Northwestern Journal of International Law & Business

Volume 40
Issue 2 *Winter*

Article 3

Winter 2020

Do You Accept These Cookies? How the General Data Protection Regulation Keeps Consumer Information Safe

Jayne Chorpash

Vol. 40, No. 2
Northwestern Journal of International Law & Business

Do You Accept These Cookies? How the General Data Protection Regulation Keeps Consumer Information Safe

Jayne Chorpash*

Abstract:

This note examines the General Data Protection Regulation implemented in the EU in 2018. The GDPR was the result of a long history of data privacy laws that have been met with varying levels of success. While the GDPR has retained many characteristics that have made past privacy laws successful, it has also made some important changes. Most notably, the GDPR gives generous rights to consumers to guard and protect their data, which is of growing concern in light of how easy it is to share information in our modern age. Additionally, the GDPR has a much broader territorial scope, covering data processing activities related to either the offering of goods or services to EU data subjects or the monitoring of their behaviors within the EU. As a result, the hefty fines imposed for violating the GDPR have forced many companies to comply quickly. This note continues by comparing the GDPR's regulations with those of the United States and concludes that, although there may be more upfront barriers and costs to adopt regulations as stringent as the GDPR, overall, the GDPR is superior to privacy laws in the United States. Finally, this note concludes by briefly examining the future of the GDPR, as well as the potential for GDPR-like regulations to be adopted in the United States.

* Jayne Chorpash J.D., Northwestern Pritzker School of Law, 2020. The author would like to thank the Northwestern Journal of International Law and Business editorial staff for their help in refining this Note.

TABLE OF CONTENTS

I. INTRODUCTION

The General Data Protection Regulation (GDPR) was proposed in 2012, adopted in mid-April of 2016, and implemented on May 25, 2018.[1] It regulates privacy and data protection for the European Union (EU) and the European Economic Area (EEA).[2] These new reforms are part of a movement to modernize privacy laws as the race to keep up with changing technology continues. Although these new regulations are not entirely dissimilar from the ones which they replaced, the GDPR will have far-reaching impacts, not only within the EU, but across the globe. Even though the exact effect of the GDPR is still unknown, the GDPR is the future of privacy laws in our new digital age and is better suited to regulate the United States' privacy laws than the system currently in place.

Although privacy is now seen as a fundamental right of citizens in the EU, it was a long road to the acceptance of this perspective for the bloc. A unified regime of privacy legislation in the EU did not begin until the mid-nineteen-nineties. Before 1995, each EU member state created its own privacy legislation, the efforts of which were completely undermined when data would be transferred between member states since the new member states' law would apply.[3] This led to the 1995 adoption of the EU Data Protection Directive in order to harmonize the data protection policies fragmented across the EU.[4] Not only did this allow all EU citizens to retain their right to data privacy, but it also guaranteed the "free flow of personal information between member states."[5] This was the first sort of legislation that protected all citizens of the EU regardless of which member state they inhabited.[6] Among the rights given to citizens under the EU Data Protection Directive were the rights to delete or correct personal data and to be notified of uses and disclosures of data collection.[7] The 1995 Directive imposed duties upon both EU companies as well as collectors of EU data, which also included third party data collectors located in other countries but utilized by EU companies.[8]

While the 1995 Directive was effective within the EU, it cut the EU off

---

[1] 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, 96–97 (2016); Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Jan 21, 2019), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

[2] *Id.; see also* Phillip Rees et al., *Transferring Personal Data Outside the EEA: The Least Worst Solution*, 13 COMPUTER & TELECOMM. L. REV. 66 (2007).

[3] Curtiss, *supra* note 1, at 98.

[4] *Id.* at 97.

[5] *Id.* at 99.

[6] *Id.* at 98.

[7] *Id.* at 99.

[8] *Id.*

from transfers of information outside of the bloc.[9] The Directive forbade transfers of personal data outside of the EU unless the country the data was to be transferred to had adequate measures in place to safeguard the information.[10] This included the United States.[11] However, the United States and the EU were able to overcome this obstacle by creating the Safe Harbor Framework.[12]

The Directive on Privacy and Electronic Communications, enacted in 2002 as a complementary directive to the 1995 Directive, expanded protections to include electronic communications "such as the internet and mobile and landline telephony and via their accompanying networks."[13] There were subsequent alterations to the 2002 Directive in the Data Retention Directive and the 2009 Amendment Directive, which included further clarifications on retention schedules for data, as well as rules on the use of cookies on websites.[14]

All of these changes in EU privacy laws set the stage for the GDPR proposal in 2012. It built on many parts of the 2002 Directive that worked well, but also updated the laws to adapt to the significant changes in technology that have occurred across the globe in recent years.[15]

Part II of this Note will provide an overview of the GDPR, including its purpose, how to comply with its regulations, and the main parties impacted by its enactment. Part III will focus on the United States' historical handling of consumers' personal data. This includes the United States' pattern of conduct when dealing with data transfers with the EU. Finally, Part IV will argue that the GDPR is the preferred method of data protection in today's modern world, although the effectiveness of the GDPR is still unclear just over a year after its enactment. This Note recommends that the United States pass uniform legislation to regulate data privacy that is similar to the GDPR because of advances in technology that put consumers at a higher risk of data mishandling, as well its interest its laws consistent with those of the EU. Finally, the Note will conclude by outlining changes in the United States' privacy laws and predictions as to whether the U.S. will adopt GDPR-like changes.

---

[9] *See* Craig McAllister, *What About Small Businesses? The GDPR And Its Consequences for Small, U.S.-Based Companies*, 12 BROOK. J. CORP. FIN. & COM. L. 187, 190 (2017).

[10] *Id.*

[11] *Id.*

[12] *See* discussion *infra* Part III.

[13] *Data Protection in the Electronic Communications Sector*, EUR-LEX, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24120 (last visited Jan. 13, 2020); *see* Directive 2002/58/Ec of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37.

[14] Curtiss, *supra* note 1, at 100.

[15] *Id.* at 97.

II. THE PURPOSE OF THE GDPR

When the GDPR went into effect in 2018, it replaced the previous 2002 Directive and its subsequent changes and amendments.[16] Instead of each member state needing to enact the GDPR in order for it to come into effect, the policies became valid immediately on May 25, 2018. The regulations create a single supervising authority to regulate enforcement for each impacted organization depending on the organization's location or, if an organization has more than one location, its "main establishment."[17]

Enforcement of the GDPR is accomplished through Supervisory Authorities (SAs).[18] Each member state in the EU appoints a SA, all of which are coordinated by the European Data Protection Board.[19] SAs have the authority to conduct audits, issue warnings and fines, and impose limits or bans on processing, amongst other powers.[20]

There are two main purposes behind the GDPR. The first is to preserve the harmonization of the 1995 and 2002 directives while modernizing data laws to accommodate new technology.[21] In the past decade alone, the role of technology in people's daily lives has drastically changed in developed countries across the globe. However, data privacy laws have not adapted as quickly. As a result, many questions arose about how to regulate this new technology under the prior directives, while permitting it to function properly in the modern world.[22] The GDPR hopes to answer these questions but still be adaptable to the changing times.

The other purpose of the GDPR is to give EU citizens more control over their personal data.[23] The improvements in technology have given companies a farther reach in data collection than ever before–it is much easier for businesses in the United States to capture customers in the EU than in the past because of the interconnectedness of the contemporary world.[24] However, this increased reach, through what was a somewhat unregulated medium, poses a threat to consumers, who bear the risk of unauthorized data sharing and the consequences of data breaches. The GDPR works to correct

---

[16] McAllister, *supra* note 9, at 187.

[17] *Id.* at 193.

[18] *Who Enforces GDPR Compliance?*, SERA-BRYNN (Mar. 30, 2017), https://sera-brynn.com/enforces-gdpr-compliance.

[19] *Id.*

[20] *Id.*

[21] Curtiss, *supra* note 1, at 97.

[22] For example, how will the GDPR regulate smaller companies that are working towards compliance but are not completely compliant yet? How can the regulation balance consumer safety while still giving companies the opportunity to make significant changes to their business models? *See* Corey Nachreiner, *Global Confusion Still Surrounds GDPR Compliance*, ITPROPORTAL (Nov. 2, 2017), https://www.itproportal.com/features/global-confusion-still-surrounds-gdpr-compliance.

[23] McAllister, *supra* note 9, at 207.

[24] *Id.* at 194.

this potential pitfall by offering protections to citizens of the EU both from companies at home and abroad.[25]

A. How the GDPR Compares to Previous Directives

The GDPR accomplishes its two purposes with many adjustments from the previous directives, some slight and some substantial.[26] It establishes new requirements in the realm of data protection, data breach notification, limits on processing, transparency, data privacy rights, and limits on data transferring outside the EU.[27]

These protections apply to "data subjects," which essentially include "any person whose personal data is being held, collected, or processed."[28] For the purposes of the GDPR, these protections apply to citizens in the EU.[29] The protections also depend on whether a product or service is delivered in the EU and personal data is processed and/or monitored as a result, which can apply to any person who, for example, purchases a pair of shoes in the EU to be delivered to Australia.[30]

In terms of privacy notices, the kind of information that companies must provide to website visitors and customers is expanded under the GDPR.[31] Article 13 of the GDPR mandates that data subjects "receive clear, concise, and easily-understood information regarding, among other things, the data that is being processed, the purpose(s) for which the data is being processed, and the identity of the data controller."[32] For some companies, this may mean an update to their websites and other online portals.[33] Data subjects are entitled to more information about the company's use of their data, regardless of whether the data subjects take the time to read it or not.

Additionally, consent by data subjects must be "freely given, specific, informed and unambiguous."[34] Data subjects must know exactly what they are opting into and cannot be misled.[35] Companies must also inform data

---

[25] *Id.*

[26] *See generally* McAllister, *supra* note 9.

[27] Daniel K. Alvarez, *The EU General Data Protection Regulation Is Coming–Is Your Client Ready?*, 63 PRAC. LAW. 19, 19 (2017).

[28] *What is A Data Subject?* EU GDPR COMPLIANT, https://eugdprcompliant.com/what-is-data-subject (last visited Dec. 10, 2019).

[29] *GDPR Doesn't Only Protect EU Citizens - Who Does GDPR Affect?*, SITEIMPROVE (Oct. 18, 2018), https://siteimprove.com/en/gdpr/who-gdpr-affects-and-whose-data-is-protected.

[30] *Id.*

[31] Alvarez, *supra* note 27, at 19.

[32] *Id.*

[33] *Id.*

[34] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 34 [*hereinafter* General Data Protection Regulation].

[35] *See* Alvarez *supra* note 27, at 20.

subjects of their right to withdraw their consent at any time, and it must be as easy for users to withdraw consent as to initially give their consent.[36] The burden is on the controller of the data to show that the consent given was adequate.[37]

Data subjects have additional and expanded privacy rights under the GDPR.[38] These include "the rights of access, rectification, erasure, data portability, and objecting to certain types of processing."[39] These rights apply both to data collected directly from the data subject as well as data collected from a third party.[40] While the previous EU directives provided for some of these rights, the GDPR creates new rights for data subjects such as the right to erasure and the right to be forgotten.[41]

There are added security requirements that businesses must comply with as well.[42] The GDPR mandates an "appropriate level of security" for personal data collected by companies.[43]

This includes protection against unlawful processing, damage, destruction, or accidental loss.[44] The GDPR lists a number of factors for businesses to determine whether they have met the threshold of "appropriate" security, including "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."[45] These factors are important for companies to contemplate and in designing systems to safeguard data subjects' data.[46]

One of the new requirements under the GDPR includes creating a data protection impact assessment (DPIA).[47] A DPIA must be conducted by a data protection officer (DPO) before a company processes any data likely to pose a high risk to the rights of a data subject.[48] While some companies already have a DPO, many other companies had to scramble before the GDPR was implemented to find someone to fill this role.[49] There are four main requirements in creating the DPIA:

---

36 *Id.*

37 *Id.*

38 *Id.*

39 *Id.*

40 W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAW. 222, 225 (2016-2017).

41 *Id.*

42 Alvarez, *supra* note 27, at 20.

43 General Data Protection Regulation, 2016 O.J. (L 119) 1, 51-52.

44 *Id.*

45 *Id.*

46 *See* Alvarez, *supra* note 27.

47 Voss, *supra* note 40, at 228.

48 Alvarez, *supra* note 27, at 20.

49 *Id.*

> 1) a systematic description of the processing, 2) evaluation or assessment of the respective risks. . . . 3) measures to address the risk (including safeguards, security measures, and mechanisms to ensure data protection and regulatory compliance) and 4) an assessment of the 'necessity and proportionality of the processing operations in relation to the purposes.'[50]

The DPO's independent review allows for further transparency and a reduced risk of mishandling of data subjects' information in mandating.[51]

Another shift from the previous directives is the breach notification requirement in the GDPR, which is the first breach notification law in the EU.[52] Under the GDPR, the data controller is required to notify the appropriate DPO no more than seventy-two hours upon becoming aware of a data breach.[53] It also requires the data subjects impacted to be notified and implements record-keeping requirements for companies if there is a data breach.[54]

While those are the most significant changes implemented by the GDPR, there are additional, updated practices for service providers. There are also regulations that have undergone no noteworthy changes, such as in cross-border transfer regulations from previous directives.[55]

The changes caused by the GDPR have ramifications for businesses, as they will incur the cost of compliance. Businesses are essentially forced to obey the GDPR or face hefty suits by data subjects and regulators.[56] Authorities in the EU have the ability to impose much higher fines on companies that do not comply with the new regulations totaling "up to EUR 20,000,000 or in the case of an undertaking, up to four percent of its total worldwide annual turnover of the preceding financial year, whichever is higher" for noncompliance.[57] Prior to the GDPR, there was significant variance across the member-states as to fines, but the highest fine imposed before the GDPR's implementation was £400,000, or over $500,000.[58]

These steep fines evidence the seriousness of noncompliance; however, the EU has policed these fines with varying levels of force over the past year or so. While the fines may be extreme, the monetary damage is only one half

---

[50] Voss, *supra* note 40, at 225.

[51] *Id.* at 229.

[52] Alvarez, *supra* note 27, at 20.

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *See* Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INFO. POL'Y, 479, 495 (2016).

[57] *Id.*

[58] Michelle Drolet, *GDPR Fines: How Much Will Non-Compliance Cost You?*, CSO (Oct. 23, 2017, 8:07 AM), https://www.csoonline.com/article/3234685/data-protection/gdpr-fines-how-much-will-non-compliance-cost-you.html.

of the risk of noncompliance. Reputational harm is also likely to result should a company fail to meet the standards of the GDPR. Bad press, customer avoidance of the company, and loss of consumer trust are all foreseeable issues that could arise should a company fail to comply with the provisions of the GDPR.

If companies outside of the EU think they can turn a blind eye to the consequences of violating the GDPR, they are quite wrong. Even businesses outside of the EU must comply with the GDPR if they do business with EU citizens.[59] Under Article 3(1) of the GDPR, the territorial scope of its application is defined as covering the "processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."[60]

The GDPR zeroes in on where the data itself is processed as opposed to where the company physically exists.[61] Furthermore, the GDPR outlines when its regulations apply to places outside of the EU.[62] If data processing activities are related to either the offering of goods or services to EU data subjects or the monitoring of behaviors of data subjects within the EU, those companies are subject to the GDPR's iron grasp.[63] This expansion of the territorial scope is much wider than any of the EU's previous directives, and many businesses, regardless of their locations, must take note of this important distinction as they may be subject to much harsher regulations and fines than before.

B. Implications for Data Controllers and Data Processors

Another significant change from prior directives is that the GDPR creates affirmative duties, obligations, and responsibilities not just for data controllers, but also for data processors.[64] There has always been a distinction between data processors and data controllers, but, previously, only data controllers were subject to EU regulations.[65] The GDPR retains this distinction but levies obligations on both roles.[66] Data controllers include those who control the processing of personal data, whereas data processors are those who execute data processing for the data controller.[67]

Data controllers still must carry the most weight under the GDPR by

---

[59] Burri & Schär, *supra* note 56, at 496.

[60] *Id.* at 495.

[61] *Id.*

[62] *Id.*

[63] *Id.* at 496.

[64] *Id.* at 493.

[65] *Id.*

[66] *Id.*

[67] Debbie Heywood, *Obligations on Data Processors Under the GDPR*, TAYLORWESSING (June 2016), https://globaldatahub.taylorwessing.com/article/obligations-on-data-processors-under-the-gdpr.

ensuring that the data they process is consistent with the regulations of the GDPR and must be able to show evidence of their compliance.[68] On the other hand, data processors are required to "process personal data in accordance with the controller's instructions."[69] While these are incredibly vague mandates, the controllers and processors will likely further specify the controllers' exact requirements when creating their contract between the two parties. However, there are some specific requirements built into the GDPR: one is that data processing activities must be governed by a contract between the processor and the controller and must lay out the purpose of the processing as well as the obligations and rights of the controller.[70] Additionally, data processors must report to the controller if they think there has been a breach of the GDPR or relevant EU or Member State law, and data processors can only process data upon written instruction from the controller.[71] Therefore, although requirements for data processors now exist under the GPDR, the brunt of compliance still remains square on the backs of the data controllers.

C. Expanded Rights for Data Subjects

While the GDPR imposes many new obligations for data processors and controllers, it also creates many new rights for consumers and citizens of the EU.[72] The most significant changes under the GDPR include data subjects' right to know whether there has been a data breach, their right to be forgotten, and data portability.[73]

Companies are obligated to report a data breach to their data subjects when personal data is involved within seventy-two hours of becoming aware of the breach when feasible; If there is a risk of data subjects' personal data being transferred somewhere in which they did not consent, they must be notified "without undue delay." [74] The pressure on companies is steep to ensure that they send out notification within the short window after a breach occurs without violating the GDPR. This gives companies great incentive to keep consumers' personal data secure.

The right to be forgotten under the GDPR is an expansion of the right of erasure enacted in previous EU directives.[75] Data subjects can have their information erased and not further processed if either: 1) they withdraw their consent or object to the data processing, 2) the personal data is no longer necessary for the purposes in which it was collected, or 3) the data was

---

68 *Id.*
69 *Id.*
70 *Id.*
71 *Id.*
72 *See* Burri & Schär, *supra* note 56, at 490-91.
73 *Id.*
74 *Id.* at 493.
75 *Id.* at 490.

unlawfully processed.[76] However, the rights of these data subjects do not always apply. The controller can retain the data subject's information in order to "exercis[e] the right of freedom of expression and information," for public interest reasons, or when the information relates to legal claims.[77]

Assuming none of the exceptions apply, the right to be forgotten is quite strong for data subjects. When requested by the data subject, the controller not only must erase the data subject's data, but also must take reasonable steps to inform other controllers processing the personal data to erase links, copies, or replications of such data.[78] While cumbersome for data controllers, this assures that data subjects will have almost complete control over their personal information.

Data portability is a completely new addition to privacy policy laws. Data subjects are able to receive personal data concerning themselves that they have provided to the controller in a readable format and can transmit that data to any other controller without hindrance from the initial controller from which they received their data.[79] Data subjects can also request their data to be transmitted from one controller to another when it is technically feasible.[80] This gives the data subject even more power in handling his own data and deciding who has access to his data.

Other notable rights under the GDPR include the right for data subjects to receive transparent information, the right to access their personal data, and the right to object to processing of their personal data.[81] All of these expansive rights restrict data controllers and processors more than ever before, which highlights just how sincere the EU is about protecting the rights of consumers and citizens. Users will now have much more independence over how their data is handled and can better direct who is controlling that personal information. With so much technology that an everyday consumer may have a hard time comprehending, the GDPR strives to ensure that each person can feel more comfortable sharing his most personal data with companies and not have it extorted or mishandled.

One lingering question for some may be whether the GDPR will still apply to the United Kingdom in light of the country's upcoming "Brexit", or departure from the EU. Under the U.K.'s Repeal Bills, all direct EU legislation will still apply after the country leaves the EU unless it is explicitly repealed.[82] Since the GDPR was enacted into law before the U.K.'s exit and there has been no subsequent legislation to explicitly repeal, the

---

[76] General Data Protection Regulation, 2016 O.J. (L 119) 1, 43-44.

[77] *Id.*

[78] Burri & Schär, *supra* note 56, at 490.

[79] General Data Protection Regulation, 2016 O.J. (L 119) 1, 45.

[80] Burri & Schär, *supra* note 56, at 491.

[81] *Id.* at 490.

[82] Michael Baxter, *Brexit Provides no Let-up for UK Firms on GDPR, but it Will Mean Some Changes*, PRIVSEC REPORT (Aug. 14, 2018), https://gdpr.report/news/2018/08/14/brexit-provides-no-let-up-for-uk-firms-on-gdpr-but-it-will-mean-some-changes./.

GDPR will still apply in full force to the U.K as of now.[83]

III. UNITED STATES PRIVACY LAWS AND THE GDPR'S IMPACT

A. A History of Data Transfer Mechanisms Between the United States and the EU

With the GDPR's unprecedented territorial reach means that other countries must care about the conduct of their own citizens, and the United States is no exception. The GDPR is not the first time that the United States has been tied up with the EU when it comes to privatcy laws. Before the current directive, there was the Safe Harbor Framework made between the United States and the EU, approved in 2015.[84] Under the Safe Harbor Framework, companies in the United States were able to legally transfer personal data to the EU without violating any of the EU data protection laws.[85] United States companies complied with the Safe Harbor Framework by certifying to the United States Department of Commerce that they provided certain protections for the personal data.[86] However, there has been dissatisfaction expressed over the Safe Harbor Framework by the EU, including recommendations from the EU parliament that countries stop using the Safe Harbor Framework after proposing over 300 amendments to the agreement.[87] By the end of 2015, the EU Court of Justice deemed the Safe Harbor Framework invalid because it did not offer adequate protection to EU citizens.[88]

The EU replaced the Safe Harbor Framework with the EU-U.S. Privacy Shield, which acted as another data transfer mechanism with provisions similar to the GDPR, although the GDPR is much broader.[89] The Privacy Shield was finalized in 2016 and acted as a safeguard for EU citizens to protect their information once their data was transferred outside the borders of the EU.[90] Yet, although there are some similarities between the Privacy

---

[83] *Id.* This is still true as of January 2020. *See GDPR and Brexit: How will one affect the other?* IT PRO (Jan. 9, 2020), https://www.itpro.co.uk/general-data-protection-regulation-gdpr/what-brexit-means-for-gdpr.

[84] *US-EU Safe Harbor Under Pressure*, IAPP (Aug. 2, 2013), https://iapp.org/news/a/us-eu-safe-harbor-under-pressure./.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] Bernard Marr, *Privacy Shield -- Is Safe Harbour's Replacement Up To The Job?*, FORBES (Mar. 29, 2017, 2:42 AM), https://www.forbes.com/sites/bernardmarr/2017/03/29/privacy-shield-is-safe-harbours-replacement-up-to-the-job-in-2017/#7014278d6736.

[89] Paola Zeni, Francoise Gilbert & Max Calehuff, *GDPR and Privacy Shield: Different Tools for Different Goals*, ASS'N OF CORP. COUNSEL 78, 78 (2018).

[90] *Id.* at 80.

Shield and the GDPR, the regulations were enacted separately and were not intended to work in tandem.[91]

B. Current Privacy Laws in the United States

The kinds of data that the GDPR seeks to protect are distinct from those covered by the Privacy Shield.[92] However, where the two overlap, the GDPR tends to be much more far reaching and contains more details, so complying with the GDPR will also satisfy compliance with the Privacy Shield.[93]

Privacy law in the United States is not regulated under a single comprehensive federal law, much like the EU was before the Data Protection Directive in 1995.[94] However, there are a handful of prominent federal laws that regulate the collection, storage, and processing of personal data, although not in one uniform system. These include the Federal Trade Commission Act (FTC Act), The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB Act)), The Health Insurance Portability and Accountability Act (HIPAA), and the Fair Credit Reporting Act.

The FTC Act applies both to offline and online data protection policies.[95] Its most relevant purpose to data protection policies is "to prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce."[96] It also provides relief to consumers who are injured by such dishonest practices.

While the FTC Act focuses broadly on data protection, the GLB Act more narrowly regulates financial institutions as well as businesses that provide financial products and services.[97] Some of the requirements of the GLB Act are reminiscent of the GDPR, including regulations related to disposal of data and, in some cases, opt-out and notice requirements.[98] However, the specific limitation of the GLB Act to financial data distinguishes it from the GDPR.

HIPAA, like the GLB Act, also applies to a specific sector of data collection, in this case medical information.[99] This can be applied generally "to health care providers, data processors, pharmacies and other entities that come into contact with medical information."[100] HIPAA contains a security breach notification requirement where companies must give notice of any

---

91 *Id.*

92 *Id.*

93 *Id.*

94 IEUAN JOLLY, WEST, DATA PROTECTION IN THE UNITED STATES: OVERVIEW, PRACTICAL LAW COUNTRY Q&A 6-502-0467 (Oct. 2018).

95 *Id.*

96 15 U.S.C. §§ 41-58 (1914).

97 JOLLY, *supra* note 94.

98 *Id.*

99 *Id.*

100 *Id.*

uses of protected health information not permitted under its rules unless there is a low chance that the information has not been compromised.[101]

The Fair Credit Reporting Act applies to data protection in the context of consumer reporting agencies, including users of consumer reports as well as providers of consumer reporting information.[102] Consumer reports can be any materials used to assess a consumer's eligibility for insurance or credit.

While the laws described above are just a small handful of federal regulations that enforce data protection policies, there are a number of similar provisions that affect consumers in the United States. Additionally, industry groups commonly issue guidelines, considered the "best practices" in those industries, which are not legally enforceable but are generally followed by members of that industry group.[103]

States also can and do authorize their own sets of privacy laws. However, many are not nearly as comprehensive as the GDPR. California is paving the way for the United States' privacy laws; it was the first state to enact a data breach notification law, which many states have imitated when creating their own (all 50 states now have similar laws).[104] While many federal laws pre-empt state laws, this does not always apply to data protection laws.[105] This may lead to frustration when a company finds itself attempting to conform its data policies to both federal law and state law that regulate the same types of data.

With the invalidation of the Safe Harbor Framework, the United States is in a precarious spot with the EU when it comes to data transferability. The Safe Harbor Framework was the means by which the EU could certify that any data transfers between the United States would be safe and trustworthy.[106] Without these regulations in place, it is likely that the EU will not have that same confidence in the United States' data security. Since the EU has now heightened its data protection standards, European data collectors may be less willing to engage in data transfers with the United States companies that do not comply with the GDPR. There does not seem to be any national momentum to enact similar GDPR reforms in the United States at this point in time; thus, the relationship with the EU in terms of data transfers is just as murky as it has been since the Safe Harbor Framework was invalidated three years ago.[107]

---

[101] *Id.*

[102] *Id.*

[103] JOLLY, *supra* note 94.

[104] *Id.*

[105] *Id.*

[106] *See* Bernard Marr, *Privacy Shield -- Is Safe Harbour's Replacement up to the Job?*, FORBES (Mar. 29, 2017, 2:42 AM), https://www.forbes.com/sites/bernardmarr/2017/03/29/privacy-shield-is-safe-harbours-replacement-up-to-the-job-in-2017/#7014278d6736.

[107] *See* Shaun Nichols, *GDPR USA? 'A Year ago, Hell No ... More People are Open to it Now' – House Rep Says EU-like Law May Be Mulled*, THE REGISTER (Nov. 8, 2018, 11:04

IV. WHY THE GDPR IS PREFERABLE FOR THE UNITED STATES

While the GDPR institutes many changes to privacy regulations not just within the EU but also across the globe, the outcome will be positive internationally if the GDPR is enforced as it was intended. Although the GDPR regulations are quite new, should they have their desired impact, they will hopefully set the stage for similar adjustments to be made in other countries, including the United States.

A. Benefits of Similar GDPR Regulations in the United States

The GDPR established a new global standard of data privacy laws, and the United States risks falling behind if it does not conform its own data privacy policies accordingly. Furthermore, the invalidation of the Safe Harbor Framework leaves the United States on rocky ground in terms of data transfers between the two. In fact, EU citizens are already generally distrusting of the United States' ability to keep its data safe, and failure to enact updated reforms by the United States threatens to further erode the EU's trust.[108] When considering both the advantages and disadvantages in enacting the GDPR, an analogous set of regulations in the United States would have comparable net positives on the country and the world.

The first advantage of the GDPR is the relevancy of data. The implementation of new regulations in the GDPR ensures accurate and up-to-date information of data subjects in the EU.[109] This can help businesses keep track of both current and potential customers as well as improve their own marketing efforts. Although it does require a frontloading of work and changes to data collection, retention, and sharing processes that are already deeply engrained within a company, the result will benefit entities in how they can communicate their products and services. The more precise the records are, the better a company can tailor its marketing efforts to segments of the population who will actually be interested in what the company offers. The existing data on data subjects allows companies to better target those consumers who would be the most likely purchasers of goods and services that the companies offer. Yet, the high up-front costs of compliance coupled with the previous lack of requirements are likely why companies have not already conformed.

Another benefit resulting from the implementation of the GDPR (and a subsequent adoption of similar regulations in the United States) is the

PM) (describing the lack of efforts within Congress to enact similar reforms), https://www.theregister.co.uk/2018/11/08/gdpr_usa_congressman.

[108] Angelique Carson, *Safe Harbor-Compliant Companies Seeking Contracts: Facing an Uphill Battle in the EU*, THE INT'L ASS'N OF PRIVACY PROF.: THE PRIVACY ADVISOR (May 20, 2014), https://iapp.org/news/a/safe-harbor-compliant-companies-seeking-contracts-facing-an-uphill-battle-i.

[109] Michael Fimin, *Five Benefits GDPR Compliance Will Bring to Your Business*, FORBES (Mar 29, 2018, 7:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/#3b530892482f.

increase in consumers' rights and restoration of trust in the corporate realm. With the massive amounts of data that companies can collect, and the chaos that could ensue without appropriate regulations, the GDPR reigns in and limits what kinds of data companies are allowed to collect and the manner in which they can do so.[110] Consumers have a right to control whose hands their data ends up in, and the GDPR recognizes this—as all data protection policies should in our new modernized world. In light of recent events, such as the Equifax data breach and Edward Snowden's National Security Agency leak, consumers rightly are demanding airtight protections.[111] However, if companies in the United States are outside the reach of the GDPR, these companies will not face sanctions that are as serious as if they violated the GDPR. But the GDPR, if implemented appropriately, should provide the necessary incentives to safeguard consumer data.

Within the benefits of boosting consumer protections, the implementation of similar GDPR standards in the United States can offer companies a competitive edge if the companies are able to jump quickly onto the bandwagon. With the accessibility of the Internet, consumers can easily create their own impressions of companies based upon what is happening in the news. Complying expeditiously with the GDPR's standards offers great reputational gains because companies show consumer protection is of their utmost priority. Consumers will put more trust in a company that does not rebel against these standards. On the other hand, companies that resist these kinds of regulations will not only suffer reputational harm at the outset of the GDPR's implementation, but also incur further injury when EU regulatory officials levy any fines or damages.

Although there are not yet enough statistics to determine the result of GDPR violations on a company's reputation, consumers are demanding more information and control over their own data. A study conducted by Columbia University determined that 86% of consumers would like to exercise more control over the data that companies hold about them and 85% of consumers want to know more information about data that data companies collect.[112] Furthermore, over 75% of consumers are more willing to share personal data with companies that they trust.[113] If companies can build a reputation of honesty and reliability, customers will be more likely to give those companies their data (along with their business) and have less skepticism and distrust about what is happening to that data.

A perk to implementing standards similar to the GDPR in the United

---

[110] *Id.*

[111] Preston Gralla, *Why GDPR Can Be—Gasp!—Good for Your Company*, HEWLETT PACKARD ENTERPRISE (Apr. 18, 2018), https://www.hpe.com/us/en/insights/articles/why-gdpr-can-be-gasp-good-for-your-company-1804.html.

[112] Todd Wright, *The GDPR – Is Reputation a Bigger Risk than Fines?*, SAS (Jan. 11, 2018), https://blogs.sas.com/content/datamanagement/2018/01/11/gdpr-reputation-bigger-risk-fines./.

[113] *Id.*

States is that many businesses will have already closely conformed to these regulations if they were previously in compliance with the GDPR. Since businesses with any sort of presence in the EU must have, by this time, already reformed their policies to obey the GDPR, it will be a much easier transition process in the United States than in the EU. Thus, adoption of new regulations in the United States would probably be the most successful at this point in time. Not only would it be a more efficient adjustment process, adoption would further the goal of uniformity and change with the digital age. The policies in the United States as of now have much catching up to do with the new standards set forth in the GDPR. By not having similar protections in the United States, the United States stunts any growth in the data transfer realm with the EU since the EU was already distrusting of the United States' regulations before it instituted the GDPR.[114] The lopsidedness of the United States' and EU's regulations diminish synergies between a once strong ally of the United States in data growth and globalization.

Finally, the GDPR makes sense from a public policy perspective. The GDPR impacts some but not all companies in the United States, which leads to slanted policies in the data industry. For example, a consumer in the United States may have his data treated with greater protections and safeguards at one company that must comply with the GDPR and come to expect that kind of treatment at other companies. That consumer may be disappointed to discover that they have a completely different set of rights with respect to other companies that do not need to comply with the GDPR. This incongruity in data treatment will lead to confusion by the consumer in what he can expect to happen to his data unless the consumer is quite up to date on current events in privacy regulations. Requiring the consumer to educate himself about the kinds of protections each company that collects his data offers is a high burden to put on the everyday person visiting many websites each day. Instead, the much more efficient option would be to re-harmonize data protection law in the United States with GDPR's more comprehensive, modern regulations.

B. Potential Drawbacks of Regulations Similar to the GDPR in the United States

While there are many benefits of the GDPR, it is not without its drawbacks. The GDPR as it is enacted now acts as a "nontariff barrier" between the United States and the EU.[115] A nontariff barrier occurs when "one country has a higher standard than the other."[116] This makes the transfer of data, goods, or services more difficult between the two countries.[117] In the short term, and possibly until the United States updates its data standards to

[114] McAllister, *supra* note 9, at 188.
[115] Burri & Schär, *supra* note 56, at 499.
[116] *Id.*
[117] *Id.*

gain the EU's approval, the economies of the United States and the EU will likely suffer because of the lopsided regulations.[118] The United States and the EU should therefore begin working together to establish GDPR-like standards in the United States so that the EU will reopen the lines through which data is transferred across the Atlantic.

Another drawback of the GDPR is one that comes with almost any kind of reform: the difficulties of educating the masses about the change. Considering the GDPR's sweeping reach across the globe, it will be incredibly tough to ensure that everyone who should be compliant actually is compliant. While large international companies have probably been following the GDPR's proposal and enactment, smaller businesses may not have that same awareness. Once the GDPR became effective in May, these businesses may not have even begun the process of reforming their data protection policies simply because they were not conscious of the changes. A study in Ireland revealed that in organizations with an average of 800 employees, 63% of the financial decision makers were unaware of the new policies and requirements under the GDPR.[119] This unawareness could lead to huge fines imparted on these companies that, for smaller businesses, are simply not sustainable for them to continue operations.

The struggles applying more heavily to mid-sized and smaller companies are relevant not just in awareness of the GDPR regulations, but also in those companies' abilities to revamp their software systems. The changes demanded by the GDPR are quite extensive and are not simple enough to comply with overnight, and instead use up substantial amounts of resources. The GDPR will require data processors at companies to reexamine their approaches to product design and overall operations.[120] If companies do not—or *cannot*—comply, they must either shut out any potential customer base in the EU or risk huge fines and penalties for noncompliance.[121]

While there are no blanket exemptions for smaller businesses under the GDPR, there are many resources available to assist these kinds of companies in becoming compliant.[122] For example, quite a few blog posts online are devoted to advising small businesses on what they should be doing under the new GDPR standards.[123] These tips include, first, understanding the kinds of data the business is processing, reviewing security measures, and making

---

[118] *Id.* at 500.

[119] Charlie Taylor, *CFOs in the Dark on Data Rules Despite Approving Investments*, THE IRISH TIMES (Nov. 17, 2016, 6:30), https://www.irishtimes.com/business/technology/cfos-in-the-dark-on-data-rules-despite-approving-investments-1.2870270.

[120] McAllister, *supra* note 9, at 187.

[121] *Id.*

[122] Phil Nicolosi, *Are There GDPR Exemptions For U.S. Small Businesses?*, PHIL NICOLOSI, https://www.internetlegalattorney.com/are-there-gdpr-exemptions-for-u-s-small-businesses./.

[123] *See GDPR for Small Businesses*, COMPLIANCE JUNCTION, https://www.compliance junction.com/gdpr-for-small-business./.

consent clear and transparent.[124] Even though this still may be an intricate and time-intensive process—more so for smaller businesses—there are many ways for companies to understand and update their policies in order to become compliant with the GDPR. Once this initial hurdle is cleared, the impact of these regulations will make data processing not only safer for consumers, but also easier and more informative for the companies themselves.

Many of these benefits and drawbacks to the GDPR hinge on whether it will be followed and enforced by those it intends to impact. In January 2019, Google was slapped with a €50 million fine for violating the GDPR, the largest GDPR fine at the time.[125] Two French interest groups filed complaints against Google on the day the GDPR came into effect.[126] The Commission Nationale de l'Informatique et des Libertés (CNIL), a French data regulator, fined Google on January 21, 2019 for "a breach of the EU's data protection rules, in particular for lack of transparency, inadequate information provided to data subjects/users and lack of valid consent regarding ad personalisation [sic]."[127] Of the over 200,000 violations reported in 2018, the total fines amounted to €56 million, including Google's €50 million fine.[128] This reflects the Information Commissioner's Office's (ICO) understanding of the transitory period occurring for legislatures and companies alike, as well as allowing the ICO time to manage the influx of cases.[129]

However, more recent fines show that regulators are ready to more aggressively apply the GDPR, starting with tech behemoth Google and continuing to hit the technology sector with force. Google's fine was followed by a €183 million fine for British Airways and a proposed €99 million fine for Marriott International for the leaking and exposure of personal data.[130] These fines set the tone clearly for many other businesses and likely will lead them to clean up their private policies instead of waiting for the other shoe to drop.

Yet, an issue that is still murky even after this fine is which regulator has jurisdiction over each case. Google, in response to its January fine,

---

[124] Bret Piatt, *What Small Business Owners Should Know About GDPR and Why*, CSO (May 2, 2018, 9:00 AM), https://www.csoonline.com/article/3269578/what-small-business-owners-should-know-about-gdpr-and-why.html.

[125] Philip Lee, *Google Hit with Record €50 Million GDPR Fine*, LEXOLOGY (Jan. 25, 2019), https://www.lexology.com/library/detail.aspx?g=ae5b0e20-5158-40f5-bb4c-a84c1162f223.

[126] *Id.*

[127] *Id.*

[128] Srikanth, *Record-Setting GDPR Fines in 2019*, TECHIEXPERT (Sept. 6, 2019), https://www.techiexpert.com/record-setting-gdpr-fines-in-2019./.

[129] *Id.*

[130] Jessica Davies, '*2019 is the Year of Enforcement': GDPR Fines Have Begun*, DIGIDAY (July 11, 2019), https://digiday.com/media/2019-is-the-year-of-enforcement-gdpr-fines-have-begun./.

argued that only Irish regulators had the power to dole out fines because its European headquarters are located in Dublin.[131] However, under Article 4(16) of the GDPR, jurisdiction is in a company's central place of administration unless the decision-making concerning the relevant data processing takes place in another place in the EU.[132] Along with CNIL's fine, its decision noted that Google's headquarters in Ireland did not have the requisite decision-making power when it came to the relevant data processing.[133] Because CNIL did not view the Irish headquarters as Google's central place of administration, and no other lead authority had jurisdiction, it deemed itself competent to handle the matter.[134] Google plans to appeal this decision.[135]

This decision has left people with more questions than answers. The GDPR has a territorial scope previously unseen in data privacy regulations. Just over a year into its enactment, the world is still guessing what the outcome will be. There is great potential should the policies work out just as they were intended. However, there are many hurdles and barriers to achieve this optimal outcome.[136] At this point in time, companies, consumers, and officials are left wondering whether the GDPR will truly be the future of data privacy protection while at the same time hoping not to be the litmus test under the enforcement mechanisms.[137]

Since the GDPR was enacted only recently enacted, there has not been much to report as to its progress and effectiveness. In Februray 2018, before the GDPR was enacted, the Federation of Small Businesses (FSB) estimated that about 90% of small firms were not compliant with the impending GDPR regulations.[138] As of late June 2018, a month after when the GDPR was enacted, the FSB revealed that upwards of 5.7 million small businesses were still not compliant with the GDPR that should be compliant; thus, the actual enactment of the GDPR did not cause many companies to become compliant even after the GDPR took effect.[139] However, the GDPR enforcement bodies have been understanding, recognizing that it takes time and resources for companies to update their policies to conform with the new regulation. The

---

131 Lee, *supra* note 125.

132 General Data Protection Regulation, 2016 O.J. (L 119) 1, 41-42.

133 Lee, *supra* note 125.

134 *Id.*

135 *Id.*

136 *Complying with the General Data Protection Regulation (GDPR)*, STIBBE, https://www.stibbe.com/en/expertise/practiceareas/data-protection/general-data-protection-regulation/what-are-the-challenges (last accessed Jan 13, 2020).

137 George Anadotis, *GDPR in Real Life: Fear, Uncertainty, and Doubt*, ZDNET (May 18, 2018, 2:37 PM), https://www.zdnet.com/article/gdpr-in-real-life-fear-uncertainty-and-doubt./.

138 GDPR Report, *GDPR: What Next?*, PRIVSEC REP. (June 20, 2018), https://gdpr.report/news/2018/06/20/gdpr-what-next.

139 *Id.*

ICO took on a mostly-advisory role for the first year of the GDPR's enactment instead of harshly penalizing companies.[140] This gave all businesses, especially smaller businesses, the chance to get up to speed with compliance efforts and not operate in fear of fines and penalties. However, as evidenced by Google's fine in early 2019, the ICO either changed its tune about that advisory role or wanted to make an example out of larger companies in the hopes that others would fall into step in terms of GDPR compliance.

In the future, many companies may choose to over-share rather than risk not sharing enough and being fined or penalized for noncompliance. Many web users have seen the pop-up windows asking for consent to collect cookies before browsing on a website or additional checkboxes before a consumer signs up for a new email subscription. Do not be surprised to see an increase in data breach notifications either. It is easy to see why companies would rather disclose too much than too little when the consequences under the GDPR are so harsh. Companies stand to lose revenue as well as endure reputational damage should they breach the GDPR.

While the implementation of the GDPR has been a learning process for all, the initial fear has dissipated over the first few months of its enactment and has been replaced by policy changes that work towards compliance.[141] However, it is clear that the EU is taking this regulatory policy seriously. Although not without its drawbacks, the GDPR should have long lasting, net positive impacts. If the changes work as planned, the GDPR will create sweeping benefits across the globe both for companies and consumers. But for now, companies should continue working towards compliance and consumers should keep abreast of any changes that will impact their rights under the GDPR. The United States would benefit by staying tapped into the performance of the GDPR in the EU as well, and hopefully will start planning similar regulations of its own.

V. CONCLUSION

The enactment of the GDPR has already resulted in some changes within the United States. California has been a trailblazer when it comes to data protection laws, and just a few months after the GDPR went into effect it also passed its own similar regulations.[142] In late June of 2018, California passed a digital privacy law that became effective in January 2020.[143] The new regulations are similar to a less-restrictive GDPR, giving residents of

[140] *Id.*

[141] Rob Sobers, *The Average Reading Level of a Private Policy*, VARONIS (July 11, 2018), https://www.varonis.com/blog/gdpr-privacy-policy./.

[142] George P. Slefo, *Marketers and Tech Companies Confront California's Version of GDPR*, ADAGE (June 29, 2018), https://adage.com/article/digital/california-passed-version-gdpr/314079./.

[143] Cal. Consumer Privacy Act of 2018 §§ 1798.100 - 1798.199 (2018); *see also* Slefo, *supra* note 142.

California the power to know what data companies are collecting, why they are collecting it, and with whom they are sharing that data.[144] Consumers can also tell companies to delete their data, not share their data, or not sell their data, as well as have the ability to opt out of a company's terms and services but still have access to the company's offerings.[145] In terms of an enforcement mechanism, consumers are able to seek damages of up to $750 for each individual violation to the new regulations, while the Attorney General can sue violators for up to $7,500 for each individual infraction.[146]

While it is possible for companies to isolate those California residents and only apply protections to them, the question is whether companies will simply recognized these rights as applying to all consumers, in the EU and beyond. It is not very feasible for companies to target consumers so granularly, but it would not be a surprise if companies resisted GDPR-like regulations for as long as they possibly can. As of now, California is the only U.S. state with these stringent regulations in place. However, if more states imitate California's new privacy laws, companies may not have a choice to pick and choose to whom they extend these additional rights. While there is not much national momentum pushing forward new federal data protection rights for consumers, if enough states enact their own reforms it may be necessary to unite the regulations under one federal law. If the GDPR does end up being an effective way to safeguard consumer data in the EU, it is not farfetched to believe consumers in the United States will come together and demand similar protections here.

Part of the reason why the United States has not yet acted is because the desires of large tech companies are so different from the desires of Congress, and the tech companies are able to exert much power and influence because of their tight control on the economy. In late September 2018, six tech companies discussed federal privacy laws with the Senate Committee on Commerce, Science, and Transportation.[147] There were representatives from AT&T, Amazon, Google, Apple, Twitter, and Charter Communications; all of these companies were lobbying for comprehensive federal data privacy legislation that would pre-empt state laws, promote privacy "on their own terms," and prevent the United States from enacting another GDPR.[148] The tech companies argued that the GDPR was far too strict of a measure, expensive even for their own standards, and infeasible for smaller companies. The only agreement between the lobbyists and Senate from the discussion came from the representative at Charter Communications, who was in favor

[144] Slefo, *supra* note 142.

[145] *Id.*

[146] *Id.*

[147] Alfred Ng, *Tech Companies Really Don't Want a US Version of Europe's Privacy Law*, CNET (Sept. 26, 2018, 11:39 AM), https://www.cnet.com/news/tech-companies-really-dont-want-a-us-version-of-europes-privacy-law./.

[148] *Id.*

of the opt-in consent portion of the GDPR.[149] No other point went uncontested by the other representatives.[150]

On the other side of the discussion table, many senators did not agree with the tech companies.[151] They argued that many companies are already compliant under the GDPR—including the tech companies that had come before the Senate Committee—and that applying the same regulations across the nation would not be a far stretch.[152] Additionally, Congress did not think federal legislation would be helpful layered on top of fifty other state laws; instead, they suggested one single privacy framework, just as the GDPR has done in the EU.[153] Ultimately, Congress felt that the laws in California were headed in the right direction,[154] and replacing the California law with that proposed by the tech companies would be a step backwards for the United States.

Ultimately, this back-and-forth between companies and legislatures is likely to continue in the immediate future. Yet, it is important for the United States to begin exploring the implications of similar, GDPR-type reforms. In its early months of implementation, the GDPR has had and will continue to have sweeping benefits for both consumers and companies, and it would be wise for the United States to piggyback on the EU's likely continued success.

[149] *Id.*
[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] *Id.*
[154] *Id.*