28, 2010).

whistleblowing, meaning that companies will risk increased exposure for noncompliance from the inside as well.[113] This will be most potent for companies with employees or other facilities with direct exposure to the EU or that are located in the EU.[114] On the whole, it seems reasonable to speculate that companies will at least seek to apply some minimum standards from the GDPR if they control or process EU data in the next few years.[115] Due to whistleblower provisions and the effect of the "one stop shop" provisions outlined in Appendix I, it is also likely these decisions will correlate positively with the organization's footprint in the EU.

III. Potential Impact by the GDPR on Global DPIAs and DPOs

Due to the increased enforcement, extraterritoriality, consumer awareness, and market pressures, most companies who either control or process PII covered by the GDPR are facing tough decisions on whether they will implement the provisions globally or only in the EU. While the GDPR does have a very broad extraterritorial scope, it only applies to data received from data subjects controlled by EU law.[116] In other words, global companies may elect to apply the provisions of the GDPR differently, with certain protections available only to the data subjects protected by GDPR.[117] However, the increasing demand by

113. Karin Henriksson, *Implications of the General Data Protection Regulation On Corporate Whistleblowing*, Ethic Intelligence, (Dec. 12, 2016), http://www.ethic-intelligence.com/experts/17525-implications-general-data-protection-regulation-corporate-whistleblowing/. *See also*, Claire Johnson & Jessica Nall, *United States: Revenge of the Whistle-Blower: Possible Consequences of Compliance Failures*, Mondaq: Corp./Commercial L. Blog, http://www.mondaq.com/unitedstates/x/574742/Compliance/Revenge+Of+The+WhistleBlower+Possible+Consequences+Of+Compliance+Failures/ (last updated Mar. 7, 2017) (arguing that compliance costs in the U.S. are likely to increase due to lack of whistleblower protections).

114. *See, e.g.*, Stefan Nerinckx, Tim Van Canneyt & Gaëtan Goossens, *The New EU Data Protection Regime from an HR Perspective*, Am. Chamber of Commerce Belg., http://www.amcham.be/publications/amcham-connect/2016/march/fieldfisher-gdpr-data-protection-human-resources-hr-perspective/ (last visited Apr. 27, 2017) (discussing the increased rights of employees, where these will be strongest in the EU).

115. Because the non-compliance yields a much different inquiry, further research should be done in short order to hypothesize the number of companies that will seek GDPR adoption globally.

116. GDPR, *supra* note 1, art. 2(2). The regulation does not specify EU citizens though and the European Commission has been clear to emphasize the belief expressed in the GDPR. GDPR, *supra* note 1, at pmbl. ¶ 1. *See also Protection of Personal Data, supra* note 8 ("Everyone has the right to the protection of personal data").

117. *See* Carol Umhoefer & Caroine Chancé, *The Applicability of EU Data Protection Laws to Non-EU Businesses*, DLA Piper: Privacy Matters L. Blog (Apr. 4, 2016), http://blogs.dlapiper.com/privacymatters/europe-the-applicability-of-eu-data-protection-laws-to-non-eu-businesses/.

consumers for privacy protections, cost of differential cybersecurity infrastructure, and market competition may also drive these companies to begin prospectively applying the standards in the GDPR where they are not legally required to.[118] As such, companies who want to have at least minimum compliance with GDPR will likely bucket GDPR compliance decisions into three categories. These categories will include: A) provisions they will only apply in the EU; B) provisions they will apply globally; and C) provisions they may apply regionally or are otherwise unsure of until enforcement actions are made.[119] Companies opting to make decisions under A) and B) are analyzed in turn below.

A. *Provisions Applicable only in the EU or on a Limited Regional Basis*

Companies are beginning to draw lines in the sand for provisions they feel are too burdensome to implement globally or that they feel may restrict another human right if implemented as required by the EU.[120] Just because the EU wishes to have certain protections does not mean other countries will share the same feelings; freedom of speech has at times come in direct conflict with some privacy protections, such as the "right to be forgotten."[121] Otherwise, if a company feels that the GDPR will disrupt its ability to earn revenue or do business and that consumers with different cultural feelings will not share the same concerns outside the EU, they will refuse to implement the changes globally.[122] Thus, companies are likely to resist a global compliance regime for GDPR provisions they believe are too burdensome, too expensive, or that are contrary to their own corporate visions of human rights

118. *See, e.g.*, Warwick Ashford, *European data protection law to give consumers more control*, COMPUTER WEEKLY (Mar. 6, 2017), http://www.computerweekly.com/news/450414345/European-data-protection-law-to-give-consumers-more-control/.

119. More research should be done to determine how companies are making these decisions, especially for provisions they will only provide regionally or await further enforcement actions from the DPAs first.

120. For an analysis of some GDPR provisions found to be frustrating for U.S. companies and privacy proponents, see Lindsay Rowntree, *An American Perspective: The Three Worst Things About the EU GDPR*, ExchangeWire, (July 7, 2016), https://www.exchangewire.com/blog/2016/07/07/an-american-perspective-the-three-worst-things-about-the-eu-gdpr/.

121. *See, e.g.*, 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, sec. V (2000), http://www2.law.ucla.edu/volokh/privacy.htm (comparing the protections of the First Amendment to informational privacy demands).

122. Sherri J. Deckelboim, *Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying the EU-U.S. Privacy Shield Framework and How the Framework will Impact Privacy Advocates, National Security, and Businesses*, 48 GEO. J. INT'L L. 263, 293 (2016), https://www.law.georgetown.edu/academics/law-journals/gjil/recent/upload/Deckelboim.PDF/.

protections. Some of these provisions are likely to include the age of consent, data portability, and the right to data erasure.[123]

Because the GDPR is so large in both its scope and the level of change it will bring to privacy protections around the world, there are dozens of provisions that require clarification.[124] Just to help interpret the law, the EC has written hundreds of recitals to accompany the eighty-eight-page law.[125] As such, organizations will continue to analyze whether the global application of a provision would be cost effective and within the corporate vision, but they will most likely only do this once they have confidence in how the EU is likely to enforce the provision.[126] Furthermore, certain provisions may be required to utilize the EU's adequacy findings and mechanisms available to only select countries; this may lead those companies to apply the restrictions only to the level required by the applicable laws in those countries.[127] Some of these provisions might include the breach notification provisions, right to object to processing, and consent agreements.[128]

---

123. The right to be forgotten is, perhaps, the most controversial privacy protection in to date, and while there is not sufficient time to elaborate on it in depth here the following may provide a brief, but helpful analysis. At points where the right to be forgotten may conflict with the right to free speech, the EU has held that it is a fundamental human right to have your information removed from any public place. Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131/. This concept has been distilled into regulatory language in GDPR Article 17, titled the "Right to erasure 'right to be forgotten'," and explains that data subjects have the right to request erasure of their data without "undue delay" from controllers or processors of the data subject's personally identifiable information. GDPR, *supra* note 1, art. 17. Furthermore, as one article has argued, this digital right is of such great importance because medical research has found that the ability for the human brain to forget is "as critically important to consciousness as the ability to recall." Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH 349, 352 (2015).

124. For a list of all recitals to the GDPR, see *Recitals*, INTERSOFT CONSULTING, https://gdpr-info.eu/recitals/ (last visited Apr. 27, 2017).

125. *Id.*

126. The ICO's political data inquiry in Cambridge Analytica and Facebook may be one example of this type of decision; however, with Brexit still pending, many companies will want to see the actions of other DPAs as well. *See* David Pegg & Alex Hern, *What Triggered the ICO's Political Data Inquiry?*, Guardian (July 10, 2018, 7:01 PM), https://www.theguardian.com/uk-news/2018/jul/11/what-triggered-the-icos-political-data-inquiry/.

127. *See generally* Deckelboim, *supra* note 122 (discussing the actions organizations may take in the wakes of the Privacy Shield Program's creation and installment of the GDPR).

128. Though beyond the scope of this paper, the new definition for consent is proving to be a hot button issue. The GDPR defines consent as a "freely given, specific, informed and unambiguous indication" in the form of a statement, or "clear affirmative action," and prescribes detailed conditions for its validity. GDPR, *supra* note 1, art. 4(8), 7. *See also* Alex van der Wolk & Sotirios Petrovas, *The EU General Data Protection Regulation: A Primer for International Business*,

B. *Likelihood of DPIA and DPO Provisions to be Implemented Globally*

Companies are likely to implement regulations in the GDPR globally where the provisions will provide opportunities for improved infrastructure for the company; where a policy creates an unrecoverable sunk cost when applied in the EU; or where the consumers or investors are beginning to demand the protections elsewhere.[129] Among this growing list of provisions, the requirements for data protection officers and data impact assessments stand as two of the most likely and most impactful provisions to be implemented globally by firms seeking GDPR compliance.[130]

1. Data Protection Impact Assessment Provision

The DPIA requires companies that act as controllers to think constructively – with the consumers' rights in mind – about the scope of how data is collected, retained, and utilized.[131] While this is technically only required for PII received from data subjects residing in the EU, many companies may find that applying the DPIA broadly throughout their entire business practice will not only act as a sign of good faith to the DPAs but also to their consumers worldwide.[132] The U.K. Modern Slavery Act[133] may prove a useful foil for just this kind of consumer demand for transparency, and though not a perfect correlation, The Charter of Fundamental Rights of the European Union emphasize

---

MORRISON FOERSTER PRIVACY & DATA SECURITY L. BLOG (Mar. 23, 2016), https://www.mofo.com/resources/publications/the-eu-general-data-protection-regulation-a-primer-for-international-business.html/ (providing an outside analysis of how this might be interpreted for firms).

129. *See generally* EU FINALIZES GENERAL DATA PROTECTION REGULATION: IMPLICATIONS FOR U.S. BUSINESSES, Wiley Rein: Privacy in Focus 4, 4-6 (Jan. 2016), https://www.wileyrein.com/media/newsletterissue/183_Privacy%20In%20Focus%20January%202016.pdf/.

130. *See, e.g.*, Rafael Garcia del Poyo, Samuel Martinez & Jon Lanz, *Europe's General Data Protection Regulation from a cyber security perspective*, FINANCIER WORLDWIDE (Sep. 2016), https://www.financierworldwide.com/europes-general-data-protection-regulation-from-a-cyber-security-perspective/#.WPuFw1PyvVo/ (providing an analysis of other provisions, including the more nuanced cybersecurity rules, also discussing the expectation for the GDPR to have a "considerable impact" on the global treatment of data use, protections, and security).

131. GDPR, *supra* note 1, art. 35(9) ("Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations").

132. Alessandro Mantelero, *Competitive Value of Data Protection: The Impact of Data Protection Regulation on Online Behavior*, 3 INT'L DATA PRIVACY L. 229, 229-30 (2013). *See also* Daniel Burrus, *The Privacy Revolt: The Growing Demand for Privacy-as-a-Service*, WIRED, https://www.wired.com/insights/2015/03/privacy-revolt-growing-demand-privacy-service/ (last visited Apr. 27, 2017).

133. Modern Slavery Act 2015, c. 30 (Eng.), http://www.legislation.gov.uk/ukpga/2015/30/pdfs/ukpga_20150030_en.pdf.

both human rights demands for greater supply chain and data transparency.[134] The U.K. Modern Slavery Act may also provide useful comparative analysis in the context of applying the U.N. Guiding Principles on Business and Human Rights to corporate impact assessments. This comparison may provide the best analysis to the hypothesis that companies seeking GDPR compliance are more likely than not to use the DPIA globally rather than simply constraining it to data subjects directly protected by the law.

a. Current Law Comparison: UK Modern Slavery Act

The Modern Slavery Act of 2015 was enacted in the United Kingdom in March 2015.[135] The law was passed to curtail global slavery, human trafficking, and labor exploitation.[136] While still relatively new, the law has spawned several statements of support from major businesses such as Unilever.[137] Section 54 of the law, entitled "Transparency in supply chains etc [sic]" requires all businesses that "suppl[y] goods or services"[138] in the United Kingdom above a certain size (currently £36 million in global revenue) to make clear statements regarding their supply chain and its policies to avoid subsidizing human trafficking or slavery.[139] Though somewhat untested, this disclosure process has been thought of by many organizations as an evolving process that will yield more transparency as more companies recognize the demand from

134. Charter of Fundamental Rights of the European Union art. 8(1), Dec. 7, 2000, O.J. (C 364) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?uriCELEX%3A32000X121 8%2801%29/ (last visited Apr. 13, 2016) (providing "that everyone has the right to the protection of personal data concerning him or her." GDPR, *supra* note 1, at pmbl. ¶ 1. *See also* Daniel Burrus, *supra* note 132.

135. *UK Modern Slavery Act*, Business and Human Rights resource center, https://business-humanrights.org/en/uk-modern-slavery-act/ (last visited Apr. 27, 2017).

136. Jason Haynes, *The Modern Slavery Act (2015): A Legislative Commentary*, 37 STATUTE L. REV. 33, 33-35 (2016).

137. *See, e.g.*, *UK Modern Slavery Act Transparency Statement*, UNILEVER (Jan. 2017), https://www.unilever.com/Images/unilever-slavery-and-human-trafficking-statement-2017_tcm244-498073_en.pdf ("We welcome the requirements of section 54 of the Modern Slavery Act and see the transparency it encourages as coherent with our support for the UN Guiding Principles on Business and Human Rights and their requirement to 'know and show' that we are working to respect human rights").

138. Modern Slavery Act 2015, c. 30 § 54 (Eng.), http://www.legislation.gov.uk/ukpga/2015/30/pdfs/ukpga_20150030_en.pdf.

139. For further analysis of the law, see Squire Patton Boggs, *The Modern Slavery Act: 10 Key Points for Businesses*, GLOBAL SUPPLY CHAIN L. BLOG, http://www.globalsupplychainlawblog.com/files/2015/09/20453-Modern-Slavery-Act-Alert.pdf/ (last visited Apr. 27, 2017).

consumers, investors, and governments to comply with enhanced supply-chain transparency.[140]

While not without critique, the law has been heralded as a first-of-its-kind law encouraging a new global standard of supply-chain transparency from a single consuming nation.[141] Though enforcement of the law is both ambiguous and somewhat non-threatening from the U.K. government, companies around the globe have been advised by major consulting and accounting firms to ensure they are in compliance with the law.[142] This is despite the absence of "criminal or financial penalties for non-compliance" in the law.[143] While it is possible that companies comply out of fear of naming and shaming by the U.K. government, it is equally likely that the law itself has begun to drive consumer behaviors and company compliance simply by starting the conversation in places it had gained traction before.[144] Thus, because the GDPR has had a long build-up period, includes fines and penalties, and will be enforced by specific supervisory authorities in twenty-eight member states, the quick responsiveness and compliance by many companies to the U.K. Modern Slavery Act should serve as a floor for the expected participation in the GDPR.[145]

---

140. *See, e.g.*, Michael R. Littenberg & Amanda N. Raad, *United Kingdom Publishes Modern Slavery Act Guidance: An Overview, Selected Next Steps and Takeaways*, ROPES & GRAY ALERTS (Oct. 30, 2015), https://www.ropesgray.com/~/media/Files/Mini-Sites/CSRSC/20151030_CSR_Alert.ashx.

141. Christine Beddoe & Vicky Brotherton, *Class Acts?: Examining Modern Slavery Legislation Across the UK*, THE Anti Trafficking Monitoring Group (Oct. 2016), http://www.antislavery.org/wp-content/uploads/2017/01/atmg_class_acts_report_web_final.pdf. *See also UK Modern Slavery Act*, BUSINESS AND HUMAN RIGHTS, *supra* note 134.

142. Patrick Shaw-Brown & Emily Coates, *The Modern Slavery Act: How should businesses respond?*, PwC, https://www.pwc.co.uk/assets/pdf/msa-updated-briefing-document.pdf (last visited Apr. 27, 2017).

143. Paul Callegari & Christine Braamskamp, *Modern Slavery Act 2015*, K&L GATES: LEGAL INSIGHT (Sept. 29, 2015), http://m.klgates.com/files/Publication/3e14e0c1-ee86-4a28-bb7e-4f80ad5567b6/Presentation/PublicationAttachment/ebde8770-e36f-4710-b61b-5f5b1470264a/Alert%20Modern%20Slavery%20Act%2022092015.pdf.

144. See, e.g., *Modern Slavery: How new regulation will impact consumer companies*, SCHRODERS, http://www.schroders.com/en/sysglobalassets/digital/insights/2016/pdfs/responsible-investment/modern-slavery/modern-slavery-90307.pdf for an analysis of the law's impact on consumer businesses.

145. Anna Jakobsen, *Modern Slavery Act 2015*, ERNST & YOUNG, http://www.ey.com/Publication/vwLUAssets/EY-Modern-Slavery-Act-2015-Call-for-transparency/$FILE/EY-Modern-Slavery-Act-2015-Call-for-transparency.pdf.

b. How Can Companies Use the UNGPs to Pivot Their Changes?

The DPIA poses an interesting opportunity for companies to apply the U.N. Guiding Principles on Business and Human Rights (UNGPs) by creating a clear reporting framework.[146] Intentional parallels can be drawn between the U.K. Modern Slavery Act's requirements and the UNGPs as many of the early responders to the UNGPs, including companies such as Unilever, Nestle, and H&M, were also non-coincidently early adopters of the required disclosures under the U.K. Modern Slavery Act.[147] The three main pillars of the UNGPs, namely "Protect, Respect, and Remedy," dovetail with many of the stated principles behind the disclosure requirements of the GDPR.[148] As just one example, the stakeholder engagement framework set forth in the UNGPs instructs companies that by explaining in an impact report how the company engages with stakeholders, the company can more fully develop and explain a process for taking "perspectives into account in its decisions and actions."[149] The GDPR echoes this by specifically calling on companies to "consult relevant stakeholders" as they formulate their code of conduct in relation to the DPIA.[150] The GDPR's nuance, however, is that companies are required to submit the DPIAs to their supervisory authority, which may use the DPIAs in further assessments of the companies and in responses to consumer complaints[151] This enforcement piece is likely to yield more honest and introspective DPIAs than might otherwise exist to simply drum up consumer respect by following the UNGPs, but it is unclear whether this will yield more consumer protections because there is no technical requirement to publish the

146. UN Human Rights Office of the High Commissioner, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

147. *Unilever releases first-of-its-kind Human Rights Report*, UNILEVER (June 30, 2015), https://www.unilever.com/news/press-releases/2015/Unilever-releases-first-of-its-kind-Human-Rights-Report.html. *See also* Dame Fiona Kendrick, *Modern Slavery and Human Trafficking Report 2016*, NESTLE (Sept. 2016), http://www.nestle.co.uk/asset-library/documents/39506_nestle_mod-slave-act_ab_30sep.pdf; *The H&M Group Modern Slavery Statement*, H&M (Jan. 30 2017), https://sustainability.hm.com/content/dam/hm/about/documents/masterlanguage/CSR/2017%20Sustainability%20report/HM_GROUP_Modern_Slavery_Statement_2017.pdf.

148. *Compare UN Guiding Principles: Reporting Framework with implementation guidance* (2015), http://www.ungpreporting.org/wp-content/uploads/2017/04/UNGPReportingFramework_withguidance2017.pdf, *with* GDPR, *supra* note 1, art. 35, 36.

149. *UN Guiding Principles: Reporting Framework*, *supra* note 147, at 59.

150. GDPR, *supra* note 1, at pmbl. ¶ 99.

151. EU Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 17, WP 248 (Apr. 4, 2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=44137/.

DPIAs publicly.[152] In short, companies that have previously applied the UNGPs to formulate their privacy policies will stand in a stronger position as they seek compliance with the GDPR. Furthermore, increasing pressure to adopt the UNGPs from consumers, investors, and DPOs will naturally encourage compliance.

2. Data Protection Officer

Because the Data Protection Officer role must be independent and report directly to the managing directors (frequently the board of directors), there is structurally very little reason for a company to confine the role only to the EU.[153] The role is odd, however, in that the DPO must be independent yet maintain a deep understanding of the structural and technical uses of PII in the company itself; because the DPO is insulated from C-Suite management, their role in conducting a privacy analysis is quite different from the internal audit process required by SOX.[154] The GDPR also provides an additional benefit beyond the UNGPs by mandating an internal chain of command for treatment of PII and providing an integrated compliance officer.[155,156] This built-in internal compliance officer will naturally be adopted globally by all companies seeking compliance with the GPDR both because the officer is an explicit requirement with direct ties to the board of directors, but also because, as the Sarbanes-Oxley Act compliance history shows, companies are encouraged by market forces to disclose

152. *Id.*

153. *See generally* GDPR, *supra* note 1, art. 37-38, for description of the roles and responsibilities of the data protection officer.

154. *Compare id., with* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 §§ 302, 404 (2002), https://www.sec.gov/about/laws/soa2002.pdf [hereinafter SOX]. *See also* The Institute of Internal Auditors, Internal Auditing's Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002 4-5 (2004), https://na.theiia.org/standards-guidance/Public%20Documents/Act%20Internal_Auditings_Role_in_Sections_302__404__FINAL.pdf.

155. See GDPR, *supra* note 1, art. 37-38, for a discussion about the encouragement for governments to require "non-financial" human rights statements be verified by "an independent assurance service provider." See also Richard Karmel, *Why due diligence and assurance of human rights performance are essential tools to protect people and companies – Part 2*, MAZARS BLOG (May 17, 2016), http://www.mazars-blog.co.uk/why-due-diligence-and-assurance-of-human-rights-performance-are-essential-tools-to-protect-people-and-companies-part-2/, for a discussion of how the UNGPs can assist companies to "know and show" the impacts of their business operations.

156. See GDPR, *supra* note 1, art. 37-38, for a discussion about the encouragement for governments to require "non-financial" human rights statements to be verified by "an independent assurance service provider." See also Karmel, *supra* note 155, for a discussion of how the UNGPs can assist companies to "know and show" the impacts of their business operations.

legal compliance through an independent audit source, a position easily filled by the DPO.[157]

a. Current Law Comparison: Sarbanes-Oxley Act

While different in scope and purpose, SOX is similar to the GDPR in that it has reporting requirements and, though not specified in as much detail as the GDPR, required significant compliance and structural changes that have firmly taken root.[158] Enacted in 2002, SOX was written for the purpose of protecting "investors by improving the accuracy and reliability of corporate disclosures."[159] SOX was developed in response to the financial scandals involving Enron, WorldCom, and Global Crossing as consumers and investors demanded better protections for whistleblowing and deeper fiscal accountability.[160] The law requires public companies to "establish a method" whereby employees anonymously report "possible financial improprieties."[161] SOX also requires those companies to develop a "company code of ethical conduct."[162] Though initially made to target U.S. financial scandals, the impact of the law has seeped throughout the globe, with the SEC now involved in "international relations."[163] One author has suggested that this is largely due to the impact of technological advances and globalization, both of which have led to SOX "repercussions around the world."[164] One survey found that compliance costs varied greatly depending on the type and size of a firm, but often range over $1

157. A helpful comparison between the two laws beyond the scope of this paper might also contemplate the evolution of responsibilities under SOX and recognize the shortfalls that occurred when compliance was put only before C-Suite executives and not the board of directors themselves. *See, e.g.*, Frederick E. Allen, *Sarbanes-Oxley 10 Years Later: Boards Are Still the Problem*, FORBES (July 29, 2012, 1:56 PM), https://www.forbes.com/sites/frederickallen/2012/07/29/sarbanes-oxley-10-years-later-boards-are-still-the-problem/#5aecd0292345/ (discussing general issues with SOXs boards).

158. *See, e.g.*, SOX, *supra* note 154, at §§ 302, 404.

159. *Id.*

160. *Sarbanes Oxley FAQ*, SARBANES OXLEY 101, http://www.sarbanes-oxley-101.com/sarbanes-oxley-faq.htm (last visited Apr. 27, 2017).

161. 2 Carole Basri, LexisNexis Corporate Compliance Practice Guide: The Next Generation of Compliance § 32.09 (Matthew Bender, ed. 2018).

162. *Id.*

163. Lawrence A. Cunningham, Professor of Law and Business, Boston College, Address to the Federation of European Securities Exchanges: Sarbanes-Oxley and All That: Impact Beyond America's Shores (June 12, 2003), http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1000&context=lslp/.

164. Paul Lanois, *Between a Rock and a Hard Place: The Sarbanes-Oxley Act and Its Global Impact*, 5 J. INT'L L. & POL'Y 4:1 (2007).

million per year.[165] These costs and other implications from an oversight law like SOX can provide helpful gauges for the GDPR and the impact having an internal auditor can bring. It should be anticipated that the DPO provisions in the GDPR will have a similar, if not greater, impact on internal compliance.

b. The Power of Internal Compliance

Perhaps the greatest corollary between the GDPR and SOX is simply the oversight of "an internal auditor."[166] While the DPOs and SOX internal auditors' functions are different, there has long been a consumer and investor demand[167] for internal audit controls whenever a law demanding compliance is enacted.[168] Mazars has explained that companies which are truly seeking to enforce human rights will utilize internal audits as a key tool to ensure their organization remains in compliance with the internal code of conduct and corresponding external framework.[169] This means that companies will be actively encouraged by investors and consumers to show that they are doing what they say they are doing.[170] Shift, a partner with Mazars in facilitating the UNGPs, has also suggested that a clear framework can provide helpful insight to these "internal auditor[s]."[171]

IV. Conclusion

While it is difficult to determine exactly what impacts the GDPR will have on privacy protections around the globe, the DPIA and DPO

165. *Understanding the Costs and Benefits of SOX Compliance*, Protiviti, https://www.protiviti.com/sites/default/files/united_states/insights/2016-sox-survey-protiviti.pdf (last visited Jan. 3, 2019).

166. *Compare* GDPR, *supra* note 1, art. 37, *with* SOX, *supra* note 154, at §301. *See also* Staying on Course: A guide for audit committees, Ernst & Young Center for Board Matters, http://www.ey.com/Publication/vwLUAssets/A_guide_for_audit_committees/$FILE/EY-Staying-on-course-guide-for-audit-committees.pdf (last visited Apr. 27, 2017).

167. *See, e.g.*, How Multinational Internet Companies assist Government Censorship in China, Human Rights Watch (Aug. 2006), https://www.hrw.org/reports/2006/china0806/5.htm (an example of consumer and civil society frustrations with corporate actions regarding censorship).

168. *See, e.g.*, *Yahoo Business & Human Rights Program*, Yahoo, https://yahoobhrp.tumblr.com/post/75507678786/human-rights-impact-assessments-yahoo-has/ (an example of a corporate response to consumer demands; Yahoo first formulated their BHRP in 2008 as a response to censorship concerns generated in the early 2000s).

169. Karmel, *supra* note 155.

170. *Id.*

171. *Human Rights Reporting and Assurance Frameworks Initiative*, Shift Project (Nov. 2012), http://www.shiftproject.org/resources/collaborations/human-rights-reporting-assurance-frameworks-initiative/.

provisions will set a floor for privacy protections for any consumer who deals with a company already seeking to abide by the regulations in the GDPR. As with the FCPA, it may take some time for the DPAs to adequately get up to speed on enforcement and for the market to accept the implications of the new regulatory framework. However, the comparatively fast adoption of the U.K. Modern Slavery Act seems to indicate that many companies are willing to quickly comply with disclosure and human rights protections for business reasons, as the law does not exact meaningful penalties outside of "naming and shaming." Under the GDPR, however, the law allows supervisory agencies to fine at levels that put SOX and FCPA fines to shame. Thus, while companies may elect differential levels of compliance under the GDPR, the floor for participation and enforceable protections will be much higher by comparison than prior extraterritorial laws that have changed how business is done globally in the past. Enforcement began in May 2018, but as the year progresses and as the GDPR becomes more of a mainstay, consumers all around the globe can begin to expect public disclosures and a more hands-on approach to privacy protections for many transnational corporations as the organizations' boards of directors begin to adopt an increasingly European-view on privacy protections for no other reason than self-preservation. Truly, the GDPR is changing how the game is played.

APPENDIX I

A. *Growth of the EU's Data Protection Authorities*

The DPD created an Article 29 working group on Data Protection Authorities, now commonly referred to as the Working Party 29 (WP29).[172] The goal under the DPD was to create an EU-wide structure of enforcement authorities that would get together each year and determine the next steps for enforcement of the data protection directive and subsequent laws, agreements, and regulations.[173] As the major EU body dealing with privacy matters, the WP29 has continued to be charged with interpreting much of the ambiguity in the GDPR.[174] Additionally, they continue to hold meetings to review practices and

172. Directive 95/46/EC, *supra* note 20, art. 29.

173. For expressions of goals by the EU Parliament and Council to curb invasion of privacy issues, see *id.* art. 30; Directive 97/66/EC, art. 14, 1998 O.J. (L 024) 1 (EC), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML/.

174. *See, e.g.*, *Guidelines on Data Protection Officers ('DPOs')*, *supra* note 64, at 15-16.

procedures, as well as to assist their member DPAs prepare for enforcement under the new law.[175]

DPA capacity has been an issue in years past, with many on the industry side arguing that they cannot participate in constructive discussions with DPAs due to a lack of resources.[176] Thus, one can only speculate as to whether the DPAs with their current resources will be able to enforce the massive new law. If Ireland is to be an example of how other governments may respond, it appears compliance enforcement will increase, and rather dramatically.

The Ireland DPA has become one of the most influential authorities, as Ireland finds itself home to Dublin's "Silicon Docks," where tech giants such as Google, Facebook, Twitter, LinkedIn, Amazon, Etsy, PayPal, Groupon, AirBnB, Uber, Siemens, HP, Intel, Dell, Microsoft, Symantec, and Apple, among many others, are headquartered.[177] In anticipation of the new regulations and enforcement powers they will have under the GDPR, Ireland has begun to ramp up funding and employment for their DPA, including a new headquarters in Dublin itself.[178] In 2014, the Irish DPA was being funded at €1.89 million per year; in order to more than double staff by "hiring 45 new people,"[179] that number was bumped up by more than ninety percent to €3.65 million for 2015.[180] Still feeling the pressure to add more resources, the budget was increased by another €1.2 million for 2016.[181] Other data protection authorities, such as the Information Commissioner's Office (ICO) have requested additional

175. *See, e.g.*, Article 29 Working Party, *Plenary Meetings*, EUR. UNION (Jan. 18, 2019), https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1309.

176. *DIGITALEUROPE's response to the European Commission's questionnaire on the General Data Protection Regulation*, DIGITAL EUROPE (Feb. 10, 2017), http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2353&language=en-US&PortalId=0&TabId=353/.

177. *Tech Companies in Ireland*, TECH LIFE IRELAND (Apr. 26, 2016), https://techlifeireland.com/tech-in-ireland/tech-companies-in-ireland/.

178. Michael McAleer, *Data Protection Commissioner gets €1.2m funding: Office at the centre of 'Safe Harbour' case now has a budget of over €4.7 million*, IRISH TIMES (Oct. 15, 2015, 4:19 PM), http://www.irishtimes.com/business/technology/data-protection-commissioner-gets-extra-1-2m-funding-1.2393311/.

179. *See* Elaine Edwards, *Data Protection Commissioner to recruit new staff: Regulator to 'immediately' begin hiring for new roles with 45 extra jobs to be created in total*, IRISH TIMES (Jan. 7, 2015, 4:53 PM), http://www.irishtimes.com/news/social-affairs/data-protection-commissioner-to-recruit-new-staff-1.2057948/.

180. Aine McMahon, *Data protection gets funding doubled: Office of the Data Protection Commissioner to receive €3.65m for 2015*, IRISH TIMES (Dec. 18, 2014, 8:04 PM), http://www.irishtimes.com/news/politics/data-protection-gets-funding-doubled-1.2043073/.

181. *Id.*

funding from their member states.[182] When compared with funding from IAPP surveys from 2009,[183] 2010,[184] and 2011,[185] one can only speculate the funding that will be available to many of the DPAs by May 2018.

B. *New Powers*

Out of all the new arrows added to the EU DPAs' quivers, Article 79 sets forth the most potent, powerful, and easily understood.[186] A Capgemini Consulting study of 300 managerial level executives at Consumer Product companies has estimated that these fines could reach up to $323 billion for just that industry.[187] Surely, as more CFOs become aware of the GDPR and the potential fines that may apply there will be more internal pressure to comply with the framework and meet DPA demands and recommendations.[188]

This power to enact immense new fines will surely encourage more compliance, but other tools will add carrots and sticks to the DPAs arsenal. These new powers include administrative fines, suspension of cross-border transfers, and authority to conduct expanded investigations.[189] The goal appears to have been to provide new powers and independence to enhance enforcement while maintaining national

182. *Statement on extra resources needed by the ICO under GDPR*, INFORMATION COMMISSIONER'S OFFICE (Mar. 13, 2017), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/03/statement-on-extra-resources-needed-by-the-ico-under-gdpr/ (requesting additional resources to deal with the "significant additional responsibilities"). *See generally* Newsroom Editor, *List of Competent Authorities*, EUR. UNION (Jan. 19, 2014) https://ec.europa.eu/digital-single-market/en/news/list-competent-authorities/ (a list of DPAs and the respective Commissioners).

183. J. Trevor Hughes, *Data Protection Authorities: 2009 Global Benchmarking Survey*, INT'L ASS'N OF PRIVACY PROFESSIONALS, https://iapp.org/media/pdf/knowledge_center/DPA_Survey.PDF (last visited Apr. 27, 2017).

184. J. Trevor Hughes, *Data Protection Authorities: 2010 Global Benchmarking Survey*, INT'L ASS'N OF PRIVACY PROFESSIONALS, https://iapp.org/media/pdf/knowledge_center/IAPP_DPA2010_GlobalBenchmarking_Survey.pdf (last visited Apr. 27, 2017).

185. J. Trevor Hughes, *Data Protection Authorities: 2011 Global Survey*, INT'L ASS'N OF PRIVACY PROFESSIONALS, https://iapp.org/media/pdf/knowledge_center/DPA11_Survey_final.pdf (last visited Apr. 27, 2017).

186. GDPR, *supra* note 1, art. 79.

187. CAPGEMENI CONSULTING, CONSUMER INSIGHTS: FINDING AND GUARDING THE TREASURE TROVE (2016), https://www.capgemini-consulting.com/resource-file-access/resource/pdf/consumer_insights_08072016_final.pdf/.

188. *See* Sean Duffy, *Almost 70pc of chief financial officers are unaware of new data protection laws*, Independent (Nov. 17, 2016, 9:33 am), http://www.independent.ie/business/almost-70pc-of-chief-financial-officers-are-unaware-of-new-data-protection-laws-35223014.html/ (finding only 28 percent of CFOs at Irish and other multinational companies were aware of GDPR).

189. GDPR, *supra* note 1, art. 53, 58.

sovereignty.[190] DPAs will also be integral to advising and enforcing each of the derogations the member state may make.[191]

Per Article 52, DPAs will also now shoulder the burden of many other tasks.[192] One firm has found these tasks to include at a minimum "monitoring compliance; promoting awareness; advising governments; providing information to individuals; handling complaints; cooperating with other authorities; conducting investigations; drafting standard contracts for data transfers; drawing up requirements for PIAs; encouraging private codes of conduct and certification mechanisms; and fulfilling any other tasks related to data protection."[193] Coupled with their new powers, these sections of the GDPR dovetail with Chapter VII of the GDPR, which focuses on cooperation and consistency between the various DPAs.[194]

C. *The "One Stop Shop" Supervisory Authority*

In order to bring more legal certainty, the GDPR sets forth the requirement for each "supervisory authority," or DPA, to "contribute to the consistent application" of the regulation.[195] The EC has explained that the "One Stop Shop" provision allows for greater clarity and understanding for organizations by creating a lead supervisory authority for controllers that are established in the EU.[196] By "helping companies identify"[197] a lead DPA, others have argued that this provision should have the benefit of bringing greater uniformity to DPA rulings.[198] Additionally, some have argued the goal was to restrict businesses to

190. GDPR, *supra* note 1, art. 52-58.

191. *See, e.g.*, UK's ICO's list of derogations https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/national-derogations/.

192. GDPR, *supra* note 1, art. 57. *See also id.* art. 52.

193. Alex van der Wolk & Sotirios Petrovas, *The EU General Data Protection Regulation: A Primer for International Business*, MORRISON FOERSTER PRIVACY & DATA SECURITY L. BLOG (Mar. 23, 2016), https://www.mofo.com/resources/publications/the-eu-general-data-protection-regulation-a-primer-for-international-business.html.

194. GDPR, *supra* note 1, at ch. VII.

195. *Id.* art. 51(2).

196. *Id.* at pmbl. ¶¶ 127-128.

197. EU Article 29 Working Party, *Guidelines for identifying a controller or processor's lead supervisory authority*, at 11, WP 244 (Dec. 13, 2016), http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf.

198. Phil Bradley-Schmieg, *New EU GDPR Guidance: Data Portability, Data Protection Officers, and the One Stop Shop*, INSIDE PRIVACY L. BLOG (Dec. 16, 2016), https://www.insideprivacy.com/international/european-union/new-eu-gdpr-guidance-data-portability-data-protection-officers-and-the-one-stop-shop/. *See also* Dariusz Kloza & Anna Moscibroda, *Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law*, 4 INT. DATA

interact with a single DPA who could become familiar with their practices to improve enforcement and reduce forum shopping.[199] However, while Article 56 spells out that the supervisory authority is the "country where the main establishment of the organization is based," there are many other controlling criteria.[200] Controllers and Processors who are under investigation by a DPA may be forced to defend their practices where "the individual has his or her habitual residence," even if it is not the where that company is headquartered in the EU.[201] Otherwise, Article 79 also describes that the controller or processor "shall be brought before the courts of the Member State" in which the business "has an establishment."[202]

Furthermore, the lead supervisory authority mechanism is only triggered in the context of cross-border processing, defined under GDPR Article 4(23) as the "processing of personal data" either by activities of "establishments in more than one Member State" or of a single establishment but that "substantially affects or is likely to substantially affect" individuals in multiple member states.[203] While there are other criteria, the long and short of it is that there will still be a reasonable amount of uncertainty for many companies, especially those not well established throughout the EU.[204]

PRIVACY L. 120, 120 (May 1, 2014) (arguing for enhanced enforcement cooperation to gain much of the effectiveness experienced with competition law orders throughout the EU).

199. Maclean & Docherty, *supra* note 58.

200. GDPR, *supra* note 1, art. 56.

201. GDPR, *supra* note 1, art. 79(2).

202. *Id.*

203. EU ARTICLE 29 WORKING PARTY, ANNEX II: FREQUENTLY ASKED QUESTIONS, WP 244 (Dec. 13, 2016), http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_annexii_en_40858.pdf.

204. *See* Centre for Information Policy Leadership, *The One-Stop-Shop and the Lead DPA as Co-operation Mechanisms in the GDPR*, at 5-8 (Nov. 2016), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_the_gdpr_one-stop-shop_30_november_2016.
pdf (recommending further clarifications and implementation changes to the WP29 regarding the one-stop shop provisions).