Journal of Business & Technology Law

Volume 15 | Issue 1 Article 6

The General Data Protection Regulation: American Compliance Overview and the Future of the American Business

Cymone Gosnell

The General Data Protection Regulation: American Compliance Overview and the Future of the American Business

CYMONE GOSNELL*©

ABSTRACT

In 2016, the European Union ("EU") created heightened data privacy rights for its citizens by enacting the General Data Privacy Regulation ("GDPR"). The most drastic change from the previous regulation, enacted in 1995, lies within the expanded territorial scope. The change now subjects companies to fines for violations of the regulation, even if those companies are not domiciled in the EU. Data privacy has always been considered a fundamental human right in the EU; however, within the United States, there is no fundamental right to privacy. Rather, the country's privacy laws are based on a complicated sectoral structure that often leads the country's citizens confused as to what rights they actually have. This paper will review the EU and United States' fundamental differences in privacy laws, the changes implemented by the GDPR (including the expanded territorial scope), the compliance plans of some major players within the United States, and what the future looks like for American businesses that hold or process the data of EU citizens under the GDPR.

INTRODUCTION

Within the United States, buying, selling, and trading citizens' personal data has become normalized.[1] Companies use social media[2] and every day personal devices[3] to collect basic data including e-mail addresses and birthdays.[4] Those same businesses also use technology to collect intimate data such as work and residential addresses[5] and the blueprints of individual homes.[6] In conjunction with some recent privacy scandals,[7] Americans have taken an increased interest in protecting their personal data privacy rights.[8]

Many US citizens did not view privacy as a concern until Edward Snowden, who worked for the National Security Agency ("NSA"),[9] released documents exposing how United States government agencies used extreme data collection techniques to collect information about innocent American citizens under the guise of the Foreign Intelligence Surveillance Act of 1978.[10] Many Americans fail to realize the

* The author is a J.D. Candidate, 2020, University of Maryland Francis King Carey School of Law. I would like to thank the editors and staff on the *Journal of Business and Technology Law*, specifically Kevin Redden, Samuel Schwartz, Samuel Kava, and Taylor Nichols for their insightful feedback and suggestions throughout the writing process. I would also like to thank Professor Markus Rauschecker for his time and his invaluable feedback. Finally, I would like to thank my mother, Yvette Bryant, my grandparents, Marvin and Emma Bryant, and the rest of my family for all of their support, encouragement, and love.

1. *See* Kalev Leetaru, *Social Media Companies Collect So Much Data Even They Can't Remember All the Ways They Surveil Us*, FORBES (Oct. 25, 2018, 12:54 PM), https://www.forbes.com/sites/kalevleetaru/2018/10/25/social-media-companies-collect-so-much-data-even-they-cant-remember-all-the-ways-they-surveil-us/#631abfc77d0b.

2. *Id*.

3. *See* Kelsey Sutton, *Google Is Collecting Your Data—Even When Your Phone Isn't in Use*, ADWEEK (Aug. 21, 2018), https://www.adweek.com/digital/google-is-collecting-your-data-even-when-your-phone-isnt-in-use/.

4. For example, when creating a Facebook account, a person must enter a name, email address and date of birth.

5. *See* Bernard Marr, *21 Scary Things Big Data Knows About You*, FORBES (Mar. 8, 2018, 2:23AM), https://www.forbes.com/sites/bernardmarr/2016/03/08/21-scary-things-big-data-knows-about-you/#19ee52f56e7d.

6. *See* Allen St. John, *How to Keep a Roomba Vacuum Cleaner from Collecting Data About Your Home*, CONSUMERREPORTS (July 31, 2017), *https*://www.consumerreports.org/roomba/how-to-keep-a-roomba-vacuum-cleaner-from-collecting-data-about-your-home/.

7. *See* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

8. *See* Derek Hawkins, *The Cyber Security 202: Why A Privacy Law Like the GDPR Would be a Tough Sell in the U.S.*, THE WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/?utm_term=.91aaf85a1800.

9. FREE SNOWDEN, https://edwardsnowden.com (last visited Sep. 30, 2019).

10. Emily Berman, *The Two Faces of the Foreign Intelligence Surveillance Court*, 91 IND. L.J. 1191, 1192 (2016).

constitutional protection of privacy controlling government conduct does not extend to private corporations.[11] Rather, private companies are governed by sectoral laws.[12] Within the United States, citizens have rationalized companies systematically ignoring privacy rights and argue that Americans would not be interested in new data privacy regulation.[13] However, citizens should understand that data collected by companies can be "used to intimidate your family," or even "cheat you out of your hard-earned money."[14] The invasion of privacy United States citizens face has not been globally normalized. In fact, within the European Union privacy protections against both companies and governments are considered a fundamental right.[15]

Compared to the United States, the European Union ("EU") has consistently employed fairly rigid privacy protection regulations to protect its citizens' data.[16] In 1995, the EU began regulating businesses under the Data Protection Directive ("1995 Directive"),[17] which increased regulations relating to data collection and processing.[18] These regulations led to the creation of the General Data Protection Regulation ("GDPR"), the most stringent of the EU's privacy regulations.[19] The EU approved the regulation on April 14, 2016, but the GDPR did not become applicable until May 25, 2018, more than two years later.[20] The GDPR implements several changes to general privacy rights, which will be discussed in detail below. One of the biggest changes by far, and one of the biggest challenges for American companies, is the expanded territorial scope of the rule.[21] If American businesses wish to continue operating within the EU, without being subjected to heavy penalties, those businesses must update their procedures to fully comply with the

11. *See* Christopher Dunn, *Applying the Constitution to Private Actors,* NYCLU, ACLU OF N.Y. (Apr. 28, 2009), https://www.nyclu.org/en/publications/column-applying-constitution-private-actors-new-york-law-journal.

12. *See infra* notes 31-34 and accompanying text.

13. *See* Derek Hawkins, *The Cyber Security 202: Why A Privacy Law Like the GDPR Would be a Tough Sell in the U.S.*, THE WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/?utm_term=.91aaf85a1800.

14. Troy Hatfield, *The Great Divide: Recent Trends Could Help Bridge the Us/EU Data Privacy Gap*, 14 SEATTLE J. FOR SCO. JUST. 269, 269 (2015).

15. *See infra* text accompanying notes 49-50.

16. *See* Kimberly A. Houser & Gregory Voss, *Can Facebook and Google Survive the GDPR*, U. OF OXFORD FAC. OF L. BLOG (Aug. 29, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/08/can-facebook-and-google-survive-gdpr.

17. Marc Rotenberg & David Jacobs*, Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 617 (2013).

18. *Id.* at 623–30.

19. Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or A New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 3, 58 (2018).

20. *Id.*

21. *See* Sarah Jeong, *No One's Ready for GDPR*, THE VERGE (May 22, 2018, 3:28 PM), https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu.

newly enacted GDPR.[22] Although the regulation has already been implemented, many businesses, both in the United States and the EU, remain out of compliance and unsure of the necessary steps they need to take to come into compliance.[23]

Major companies such as Facebook and Microsoft have already implemented procedures to ensure some compliance with the GDPR,[24] whereas other companies, like Apple, are still assessing their products and services to ensure they are in full compliance.[25] Companies in compliance have adopted one of two popular approaches to ensure compliance: (1) providing different rights to individuals depending upon their location; or (2) affording the same heightened GDPR privacy rights to all users globally.[26] There are concerns that smaller companies may have difficulty complying with the regulation due to a lack of monetary and personnel resources.[27] However, the real question is how, and to what extent, large and small businesses in the United States will be impacted by the GDPR.

Section I of this paper examines data privacy regulation within the United States and compares it to the data privacy regulation within the European Union. Section II reviews the major changes implemented by the General Data Protective Regulation. Section III examines the steps large American businesses have taken to come into compliance with the GDPR, and some initial steps taken by smaller American companies. Section IV examines whether the regulation requires too much of companies outside of the European Union, specifically American businesses, and whether American businesses will actually be able to adapt, on a wide-scale basis, to these new regulations. Finally, Section V provides a review and conclusion of this paper.

II. DATA PRIVACY IN THE UNITED STATES AND DATA PRIVACY REGULATION IN THE EU

A. Data Privacy in the United States

The United States "prioritiz[es]…security over privacy,"[28] and the government has clearly established that, "personal privacy may be infringed upon if it means that

22. Houser & Voss, *supra* note 19, at 96.

23. *See* Jeong, *supra* note 21.

24. *See* Matt Burgess, *How Apple, Facebook and Google are Changing to Comply with GDPR*, WIRED (May 24, 2018), https://www.wired.co.uk/article/gdpr-facebook-google-analytics-apple-amazon-twitter.

25. APPLE, https://www.apple.com/legal/privacy/en-ww/governance/ (last visited Sep. 28, 2019). Currently, the company's privacy policy reads as follows "[a]s part of our EU General Data Protection Regulation (GDPR) work, we are undertaking Privacy Impact Assessments (PIA) of our major products and services and integrating PIAs as we develop new products and services." *Id.*

26. *See* Burgess, *supra* note 24.

27. *See* FORBES TECHNOLOGY COUNCIL, *15 Unexpected Consequences of GDPR,* FORBES (Aug. 15, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#4e7dd15a94ad.

28. Hatfield, *supra* note 14, at 270.

citizens are safe from threats, such as terrorism."[29] The government enforced and expanded upon this concept after September 11, 2001, ("9/11"), in the name of increasing national security.[30] Americans' lack of privacy rights in the name of public safety begs the question as to what concrete rights to privacy American citizens enjoy with respect to data privacy when it comes to private companies collecting data from its users.

Before examining the privacy laws available to United States citizens, it is important to first examine the structure of the laws. The United States uses "sectoral" laws,[31] "meaning only certain types of data, such as medical and financial data, are protected but only to the extent provided in the applicable statute."[32] Two well-known examples of sectoral rights are the Health Insurance Portability and Accountability Act ("HIPAA")[33] and the Family Educational Rights and Privacy Act ("FERPA").[34]

Through examination of the above statutes and their attendant regulations, it may appear as though the United States has a comprehensive privacy regulatory scheme; however, the American privacy regulatory scheme has been negatively impacted by both the Foreign Intelligence Surveillance Act ("FISA") and the National Security Letters ("NSLs").[35] FISA is designed to permit electronic surveillance in order to garner foreign intelligence information.[36] NSLs "are administrative subpoenas issued by the Federal Bureau of Investigation ("FBI")…'to protect against international terrorism or clandestine intelligence activities.'"[37] The NSL "works as

29. *Id.* at 271.

30. *Id.* at 288–89.

31. *Id*. at 286. Sector is defined as "a sociological, economic, or political subdivision of society between the public and private sectors" MERRIAM WEBSTER'S DICTIONARY, https://www.merriam-webster.com/dictionary/sector (last visited Oct. 2, 2019).

32. *See* Kimberly A. Houser & Gregory Voss, *Can Facebook and Google Survive the GDPR*, U. OF OXFORD FAC. OF L. BLOG (Aug. 29, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/08/can-facebook-and-google-survive-gdpr.

33. Hartfield, *supra* note 14, at 286. "A major goal of [HIPAA] is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing." U.S. DEP'T OF HEALTH & HUMAN SERV., OFFICE OF CIVIL RIGHTS, SUMMARY OF THE HIPAA PRIVACY RULE (2003).

34. "The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). FERPA is codified at 20 U.S.C. § 1232g and the FERPA regulations are found at 34 CFR Part 99." U.S. Department of Education, https://studentprivacy.ed.gov/faq/what-ferpa (last visited Oct. 2, 2019).

35. Hartfield, *supra* note 14, at 287.

36. U.S. DEPARTMENT OF JUSTICE, https://it.ojp.gov/privacyliberty/authorities/statutes/1286 (last visited Oct. 2, 2019).

37. Hartfield, *supra* note 14, at 287.

a sort of exception to United States data protection and, like FISA, allows broader access to otherwise protected information."[38]

While the laws above are theoretically designed to protect Americans from potential foreign threats, the NSA and the FBI have managed to commandeer private information from telephone companies about American citizens.[39] For example, in April 2013, by top secret order, the FBI required Verizon to produce an electronic copy of all call detail records between United States citizens and citizens of a foreign country, as well as calls that occurred entirely within the United States.[40] After learning of the directive, the American Civil Liberties Union ("ACLU") discovered that the order belonged to a larger program initiated by the government almost a decade earlier.[41] In October 2016, the ACLU filed a motion requesting the Foreign Intelligence Surveillance Court release any opinion with "'novel or significant interpretations' of law, issued between 9/11 and the passage of the USA Freedom Act in June 2015."[42]

As indicated by Snowden, under the guise of these regulations and several NSA programs, the American government collaborated with tech giants like Microsoft, Apple, and Facebook to collect data for government analysis.[43] Where, as is the case in the United States, the government uses private corporations to monitor citizens, it is difficult to understand individual privacy rights regarding the data stored by companies.[44] The majority of Americans believe personal data collection violates their individual liberties;[45] however, sectoral laws make it difficult for Americans to understand the rights to which they are entitled.[46] The sectoral law structure means individual rights vary based upon the specific act or regulation at issue

38. *Id*.

39. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (Jun. 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

40. *Id*.

41. *ALCU Motions Requesting Public Access to FISA Court Rulings on Government Surveillance*, ACLU (Feb. 26, 2018), https://www.aclu.org/cases/aclu-motions-requesting-public-access-fisa-court-rulings-government-surveillance.

42. *Id*. The ACLU believes the orders contain information about many surveillance activities including warrantless searches under the FISA, mass searches of emails within Yahoo! Accounts, as well as the use of phone tracking devices. *Id*.

43. FREE SNOWDEN, https://edwardsnowden.com/surveillance-programs/ (last visited Oct. 2, 2019).

44. *See* Lauren Cassani Davis, *How Do Americans Weigh Privacy Versus National Security?*, THE ATLANTIC (Feb. 3, 2016), https://www.theatlantic.com/technology/archive/2016/02/heartland-monitor-privacy-security/459657/.

45. *Id.* This article indicates that in 2016, 53% of Americans believed "the collection and use of their data by businesses, law enforcement, individuals and other groups violated their personal privacy, safety, financial security, and individual liberties." *Id*.

46. *See* Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACH PRIVACY BLOG (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/.

because the Constitution grants no express right of privacy.[47] As a result of the complex legal structure surrounding privacy, many individuals within the United States have no way of knowing whether or not their privacy rights have been violated, and if so, whether or not they are entitled to a remedy against a business or a government agency.[48]

B. Data Privacy within the European Union

Whereas the United States is willing to sacrifice its citizens' privacy in the name of national security, "the EU considers personal privacy to be a fundamental right," and its citizens have an "absolute right" to privacy.[49] Rather than using sectoral-based privacy regulations, the EU utilizes an "omnibus" regulatory scheme for privacy rights, meaning "no sector (or type of data) is left unprotected because all data is treated the same, regardless of what it is used for or what it contains."[50]

Before the GDPR, the 1995 Data Directive served as the basis for all member states' local privacy laws.[51] The 1995 Directive "create[d] a legal framework that govern[ed] movement of personal data across national borders within the EU and [set] a baseline for the required security to be provided for the storage, transmission, and processing of personal information."[52] The regulation broadly defined both "processing" and "personal data" to ensure the protection of the EU citizens' fundamental right to privacy.[53] The minimum requirement for member states, discussed above, required the states to ensure data processors only collected data for "legitimate purposes" and that the processors keep data in a form that allows for identification "no longer than is necessary."[54] Under the 1995 Directive, citizens had the right to access their data being processed, as well as the right to dispute whether or not the data being collected was of public interest, or another "legitimate interest."[55]

However, the 1995 Directive had notable shortcomings that prompted the EU to strengthen its data privacy regulations.[56] First, the 1995 Directive did not "have binding legal force throughout every EU member state," and was not "directly

47. Ryan Moshell, *…And Then There Was One: The Outlook for A Self-Regulatory United States*, 37 TEX. TECH. L. REV. 357, 373 (2005).

48. *See* Solove, *supra* note 46.

49. Hatfield, *supra* note 14, at 271.

50. *Id.*

51. Houser & Voss, *supra* note 19, at 58.

52. Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 617 (2013).

53. *Id.* at 617. The regulation defined "personal data as "any information relating to an identified or identifiable natural person," and defined processing as "any operation or set of operations which is performed upon personal data." *Id.*

54. *Id.* at 618.

55. *Id.* at 618–19.

56. *Id.* at 623–630.

applicable in every member state."[57] Additionally, the EU enacted the 1995 Directive before the rise of globalization and the internet.[58] Ultimately, "such drastic changes in technology…presented significant new challenges…[which] the original Directive [was] not well equipped to handle."[59] For these reasons, the EU adopted the GDPR.[60]

The GDPR attempts to rectify the shortcomings of the 1995 Directive.[61] The GDPR is a comprehensive regulation designed "to protect all EU citizens from privacy and data breaches in today's data-driven world."[62] The GDPR "standardizes data protection law across all 28 EU countries and imposes strict new rules on controlling and processing personally identifiable information ("PII")."[63] The GDPR augments the 1995 Directive by expanding the jurisdictional reach of the regulation, significantly increasing the penalties for companies that violate the regulation, granting greater consent requirements, granting access and erasure rights to citizens, creating breach notification requirements, and requiring companies to use compliance tools.[64] The section below explores the major differences implemented by the GDPR, and what those differences actually mean in regards to data collection, data processing, and data privacy.

III. ENHANCED PRIVACY RIGHTS UNDER THE GDPR

A. Territorial Scope

Territorial scope refers to the enforceability of the regulation within and outside of member states.[65] The 1995 Directive provided little clarity in regards to the territorial applicability of the regulation.[66] The GDPR has added clarity by drafting the regulation to apply to data processing of any EU citizen, "*regardless of whether the processing takes place in the Union or not.*"[67] In other words, if an entity

57. Houser & Voss, *supra* note 19, at 59.

58. Rotenberg & Jacobs, *supra* note 52, at 630.

59. *Id.*

60. *Id.* at 630–631.

61. *Id.*

62. EU GDPR.ORG, https://eugdpr.org/the-regulation/ (last visited Oct. 3, 2019).

63. *See* Kris Lahiri, *What is General Data Protection Regulation?*, FORBES (Feb. 14, 2018, 1:21 PM), https://www.forbes.com/sites/quora/2018/02/14/what-is-general-data-protection-regulation/#6be71c8062dd.

64. EU GDPR.org, https://eugdpr.org/the-regulation/ (last visited Oct. 3, 2019).

65. *See* Council Directive 2016/679, art. 3, 2016 O.J. (L 119) 32–33 (EU) [hereinafter GDPR].

66. Houser & Voss, *supra* note 19, at 64.

67. GDPR EU, https://www.gdpreu.org/the-regulation/who-must-comply/ (last visited Oct. 7, 2019).

controls[68] or processes[69] the data of an EU citizen, the entity will be subject to the GDPR.[70] The European Union regards this increased jurisdictional reach as the biggest change to the regulatory landscape of data privacy.[71]

The regulation extends to companies outside of the EU that *control* or *process* any data of EU citizens.[72] Specifically, if the control or processing of data is related to the "offering of goods or services," even if a payment is not required, or if the control or processing is related to "the monitoring of…behaviour" taking place in the EU, a controller or processor outside of the EU is bound by the regulation.[73] As a result of the enhanced territorial reach, American businesses that control or process the data of EU citizens must comply with the regulation.[74]

B. Consent

The GDPR contains enhanced consent requirements for data processing.[75] Gaining an individual's express consent is only one of the six ways a company may process data under the GDPR, but the requirements surrounding consent are stringent.[76] Specifically, consent must be "freely given, specific, informed and unambiguous."[77] To ensure processors comply with these requirements, processors cannot "use long illegible terms and conditions full of legalese," especially when obtaining consent to collect information.[78] Furthermore, "the request for consent must be given in an intelligible and easily accessible form."[79] The act further articulates there is a presumption against the idea that consent has been freely given if there is not

68. *Id.* Article 4 of the GDPR defines controller as "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…" GDPR *supra* note 65, at art. 4.

69. Article 4 of the GDPR defines a processor as an entity that "processes personal data on behalf of the controller." GDPR *supra* note 65, at art. 4.

70. GDPR EU, https://www.gdpreu.org/the-regulation/who-must-comply/ (last visited Oct. 7, 2019).

71. EU GDPR.org, https://eugdpr.org/the-regulation/ (last visited Oct. 7, 2019) (emphasis added).

72. Gregory W. Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation*, 72 BUS. LAW 221, 222–23 (2016).

73. GDPR *supra* note 65, at art. 3. Processing under the regulation includes, but is not limited to, "'collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Gregory W. Voss, *supra* note 72, at 222. The bill does not define "controlling," but again, defines controller as "the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data." GDPR *supra* note 65, at art. 4.

74. GDPR *supra* note 65, at art. 4.

75. Intersoft Consulting, https://gdpr-info.eu/issues/consent (last visited Oct. 7, 2019).

76. *Id.* The other five bases for processing data are legal, which include contracting, legal obligations, vital interests of the data subject, public interest and legitimate interest. *Id.*

77. *Id.*

78. EU GDPR.org, https://eugdpr.org/the-regulation/ (last visited Oct. 7, 2019).

79. *Id.*

explicit consent given for different personal data processing operations.[80] To have informed and specific consent, the data subject must know various facts about the process, including the identity of the entity that will control the data, what specific data will be processed, and the purpose of processing the data.[81] The EU is explicitly concerned about a power imbalance between large companies with vast amounts of personal, private data, and the essentially powerless citizens of the EU.[82]

C. Increased Data Rights for Citizens

In addition to the increased territorial scope and heightened consent requirements, the GDPR gives EU citizens additional rights to control and access their data.[83] Five specific rights are highlighted by the GDPR website, including: breach notification, right to access, right to be forgotten, data portability, and privacy by design.[84]

The first increased privacy right, *Breach Notification*, compels a company to notify individuals when there has been a data breach.[85] A company that experiences a data breach must "without undue delay, and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority… unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."[86] This requirement may be harder on some companies, especially smaller companies, that control vast amounts of data.[87] The breach notification delivered to users must contain the following: (1) a description of "the nature of the personal data breach including…the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned"; (2) the name and contact information of someone with additional information about the data breach; (3) an explanation of "the likely consequences" of the breach; and (4) details about the actions the controller has taken, and will take to mitigate and rectify the breach.[88]

The next right, involves the data subject's *Right to Access*.[89] Under the GDPR, EU citizens have the right "to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for

80. GDPR *supra* note 65.

81. Intersoft Consulting, https://gdpr-info.eu/issues/consent (last visited Oct. 7, 2019).

82. GDPR *supra* note 65.

83. EU GDPR.ORG, https://eugdpr.org/the-regulation/ (last visited Oct. 7, 2019).

84. *Id.*

85. *Id*.

86. GDPR *supra* note 65, at art. 33.

87. *See* Kristy Westgard & Stephanie Bondoni, *GDPR, or Why Privacy Is Now Stronger in EU than U.S.*, BLOOMBERG (May 24, 2018, 6:00 PM), https://www.bloomberg.com/news/articles/2018-05-24/gdpr-or-why-privacy-is-now-stronger-in-eu-than-u-s-quicktake.

88. GDPR *supra* note 65, at art. 33.

89. EU GDPR.org, https://eugdpr.org/the-regulation/ (last visited Oct. 7, 2019).

what purpose."[90] Under Article 15 of the GDPR, a citizen who discovers her data is being processed is entitled to learn information such as the categories of data being collected and the recipient(s) of the data.[91] If an EU citizen requests the information from a corporation, the corporation must provide a copy, free of charge, but may charge a reasonable administrative fee for additional copies.[92]

The GDPR next confers the *Right to be Forgotten*.[93] This right has come to be known as the right to "Data Erasure," and "entitles the data subject to have the data controller erase his/her personal data, and cease further dissemination of the data, and to potentially have third parties halt processing of the data."[94] Additionally, the controller of the data may be required to delete a citizen's data for many reasons, including loss of data relevancy or misuse of data.[95] The controller may also be required to delete a user's data if the citizen withdraws consent or objects to his data being processed.[96] Finally, if the data was unlawfully processed, the data controller must delete it.[97] The EU's goal is to have withdrawal be just "as easy as giving consent."[98]

Data Portability is the fourth increased privacy right within the GDPR.[99] Data portability allows an EU data subject to access and transfer data he previously provided in a common digital format.[100] Article 20 of the GDPR dictates data subjects have the right to have their data transferred "where technically feasible," and that rights defined by the right to data portability are not in conflict with "the rights and freedoms of others."[101] The Information Commissioner's Office ("ICO")[102]

---

90. *Id.*

91. Council Directive 95/46, art. 15 2018 (L 119) (EC). In full, the citizen is entitled to know the following: the purpose of the processing; the categories data being processed; the recipient(s) of the data (especially concerning third-countries or international organizations); an idea of how long their data is being stored or how the company determines how long to store the data; and how to file a complaint with a supervisory authority. *Id.* All additional requirements can be found under Article 15.

92. Intersoft Consulting, https://gdpr-info.eu/issues/right-of-access/ (last visited Oct. 7, 2019).

93. EU GDPR.org, https://eugdpr.org/the-regulation/ (last visited Oct. 7, 2019).

94. *Id.*

95. GDPR *supra* note 65, at art. 17.

96. *Id.* There are some instances in which processing is necessary, including: "for exercising the right of freedom of expression;…for compliance with a legal obligation…; …for reasons of public interest in the area of public health…" and "for the establishment, exercise or defense of legal claims." *Id.*

97. GDPR *supra* note 65, at art. 17.

98. Intersoft Consulting, https://gdpr-info.eu/issues/consent (last visited Oct. 7, 2019).

99. EU GDPR.ORG, https://eugdpr.org/the-regulation/ (last visited Oct. 7, 2019).

100. *Id.* In other words, "data portability is the right to transfer personal data from one organization (controller) to another organization or to the data subject in the context of digital personal data…and automated processing." i-Scoop, *Data Portability Under the GDPR: The Right to Data Portability Explained,* https://www.i-scoop.eu/gdpr/right-to-data-portability/.

101. GDPR *supra* note 65, at art. 20.

102. The ICO defines itself as "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals." INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk (last visited Oct. 8, 2019).

suggests the purpose of data portability, other than allowing data subjects to control their own data, is financial.[103] Specifically, data portability lets citizens transfer their data to services that help them find discounts or allow them to track their spending habits.[104]

The final increased privacy right the GDPR affords is the concept of *Privacy by Design*, which requires creating technology designed for data privacy.[105] Privacy by design only requires "'data protection through technology design.'"[106] According to the legislature, companies are not required to undertake any predefined or exact effort to comply with privacy by design, but, rather, companies should act proactively to integrate technology that keeps their data subjects' data safe.[107] The regulation omits guidance on minimum required technology. Instead, companies are permitted to decide what type of "protective measures" they wish to implement.[108] To date, confusion exists regarding implementation of the regulation as a result of the government's implementation of flexible standards.[109]

D. Penalties

The sections above address rights guaranteed to EU citizens, and the rights American businesses must now observe and protect, if they operate or collect data within the EU. This section, on the other hand, discusses the consequences of violating the GDPR. The GDPR imposes a significantly higher maximum penalty than the 1995 Directive.[110] For example, under the 1995 Directive, a company valued at €500 billion could only be fined a maximum of €150,000.[111] However, violations of the GDPR could cost larger American businesses unprecedented amounts of money in fines.[112]

Under the GDPR, there are two categories of administrative fines, i.e., "lower level" and "upper level."[113] The "lower level" fines can total "up to €10 million,"[114]

103. INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ (last visited Oct. 8, 2019).

104. *Id.*

105. EU GDPR.ORG, https://eugdpr.org/the-regulation/ (last visited Oct. 7, 2019).

106. INTERSOFT CONSULTING, https://gdpr-info.eu/issues/privacy-by-design/ (last visited Oct 8, 2019).

107. *Id.*

108. *Id.*

109. *Id.*

110. Houser and Voss, *supra* note 19, at 60.

111. Kimberly A. Houser & Gregory Voss, *Can Facebook and Google Survive the GDPR*, U. OF OXFORD FAC. OF L. BLOG (Aug. 29, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/08/can-facebook-and-google-survive-gdpr.

112. *Id.*

113. GDPR EU, https://www.gdpreu.org/compliance/fines-and-penalties/ (last visited Oct. 9, 2019).

114. *Id.*

(approximately $11,309,530)[115] "or 2% of the worldwide revenue of the prior financial year…."[116] These fines are issued for less severe violations of the regulation.[117] "Upper level" fines, on the other hand, can cost companies up to €20 million[118] (approximately $22,674,320).[119] Rather than issuing a flat €20 million fee, the data protection authorities ("DPAs") could also fine a company, "up to 4% of the total worldwide annual turnover of the preceding financial year."[120] A company is required to pay upper level fines for severe violations.[121]

At first glance, these penalties may seem astronomical; however, they will not be issued for one violation of the GDPR, especially if the violation is minor.[122] Rather, an egregious violation of the GDPR, or repeated serious violations of the GDPR, may result in the DPA imposing the maximum fine.[123] Additionally, while 2%-4% of the global worldwide annual turnover does not seem like a large number, if DPAs select this as the fee to impose it could "potentially increa[se] maximum fines to over $1 billion for a company such as Facebook and over $3 billion for one such as Google."[124]

In order to determine the appropriate penalty, the GDPR takes "a tiered approach to fines."[125] Individual member-state advisory authorities impose fines, and consider the following factors when determining the amount to fine a non-compliant company: the nature of the infringement; the company's intention; mitigation efforts; preventative measures; history; cooperation; data type;

115. This conversion was made on November 27, 2018.

116. GDPR EU, https://www.gdpreu.org/compliance/fines-and-penalties/ (last visited Oct. 9, 2019). Actions that warrant issuance of these "lower level" fees include "infringements of" (a) the obligations of controllers and processors pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (b) the responsibilities of the certification body outlined in Articles 42 and 43; and (c) the duties of the monitoring body pursuant to Article 41(4). GDPR *supra* note 65, at art. 83.

117. INTERSOFT CONSULTING, https://gdpr-info.eu/issues/fines-penalties/ (last visited Oct. 9, 2019).

118. *Id.*

119. This conversion was made on November 27, 2018.

120. INTERSOFT CONSULTING, https://gdpr-info.eu/issues/fines-penalties/ (last visited Oct. 9, 2019). A DPA can also refer to a data processing agreement, but for the purposes of this writing, it will be considered a data protection authority. GDPR.EU, https://gdpr.eu/what-is-data-processing-agreement/ (last visited Oct. 9, 2019). Considering the stringent obligations imposed by the GDPR on data controllers, there may be a tendency towards increased use of data processing agreements. *See* Kathleen Paisley, *It's All About the Data: The Impact of the Eu General Data Protection Regulation on International Arbitration*, 41 FORDHAM INT'L L.J. 841, 869 (2018).

121. Intersoft Consulting, https://gdpr-info.eu/issues/fines-penalties/ (last visited Oct. 9, 2019). Under the GDPR, these violations include violations of Articles 5, 6, 7, 9, 12, 22, and 44-49. GDPR *supra* note 65, at art. 83.

122. *See* Elitsa Ivanova, *Austrian Data Protection Regulator Issues First GDPR Fine,* GDPR TOOLKIT, https://gdprtoolkit.eu/austrian-data-protection-regulator-issues-first-gdpr-fine/ (last visited Oct. 10, 2019).

123. GDPR EU, https://www.gdpreu.org/compliance/fines-and-penalties/ (last visited Oct. 10, 2019).

124. Houser & Voss, *supra* note 19, at 8.

125. EU GDPR.ORG, https://eugdpr.org/the-regulation/ (last visited Oct. 8, 2019). Some actions that will increase fines include an intentional violation, failing to cooperate with authorities, and failing to act to mitigate the level of harm caused by the violation. INTERSOFT CONSULTING, https://gdpr-info.eu/issues/fines-penalties/ (last visited Oct. 10, 2019).

notification; certification; and possibly, the "financial impact on the firm from the infringement."[126] After considering the factors listed above, the DPA will issue a fine that is "effective, proportionate and dissuasive for each individual case."[127] Member states can also set their own rules and penalties regarding violations of the GDPR.[128] If member states decide to create their own rules and penalties, those penalties are generally criminal.[129]

IV. HOW THE GDPR WILL AFFECT AMERICAN BUSINESSES

It should be apparent that the GDPR will require American businesses to enhance their privacy controls and record keeping procedures if they conduct business within the EU. Many American companies express concern about GDPR compliance and the impact the regulation will have on their business.[130] There are two major paths American companies have taken: (1) only extending the heightened GDPR rights to EU citizens; or (2) extending the heightened GDPR rights to EU citizens and American citizens alike.[131] There are also major companies such as Apple, that are "undertaking Privacy Impact Assessments (PIA) of [their] major products and services and integrating PIAs as [they] develop new products and services."[132] Unlike large companies such as Facebook[133] and Microsoft,[134] which have implemented plans to comply with the GDPR, many companies, especially smaller companies, lack the necessary resources to comply with such a comprehensive and demanding regulation.[135] Consequently, the EU has seen a staunch decrease in the number of investments available for startups within the EU tech industry.[136] This section will examine the actions taken by Microsoft, Facebook, and Apple for GDPR compliance, as well as review the options available to smaller companies.

---

126. GDPR EU, https://www.gdpreu.org/compliance/fines-and-penalties/ (last visited Oct. 10, 2019).

127. INTERSOFT CONSULTING, https://gdpr-info.eu/issues/fines-penalties/ (last visited Oct. 9, 2019).

128. *Id.*

129. *Id.*

130. *See* Dan Clark, *Everyone's Worried About GDPR, but it May Be the Y2K of Data Privacy*, CORP. COUNSEL (May 25, 2018, 12:59 PM), https://www.law.com/corpcounsel/2018/05/25/everyones-worried-about-gdpr-but-it-may-be-the-y2k-of-data-privacy/.

131. *See* Burgess, *supra* note 24. *See also* Arielle Pardes, *What is GDPR and Why Should You Care?*, WIRED (May 24, 2015, 6:00 AM), https://www.wired.com/story/how-gdpr-affects-you/.

132. APPLE, https://www.apple.com/legal/privacy/en-ww/governance/ (last visited Sep. 29, 2019).

133. FACEBOOK, https://www.facebook.com/business/gdpr (last visited Oct. 10, 2019).

134. MICROSOFT, https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/gdpr-overview (last visited Oct. 10, 2019).

135. *See* Forbes Technology Council, *15 Unexpected Consequences of GDPR,* FORBES (Oct. 10, 2019), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#4e7dd15a94ad.

136. Mark Scott, *Six Months in, Europe's Privacy Revolution favors Google, Facebook*, POLITICO (Oct. 10, 2019), https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/.

A. Facebook's Method for Complying

With over one billion users, Facebook, the social media giant, is known for its ability to connect individuals to their friends and family.[137] By reviewing Facebook's website, users can see it is allegedly committed to transparency, control, and accountability.[138] But, what does this really mean? It is no secret Facebook experienced issues with data privacy over the years.[139] Recently, Facebook lost the trust of the American public, in large part due to the Cambridge Analytica scandal.[140] In April 2018, Facebook announced it would implement changes to its data privacy controls and protections.[141] Facebook has changed some privacy rights for users globally—but has not necessarily extended GDPR level protections to all users.[142]

Just by looking at Facebook's website, it is difficult to determine exactly what settings have been changed for its entire user-base and which features have been enhanced exclusively for citizens within the EU.[143] This difficulty arises, in part, because the Facebook website does not list the changes in detail, but also because there does not appear to be much general information available regarding said differences.[144] Facebook is making many small changes, including giving individuals more control over what sensitive information is publicly available.[145] This change began with Facebook asking every user, globally, to examine the privacy choices associated with their profiles including everything from "the information they add to their profile to how Facebook uses their data to target ads."[146] User review of individual privacy settings confers upon Facebook consent to collect personal data, as is required under the GDPR.[147] Facebook can target ads based on an individual's past internet usage if the webpage displays a Facebook Like or Share button,

137. FACEBOOK, https://www.facebook.com/pg/facebook/about/ (last visited Oct. 10, 2019.

138. FACEBOOK, https://www.facebook.com/business/gdpr (last visited Oct. 10, 2019).

139. *See* The Editorial Board, Opinion, *'Facebook Cannot Be Trusted to Regulate Itself'*, N.Y. TIMES (Nov. 15, 2018), https://www.nytimes.com/2018/11/15/opinion/facebook-data-congress-russia-election.html.

140. *See* Herb Weisbaum, *Trust in Facebook has Dropped by 66 Percent Since the Cambridge Analytica Scandal*, NBC NEWS (April 18, 2019, 3:08 PM), https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011.

141. *See* Emily Stewart, *What You Need to Know about Facebook's New Privacy Settings*, VOX (Apr. 18, 2018), https://www.vox.com/technology/2018/4/18/17251480/facebook-privacy-scandal-changes-europe-gdpr

142. *See* Arielle Pardes, *What is GDPR and Why Should You Care?*, WIRED (May 24, 2015, 6:00 AM), https://www.wired.com/story/how-gdpr-affects-you/.

143. The company's page on the GDPR and changes made can be found here: https://www.facebook.com/business/gdpr.

144. Facebook, https://www.facebook.com/business/gdpr (last visited Oct. 10, 2019). It may be expected that Facebook would not want the specifics of the changes released because there may be general public upset about the discrepancies between the rights available to EU citizens and American citizens.

145. *See* Josh Constine, *A Flaw-by-Flaw guide to Facebook's new GDPR Privacy Changes*, TECHCRUNCH (April 18, 2018, 1:00AM), https://techcrunch.com/2018/04/17/facebook-gdpr-changes/.

146. *See* Thuy Ong, *Facebook Announces New European Privacy Controls, For the World*, THE VERGE (Apr. 18, 2018, 6:57AM), https://www.theverge.com/2018/4/18/17250840/facebook-privacy-protections-europe-world-gdpr.

147. *See* Constine, *supra* note 145.

conversion pixel, or Audience Network ad.[148] Amidst concern about data collection and targeting, Facebook will allow individuals to disable the feature permitting the company target ads to individual users.[149]

Additionally, Facebook is reinstituting facial recognition in the EU and Canada after having banned the feature in Ireland in 2012.[150] This feature will generally be used to alert individuals of photos in which they may appear.[151] Finally, Facebook will require specific protections for teenagers due to requirements within the GDPR.[152] Globally, teenagers will be asked whether they would like to see targeted ads, and also whether or not they would like to include personal information on their profile.[153] However, within the EU specifically, teenagers between thirteen and fifteen must have explicit permission from a parent or guardian to authorize target ads or to add interests to their profiles.[154] The parental consent function has received backlash because teenagers can easily defraud the system.[155] To address this concern, Facebook requires a teenager to select a parent or guardian as a friend or enter an email address to a "parent" so the parent may grant permission to adjust their privacy settings. Even so, the young users still have the ability to skirt the requirement by entering any friend's email address or even an email address they control.[156]

B. Microsoft's Method for Complying

Microsoft has taken an approach opposite of Facebook, and has been acknowledged for its expansive approach of extending the same privacy rights to both EU and United States citizens.[157] Microsoft, like the EU, believes privacy is a "fundamental right;" therefore, it is taking action to ensure all users' data is protected.[158] In addition to the increased global data privacy rights, Microsoft offers

148. *Id.*

149. *Id.*

150. *Id.*

151. *Id.*

152. *See* Constine, *supra* note 145. Under the GDPR "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data." GDPR *supra* note 65, at recital 38. This section highlights that protection of children's data is especially important when used for marketing purposes. GDPR *supra* note 65, at recital 38.

153. Constine, *supra* note 145.

154. *Id.*

155. *Id.*

156. *Id.*

157. *See* Burgess, *supra* note 24.

158. *See* Thuy Ong, *Microsoft Expands Data Privacy Tools Ahead of GDPR*, THE VERGE (May 24, 2018, 8:25 AM), https://www.theverge.com/2018/5/24/17388206/microsoft-expand-data-privacy-tools-gdpr-eu.

both products and information to assist others in complying with the regulation.[159] The company acted proactively, unlike many of its competitors, by choosing to implement privacy controls prior to the adoption of the regulation.[160]

Microsoft is dedicated to helping other companies become GDPR compliant.[161] Microsoft offers "compliance solutions" and services it believes will help companies locate and catalog its users' personal data.[162] Microsoft's tools will work for companies both domestically and internationally.[163] The company assures its clients that its programs are GDPR compliant, and even offers additional resources to ensure its clients have their questions addressed, and have the resources they need.[164]

Unlike Facebook, Microsoft has been vocal about the changes it is making to various privacy rights and statements. For example, Microsoft has a "Change History" for any modifications the company makes to its privacy statement.[165] This listing allows the user to easily see what changes have been made to the company's privacy statement.[166] In addition to adding clarity to its privacy statement, Microsoft invested in "redesign[ing] its tools and system" to ensure compliance.[167] Microsoft's action would fall into the "privacy by design" right as it is attempting to act proactively, making sure the technology is designed to protect privacy.

C. Apple's Methods of Complying

As previously stated, Apple is still working to ensure all of its products and services fully comply with the GDPR.[168] The technology conglomerate is currently "undertaking Privacy Impact Assessments (PIA)" of its products and services.[169] Despite the fact that the company is still in its assessment phase, it has implemented, or always had some privacy rights required by the GDPR.[170]

159. Microsoft, https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/gdpr-overview (last visited Oct. 10, 2019).

160. *See* Ong, *supra* note 158.

161. MICROSOFT, https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/gdpr-overview (last visited Oct. 10, 2019).

162. MICROSOFT, https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/gdpr-overview (last visited Oct. 10, 2019).

163. *See* Microsoft Office 365, *Abrona Prepares for GDPR with Microsoft 365*, YOUTUBE (May 25, 2018), https://www.youtube.com/watch?v=xYgv-O4zUj8.

164. MICROSOFT, https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/gdpr-overview (last visited Oct. 10, 2019).

165. MICROSOFT, https://privacy.microsoft.com/en-us/Updates (last visited Oct. 13, 2019).

166. *See* Thuy Ong, Microsoft Expands Data Privacy Tools Ahead of GDPR, THE VERGE (May 24, 2018, 8:25 AM), https://www.theverge.com/2018/5/24/17388206/microsoft-expand-data-privacy-tools-gdpr-eu.

167. *Id.*

168. APPLE, https://www.apple.com/legal/privacy/en-ww/governance/ (last visited Oct. 15, 2019).

169. *Id.*

170. *Id.*

Specifically, the company asserts that it employs "industry leading consent mechanisms to allow [its] customers to choose whether to share data…."[171]

The company also emphasizes it "use[s] access management and access controls commensurate with the risk to data to ensure access to data is associated with a business need," in order to make sure its users' data is safe.[172] Apple has an "iOS Security White Paper" that discusses the technical aspects of how Apple's products and services will protect its users' privacy rights.[173]

Finally, Apple has created a privacy portal to comply with the GDPR by giving users easy access to the tools they need to control their data.[174] The portal is exclusively available to citizens of the European Union, but Apple promised that all of its customers will eventually have access to the portal.[175] The portal serves as a place for users to access their activity, including "activity on the App Store, iTunes Store, iBooks Store, and Apple Music; …activity at Apple's online store and retail stores; any AppleCare support history and repairs [they] may have required; and other data like iCloud bookmarks, calendar entries, reminders, photos and other documents."[176] Allowing users to request, access, review, and delete their data, as well as deactivate their Apple Account in one place with ease, aligns with the true intent of the GDPR and makes it easier for users to take control of their privacy rights.[177]

D. What about the Little Guy?

There is a concern that smaller companies are unable to comply with the GDPR regulations, and that penalties imposed by the regulation will eventually drive them out of business.[178] Small and medium sized companies typically lack the manpower,

---

171. *Id.* Customers can access these mechanisms for the following features: Location, Contact, Reminders, Photos, Bluetooth Sharing, Microphone, Speech Recognition, Camera, Health, Homekit, Media & Apple Music and Motion & Fitness Data. *Id.*

172. *Id.*

173. APPLE, https://www.apple.com/legal/privacy/en-ww/governance/ (last visited: Feb. 4, 2019). The report can be found at https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf. While it is unclear whether the rights of the GDPR extend to American citizens as well, the GDPR, the European Union and the United States are not explicitly mentioned within this report. Apple, https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf, (last visited Oct. 15, 2019).

174. *See* Thuy Ong, *Apple Users in the EU Can Now Download All the Info the Company has on Them*, THE VERGE (May 23, 2018, 9:52 AM), https://www.theverge.com/2018/5/23/17383692/eu-apple-users-id-privacy-portal-gdpr.

175. *Id.* As of September 2019, individuals in the United States have access to the Apple data portal, which can be accessed here: https://privacy.apple.com/.

176. *Id.*

177. *See* John Russell, *Apple Introduces New Privacy Portal to Comply with GDPR,* TECHCRUNCH (May 23, 2018, 11:07AM), https://techcrunch.com/2018/05/23/apple-introduces-new-privacy-portal-to-comply-with-gdpr/.

178. *See* Forbes Technology Council, *15 Unexpected Consequences of GDPR,* FORBES, (Aug. 15, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#4e7dd15a94ad.

or the funds to hire the legal staff and other experts needed to comply with the regulation.[179] Obviously, smaller companies are unable to implement the compliance plans as readily as Microsoft and Facebook, but there are options available to them as well.[180]

As is to be expected with any new law or regulation involving the types of changes implemented by the GDPR a new market has been created to assist companies in complying with the comprehensive regulation. In addition to Microsoft's products, there are several companies that offer assistance with compliance. If one "Googles" "GDPR compliance assistance" one will find dozens of companies claiming they can help companies comply with the GDPR.[181] Of course, this assistance comes at a cost.[182]

There are a few resources various websites specifically recommend for companies that are still trying to come into compliance with the GDPR.[183] After determining the business provides services or sells products in the EU, Bloomberg recommends hiring a data protection officer to make sure the company is following the entirety of the regulation.[184] This is especially important if the company has more than 250 employees, or it is a company that collects large amounts of data.[185]

One easy solution, which many companies have opted to take, is to block individuals within the EU from their websites.[186] For example, two months after the implementation of the regulation, over 1,000 popular news sites, including the Los Angeles Times, became inaccessible to many within the EU.[187] This may be a feasible way to avoid fines until a business can ensure compliance with the GDPR.[188]

---

179. Carol Li, *A Repeated Call for Omnibus Federal Cybersecurity Law,* 94 NOTRE DAME L. REV. 2211, 2229-30 (2019).

180. *See* Manuel Grenacher, *GDPR, The Checklist For Compliance*, FORBES (June 4, 2018, 7:00AM), https://www.forbes.com/sites/forbestechcouncil/2018/06/04/gdpr-the-checklist-for-compliance/#4ea6f8045bec.

181. MICROSOFT, https://blogs.partner.microsoft.com/mpn/gdpr-service-providers-ready-help/, (last visited Nov. 3, 2019).

182. As stated above, even Microsoft has products available to its customers to assist in GDPR compliance; however, their products have a price tag. *See* Microsoft, https://products.office.com/en-US/compare-all-microsoft-office-products?tab=2 (last visited Feb. 4, 2019). *See infra* notes 210-211 and accompanying text.

183. *See* Kristy Westgard & Stephanie Bondoni, *GDPR, or Why Privacy Is Now Stronger in EU than U.S.*, BLOOMBERG (May 24, 2018, 6:00 PM), https://www.bloomberg.com/news/articles/2018-05-24/gdpr-or-why-privacy-is-now-stronger-in-eu-than-u-s-quicktake.

184. *Id.*

185. *Id.*

186. *See* Jeff South, *More Than 1,000 U.S. New Sites are Still Unavailable in Europe, Two Months After GDPR Took Effect*, NIEMANLAB (Aug. 7, 2018, 12:05 PM), http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

187. *Id.*

188. *Id.*

V. CAN THE UNITED STATES KEEP UP?

In the United States, even lawyers do not understand what happens to their personal data after reading the privacy policies of companies making it clear that action is necessary.[189] However, the GDPR is just as complex and difficult to understand as many of the existing privacy policies. Furthermore, while the regulation attempts to combat the evils of large companies (which the regulation does, discussed below), it is also having an impact on small businesses and startups within the EU.[190] The majority of American businesses do not have the financial means to implement compliance plans on the same scale as Facebook, Microsoft and Apple, regardless of the amount of their resources, both small businesses and giants are being hurt by the GDPR.[191]

Throughout 2019, the first GDPR enforcement actions and fines have been completed and issued.[192] The United States is home to leading corporations that control and process data. Coupled with the increased surveillance practices championed by the government,[193] American businesses seem to be disproportionately predisposed to violate the GDPR. In fact, Google, incorporated in Delaware,[194] is the first company under the GDPR to face a major fine. In January 2019, the French data protection authority sanctioned the company, compelling it to pay $57 million.[195] Since the Google fine, GDPR enforcement bodies levied additional fines against two large-scale companies, Marriott Hotels[196] and British Airways.[197]

189. *See* Adam Satarino, *Google is Fined $57 Million Under Europe's Data Privacy Law,* N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

190. *See* Leonid Bershidsky, Opinion, *Europe's Privacy Rules Are Having Unintended Consequences*, BLOOMBERG OPINION (Nov. 14, 2018, 1:00 AM), *https*://www.bloomberg.com/opinion/articles/2018-11-14/facebook-and-google-aren-t-hurt-by-gdpr-but-smaller-firms-are.

191. *Id.*

192. *See* Adam Satarino, *Google is Fined $57 Million Under Europe's Data Privacy Law,* N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

193. *See supra* note 30 and accompanying text.

194. *See* Juliette Garside, *Google's Alphabet Restructure could get boost from Delaware Tax Loophole*, THE GUARDIAN (Aug. 11, 2015), https://www.theguardian.com/technology/2015/aug/11/google-alphabet-delaware-tax-loophole.

195. *See* Adam Satarino, *Google is Fined $57 Million Under Europe's Data Privacy Law,* N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

196. *See* Katie O'Flaherty, *Marriott Faces $123 Million Fine for 2018 Mega-Breach*, FORBES (Jul. 9, 2019, 11:49AM) https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million/#99e489b45253. The company faced a $123 million dollar fine for "failure to undertake sufficient due diligence" after a data breach occurred. *Id.*

197. *See* Charles Riley, *British Airways faces $230 million fine. It would be a record under Europe's tough data privacy law*, CNN BUS. (July 8, 2018, 11:00AM), https://www.cnn.com/2019/07/08/tech/british-airways-gdpr-fine/index.html. The ICO issued a $230 million fine against the company, which is approximately 1.5% of the company's total annual revenue. *Id.*

Small businesses within the EU have also been sanctioned recently.[198] The sanctions are not a good omen for either large or small American businesses. However, it appears, based on a sanction in Austria, that the DPAs are fair and reasonable when issuing fines to small businesses.[199] Google and Marriott, two large companies, are the only United States companies to be fined under the GDPR.[200] Therefore, companies both within the United States and the EU are waiting to see how the DPAs will fine small American businesses.

Despite what appears to be fair and reasonable fees thus far, it is difficult to have confidence in a system working its way to the United States when European start-ups and small businesses within the EU are suffering.[201] Since the implementation of the GDPR, weekly venture deals within the EU have decreased by 17.6%.[202] Where there is clear evidence of harm in the EU, the United States does not seem to have noticed a similar decrease.[203]

Small businesses within the United States may fare well if they budget and act proactively; however, it will be difficult for the average small business to come into compliance.[204] The mere cost of purchasing Microsoft's compliance solutions may be enough to dissolve some small businesses.[205] Simply understanding the 261 page regulation may prove difficult for large and small companies alike; however, hiring an expert, or an attorney may pose a greater challenge to smaller companies with fewer resources.[206] Small companies should learn from larger companies and start by implementing procedures that further the core principles of the GDPR. For instance, smaller companies can begin communicating with customers to get consent to data collection and data sharing, like Facebook,[207] and allowing users to request the deletion of the data, like Apple.[208] A smaller business owner feeling

198. *See* Elitsa Ivanova, *Austrian Data Protection Regulator Issues First GDPR Fine,* GDPR TOOLKIT, https://gdprtoolkit.eu/austrian-data-protection-regulator-issues-first-gdpr-fine/ (last visited Nov. 3, 2019). A DPA within Austria found a small business in violation of the GDPR after it installed a CCTV that also recorded a large portion of the sidewalk outside of the storefront. The storeowner received a fine of €4800, which is approximately $5,492.00. *Id.*

199. *Id.*

200. *See supra* notes 195–196 and accompanying text.

201. *See* Leonid Bershidsky, Opinion, *Europe's Privacy Rules Are Having Unintended Consequences*, BLOOMBERG OPINION, (Nov. 14, 2018, 1:00 AM), *https*://www.bloomberg.com/opinion/articles/2018-11-14/facebook-and-google-aren-t-hurt-by-gdpr-but-smaller-firms-are.

202. *Id.*

203. *See* Julie Bort & Rosalie Chan, *44 Enterprise Startups to Bet Your Career On in 2019*, BUSINESS INSIDER (Jan. 5, 2019, 12:20PM), https://www.businessinsider.com/44-enterprise-startups-to-bet-your-career-on-in-2019-2018-12#fastly-making-websites-and-apps-faster-24. In reviewing this list of new startups, one will see that the vast majority are all located within the United States.

204. Carol Li, *A Repeated Call for Omnibus Federal Cybersecurity Law,* 94 NOTRE DAME L. REV. 2211, 2229–30 (2019).

205. *See supra* note 179 and accompanying text.

206. *See* Li, *supra* note 204, at 2230.

207. *See* supra notes 146–47 and accompanying text.

208. *See* supra notes 175–177 and accompanying text.

overwhelmed by the process may consider Microsoft's compliance assistance, or consider hiring a contractor to help the business come into compliance.[209] If smaller companies choose to move forward with a service like Microsoft's, it is important to keep the price in mind. Microsoft's "Compliance Solutions" (which are really just Microsoft Office products) range in price between $5.00-$12.50 per month, per user.[210] For a company of 250 people, GDPR compliance through Microsoft would automatically create a $15,000-$37,000 additional annual expense.[211]

It is important to remember that small businesses in the United States appear to have the gift of time. The regulation has been in place for over a year, and "has been a success as a breach notification law, but largely a failure when it comes to imposing fines on companies that fail to adequately protect their customers' data."[212] Between its enactment in May 2018, and January 2019, the EU saw just under 60,000 (59,330) reported violations of the GDPR.[213] However, during this time, the DPAs only issued €55,955,871 in fines (of which €50 million was issued to Google).[214] With this in mind, it is safe to assume small businesses, especially those not located within the EU, will be safe from fines for the foreseeable future. Furthermore, it is not cost-effective for enforcement agencies to pursue claims against smaller companies, when giants such as Google and Marriott generate millions of dollars in fines. Finally, the only companies currently under investigation within the United States are giants in the world of data control and processing, not local, independent or start-up companies.[215] So, in short, companies can take a breath, but should plan for the future.

CONCLUSION

The GDPR modifies the previously existing 1995 Directive and gives citizens within the European Union more control over what information companies are allowed to collect and distribute. Additionally, this regulation affords users more control over their own privacy rights by allowing EU residents to edit or withdraw information companies collect and disseminate about them. Importantly, the GDPR regulation expands the jurisdiction of the old directive to companies outside of the European Union that have virtually any interaction with users within the European Union.

209. *See* Raad Ahmed, *GDPR: What Small Businesses Need to Know*, FORBES YEC COUNCIL (Mar. 4, 2019, 8:00AM), https://www.forbes.com/sites/theyec/2019/03/04/gdpr-what-small-businesses-need-to-know/#2558f1ea3197.

210. MICROSOFT, https://products.office.com/en-US/compare-all-microsoft-office-products?tab=2 (last visited Oct. 16, 2019).

211. *Id.*

212. *See* Josephine Wolff, *How is the GDPR Doing?*, SLATE, (Mar. 20, 2019, 5:42PM), https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html.

213. DLA Piper's Cybersecurity Team, *DLA Piper GDPR Data Breach Survey: February 2019*, DLA PIPER (Feb. 6, 2019), https://www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/.

214. Wolff, *supra* note 212.

215. *See* supra notes 192–97 and accompanying text.

Finally, the GDPR significantly increases the maximum penalties for egregious and repetitive violations of the new regulation.

While there is no set way to adopt policies to comply with the GDPR, larger companies will likely implement policies that follow the direction of either Microsoft (implementing the same policies and rights for all customers globally), or will follow the direction of Facebook, (opting to update privacy policies). For smaller companies, there will be a greater burden, but there are services offered through larger companies like Microsoft, and independent, smaller companies, to help establish and maintain compliance. Either way, if a company cannot meet the stringent regulation requirements, depending on the size of the company, and the number and severity of the violations, that company can may face major fines. Whether or not individuals agree with the GDPR, it is apparent the legislation will likely impact companies around the globe because the regulation contains "'some rights that companies couldn't contain to Europeans even if they tried.'"[216]

216. *See* Arielle Pardes, *What is GDPR and Why Should You Care?*, WIRED (May 24, 2015, 6:00 AM), https://www.wired.com/story/how-gdpr-affects-you/.