MIND YOUR BUSINESSES: WHY GEORGIA COMPANIES SHOULD WORRY ABOUT EUROPEAN PRIVACY LAW

Emily Elizabeth Seaton[*]

TABLE OF CONTENTS

[*]J.D. Candidate, University of Georgia School of Law, 2019, B.S. in Economics, Wofford College, 2016.

I. INTRODUCTION

As society becomes increasingly dependent on technology, the issue of data privacy presents a serious concern. With the widespread use of the Internet, companies can easily expand their businesses across borders. As a result, transnational transfers of data are commonplace for many businesses; customers can now be located anywhere in the world.

Many businesses in the United States can no longer relax once they are compliant with local data privacy laws, because other countries' interests are implicated by the collection and use of their citizens' personal data. Thus, companies are left with a laundry list of applicable data privacy laws that may vary in scope and in purpose. Recent legislation will affect the ways in which companies in the United States collect and use personal data from non-citizens as well as the consequences for mishandling such data.

This Note will focus on the intersection of the European Union's recently implemented General Data Protection Regulation and the previously established EU-U.S. Privacy Shield, which governs the flow of personal data from the European Union to the United States. This Note will further address the legal implications for Georgia businesses that collect and use the personal data of EU citizens, as those businesses must also comply with Georgia-specific data privacy laws.

II. BACKGROUND

A. Overview of U.S. Data Privacy Laws

1. Federal Regulation

There is no single, comprehensive federal law that regulates the collection and use of personal data in the United States.[1] Rather, there is a patchwork of laws regulating data privacy for different types of information.[2] Federal laws regulating data privacy in the United States include: the Federal Trade Commission Act (prohibiting unfair and deceptive practices), the Children's Online Privacy Protection Act (policing the online collection and use of children's data), the Gramm-Leach-Bliley Act (governing the collection, use, and disclosure of financial information), the Health Insurance Portability and Accountability Act (regulating medical and health information), the Fair Credit Reporting Act (regulating use of consumer reports), the Controlling the Assault of Non-Solicited Pornography and Marketing Act (regulating collection and use of e-mail addresses), the Telephone Consumer Protection

---

[1] Ieuan Joly, Data Protection in the United States: Overview, Practical Law, Resource ID 6-502-0467 (July 1, 2018).

[2] *Id.*

Act (regulating collection and use of telephone numbers), and the Electronic Communications Privacy Act.[3]

2. State Regulation

Many state laws regulate the collection and use of personal data.[4] As of March 2018, all fifty states have enacted security breach notification laws.[5] Under Georgia law,

> [a]ny information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of [Georgia] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[6]

The Code defines a breach of the security of the system as the "unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector."[7] The law further requires the notice to be made "in the most expedient time possible and without unreasonable delay."[8] An information broker or data collector could be subject to civil penalties for violating the Georgia data breach notification law.[9]

3. Common Law

The common law in the United States regarding privacy may also work to regulate the collection and use of consumer data. The Restatement (Second) of Torts recognizes four common law privacy torts: unreasonable intrusion upon the seclusion of another, appropriation of the other's name or likeness, unreasonable publicity given to the other's private life, and publicity

---

[3] *Id.*

[4] *Id.*

[5] Nat'l Conference of State Legislatures, *2018 Security Breach Legislation* (Oct. 12, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx.

[6] GA. CODE ANN. § 10-1-912(a) (2017).

[7] GA. CODE ANN. § 10-1-911(1) (2017).

[8] GA. CODE ANN. § 10-1-912(a) (2017).

[9] Davis Wright Tremaine LLP, *Data Breach Notification Summary*, https://www.dwt.com/files/Uploads/Documents/Publications/State%20Statuets/BreachNoticeSummaries.pdf (last updated Mar. 26, 2018).

that unreasonably places the other in a false light before the public.[10] In addition, the common law tort of negligence may also be invoked in the information privacy context.[11] The comments to the Restatement explain that Georgia was the first state to explicitly recognize the right to privacy.[12] Now, most states recognize the common law right to privacy.[13]

B. Overview of EU Data Privacy Laws

1. Privacy as a Fundamental Right

Unlike the United States, the European Union recognizes privacy as a fundamental right.[14] This classification of the right to privacy can help explain the more stringent data privacy laws of the European Union compared to those of the United States.

2. 1995 Data Protection Directive

The European Union's first major move regarding data privacy was its 1995 Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive).[15] The Data Protection Directive attempted to regulate the processing of personal data within the European Union. However, since it was merely a directive and not a blanket regulation, its application varied from state to state within the European Union.[16] Further, the Internet had only been in existence for a short time and was not widely used when the European Union adopted the Data Protection Directive in 1995; therefore, an update was long overdue.[17]

---

[10] Restatement (Second) of Torts § 652A (AM. LAW INST. 1977).

[11] *See* Paul M. Schwartz & Daniel J. Solove, *Reworking Information Privacy Law: A Memorandum Regarding Future ALI Projects About Information Privacy Law* 1, 22 (Aug. 2012), DUKE L., https://law.duke.edu/sites/default/files/images/centers/judicialstudies/Reworking_Info_Privacy_Law.pdf.

[12] Restatement (Second) of Torts § 652A cmt. a (AM. LAW INST. 1977); Pavesich v. New England Life Ins. Co., 50 S.E. 68 (1905).

[13] Restatement (Second) of Torts § 652A cmt. a (AM. LAW INST. 1977).

[14] 2010 O.J. (C 326) 397.

[15] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

[16] *See Online Privacy Law: European Union*, LIBR. OF CONGRESS, https://www.loc.gov/law/help/online-privacy-law/2017/eu.php (last updated May 28, 2018).

[17] *See id.*

3. General Data Protection Regulation

In April 2016, the EU Parliament approved the General Data Protection Regulation (GDPR).[18] The GDPR went into effect in May 2018 and replaced the Data Protection Directive.[19] One key difference between the Data Protection Directive and the GDPR is that the GDPR is a *regulation*; therefore, the law will directly apply to all EU member states without the need for implementing legislation.[20]

a. Definition of Personal Data

The GDPR expands the definition of personal data.[21] In addition to "a person's name, photo, email address, phone number, address, or any personal identification number (social security, bank account, etc.)," the GDPR covers "things like IP addresses, mobile device identifiers, geo-location, and biometric data (finger prints, retina scans, etc.)" as well as "an individual's physical, psychological, genetic, mental, economic, cultural, or social identity."[22] This broader definition of personal data will require covered entities to significantly increase their data protection efforts.

b. Data Subjects' Rights

The GDPR includes three main provisions regarding individuals' rights relating to the collection and use of their personal data: consent, the right to access their personal data, and the right to be forgotten.[23] To process an individual's personal data, the entity must get "freely given, specific, informed and unambiguous" consent from the individual.[24] In addition, entities are required to update their terms and conditions agreements so that they are more easily understood by laypeople.[25]

---

[18] Trunomi, *The Process: Timeline of Events*, https://eugdpr.org/the-process/timeline-of-events/ (last visited Oct. 1, 2018).

[19] *Id.*

[20] *See* Allen & Overy, *Preparing for the General Data Protection Regulation* 8 (Jan. 2018), http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf.

[21] SeeUnity, *The Main Differences Between the DPD and the GDPR and How to Address Those Moving Forward*, BRIT. LEGAL TECH. F., https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf (last visited Oct. 1, 2018).

[22] *Id.*

[23] *Id.*

[24] Allen & Overy, *supra* note 20, at 12.

[25] *See* Trunomi, *GDPR Key Changes*, http://www.eugdpr.org/key-changes.html (last visited Oct. 1, 2018) [hereinafter *GDPR Key Changes*] ("[C]ompanies are no longer able

The GDPR also gives individuals the right to find out whether their personal data is being processed, where it is being processed, and for what purpose it is being processed.[26] Further, individuals may obtain an electronic copy of their personal data from the data controller, free of charge.[27] Finally, individuals have the right to have their personal data erased at their request (the "right to be forgotten" or the "right to erasure") if they withdraw their consent and there is no other legal ground for processing their personal data.[28]

c. Data Controllers and Data Processors

Data controllers are "the natural legal person, public authority, agency or other body, which determines the purposes and means of the processing of personal data."[29] Data processors are "the natural legal person, public authority, agency or other body, which processes data on behalf of the controller."[30] Data processors were not included under the Data Protection Directive; however, under the GDPR, they too are responsible for the security of personal data.[31] Both data controllers and data processors must designate a data protection officer if their core activities involve "regular and systematic monitoring of data subjects on a large scale."[32] Data controllers and data processors must also document their data protection policies and their data processing activities, unless the data controller or data processor has less than 250 employees.[33]

d. Privacy by Design

The "privacy by design" provision of the GDPR requires data controllers to implement GDPR compliance into the business from the very beginning rather than adding compliance mechanisms after the product or service has already been created.[34] In addition, data controllers may collect and use only the minimum necessary data, and access to that data must be limited to necessary persons.[35]

---

to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form . . . .").

[26] *Id.*

[27] *Id.*

[28] Allen & Overy, *supra* note 20, at 20.

[29] SeeUnity, *supra* note 21.

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *GDPR Key Changes*, *supra* note 25.

e. Breach Notification

In the event of a data breach, data controllers must notify the supervisory authority within seventy-two hours of learning of the breach.[36] The notification must provide details regarding the nature of the breach and give an estimate of the number of people affected.[37] In addition, the notification must include the data protection officer's contact information, a description of the likely consequences of the breach, and a list of mitigating steps the data controller has taken thus far.[38] Data processors must notify data controllers of any breach "without undue delay."[39]

f. Penalties

The GDPR takes a tiered approach to fines for violations.[40] The highest fines for the most serious violations will be 4% of the company's annual global turnover or 20 million Euros, whichever is greater.[41] These penalties apply equally to both data controllers and data processors.[42]

g. Scope

The scope of the GDPR reaches well beyond the twenty-eight EU member states. The GDPR will apply to an organization if any one of three tests is met: the "establishment" test, the "goods and services" test, or the "monitoring" test.[43] Under the establishment test, an organization will be subject to the GDPR if it is established in the European Union and "processes personal data in the context of the activities of that establishment."[44] Under the goods and services and monitoring tests, the GDPR will apply to a controller or processor not established in the European Union "if it processes data about individuals who are in the EU and the processing relates to either: the offering of goods or services to data subjects who are in the EU; or monitoring their [behavior], where that [behavior] takes place in the EU."[45] Therefore, the GDPR (and its potentially harsh penalties) will apply to many companies in the United States.

---

[36] SeeUnity, *supra* note 21.
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *GDPR Key Changes*, *supra* note 25.
[41] *Id.*
[42] *Id.*
[43] Allen & Overy, *supra* note 20, at 5.
[44] *Id.*
[45] *Id.*

C. International Safe Harbor Privacy Principles

1. Overview

The European Union's adoption of the Data Privacy Directive in 1995 created a stark contrast between data privacy in the United States and the European Union, which threatened the transfer of personal data between the two and gave rise to concern regarding their trade and investment relationship.[46] In response, the U.S. Department of Commerce issued, and the European Commission recognized, the Safe Harbor Privacy Principles (Safe Harbor) in 2000.[47] Safe Harbor essentially created a self-certification mechanism to bring U.S. companies into compliance with the European Union's Data Protection Directive. Safe Harbor consisted of seven basic principles: notice, choice, onward transfer, security, data integrity, access, and enforcement.[48] Any company subject to regulation by the Federal Trade Commission (FTC) was eligible for safe harbor; this did not include financial firms or telecommunications carriers.[49]

2. Schrems v. Data Protection Commissioner

In October 2015, the European Court of Justice issued a decision that immediately invalidated its decision to recognize Safe Harbor.[50] The Court determined that the Data Protection Directive required the European Commission to examine the laws of a country outside the European Union *prior to* making a determination regarding the adequacy of their data privacy protection.[51] Therefore, the self-certification and FTC oversight of Safe Harbor were insufficient.

D. EU-U.S. Privacy Shield

1. Overview

In February 2016, in response to the disparities between U.S. and EU data privacy law that once again prevailed after Safe Harbor was struck down in *Schrems v. Data Protection Commissioner*, the United States and the

---

[46] Martin A. Weiss & Kristin Archick, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, CONG. RES. SERV. 5 (May 19, 2016), https://fas.org/sgp/crs/misc/R44257.pdf.

[47] *Id.*

[48] *Id.* at 5–6.

[49] *Id.* at 6.

[50] Weiss & Archick, *supra* note 46, at 6; Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 00000.

[51] Weiss & Archick, *supra* note 46, at 6–7.

European Union released a new agreement: the EU-U.S. Privacy Shield (Privacy Shield).[52] The purpose of the agreement is to protect "the fundamental rights of anyone in the European Union whose personal data is transferred to the United States," as well as to "[bring] legal clarity for businesses relying on transatlantic data transfers."[53] The decision of an organization based in the United States to join the Privacy Shield is wholly voluntary.[54] However, such a commitment, once made through self-certification, is enforceable under U.S. law.[55]

2. Provisions

The Privacy Shield framework is centered around seven core principles: notice; choice; accountability for onward transfer; security; data integrity and purpose limitation; access; and recourse, enforcement, and liability.[56] The key provisions include informing individuals about data processing; providing free and accessible dispute resolution; cooperating with the Department of Commerce; maintaining data integrity and purpose limitation; ensuring accountability for data transferred to third parties; maintaining transparency related to enforcement actions; and ensuring that commitments are kept as long as the data is held, even if the organization leaves the Privacy Shield.[57]

3. The Judicial Redress Act of 2015

The Judicial Redress Act of 2015 extends portions of the Privacy Act of 1974 to certain foreign persons not typically protected by U.S. laws.[58] The Department of Justice explains it thus:

---

[52] *Id.* at 9.

[53] *The EU-U.S. Privacy Shield*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en (last visited Oct. 1, 2018).

[54] Int'l Trade Admin., *Privacy Shield Program Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview (last visited Oct. 2, 2018) [hereinafter *Privacy Shield Program Overview*].

[55] *Id.*

[56] Int'l Trade Admin., *Privacy Shield Framework*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/EU-US-Framework (last visited Oct. 2, 2018).

[57] Int'l Trade Admin., *EU-U.S. Privacy Shield Framework: Key New Requirements for Participating Companies*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Key-New-Requirements (last visited Nov. 2, 2017).

[58] The U.S. Dep't of Justice, *Judicial Redress Act of 2015*, https://www.justice.gov/opcl/judicial-redress-act-2015 (last updated Jan. 26, 2017) [hereinafter *Judicial Redress Act of 2015*].

> [T]he Judicial Redress Act enables a "covered person" to bring suit in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an "individual" (*i.e.*, a U.S. citizen or permanent resident alien) may bring and obtain with respect to the: 1) intentional or willful unlawful disclosure of a covered record . . . and 2) improper refusal to grant access to or amendment of a covered record . . . .[59]

A "covered person" is defined as a natural person who is a citizen of a "covered country."[60] In January 2017, the U.S. Attorney General designated as "covered countries" the entire European Union.[61] This designation means that the Privacy Shield provisions can be enforced domestically, even if the consumer involved is not a U.S. citizen.

III. ANALYSIS

A. How Will the GDRP and Privacy Shield Work Together?

The GDPR and the Privacy Shield are two fundamentally different privacy frameworks: the former is a binding regulation, while the latter is a voluntary agreement. However, companies based in the United States could find themselves trying to comply with both, which raises the question: How will they work together?[62]

Some sources explain the intersection of the two frameworks by positing that the Privacy Shield is a way for the European Union to ensure that U.S. organizations utilizing the personal data of EU citizens are compliant with the GDPR.[63] However, the GDPR requirements are notably stricter than those of the Privacy Shield. Therefore, while a company joining the Privacy Shield might give the European Union a little more faith in the company's privacy practices, an organization falling under the control of the GDPR still must ensure that GDPR requirements are met, regardless of whether that organization has opted to join the Privacy Shield.

---

[59] *Id.*

[60] *Id.*

[61] *Judicial Redress Act of 2015*, *supra* note 58; OFFICE OF THE ATTORNEY GEN.; U.S. DEP'T OF JUSTICE, NOTICE OF DESIGNATION BY THE ATTORNEY GENERAL OF "COVERED COUNTRIES" AND "DESIGNATED FEDERAL AGENCIES OR COMPONENTS", 82 Fed. Reg. 7860 (Jan. 23, 2017).

[62] *See* Alex Fugairon, *How the GDPR and Privacy Shield Regulations Relate — and What They Mean for Your Business*, PIVOT POINT SECURITY (July 13, 2017), https://www.pivotpointsecurity.com/blog/gdpr-privacy-shield-regulations/.

[63] *See id.*; *and GDPR vs. Privacy Shield*, PRIVACYTRUST, https://www.privacytrust.com/privacyshield/gdpr-vs-privacy-shield.html (last visited Oct. 2, 2018).

1. Definition of Personal Data

As previously mentioned, the GDPR defines "personal data" extremely broadly,[64] while the Privacy Shield defines it as "data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form."[65] The Privacy Shield definition of personal data references the Data Protection Directive, which has been repealed and replaced by the GDPR.[66] Understanding what qualifies as personal data is at the core of both GDPR and Privacy Shield compliance; therefore, the Privacy Shield must be updated to bring more clarity to its members. Until then, the best practice seems to be to use the stricter GDPR definition of personal data.

2. Penalties

The GDPR's potentially grave penalties comprise the most extreme provision of the new regulation. While the GDPR is very specific in detailing the possible sanctions for noncompliance, the Privacy Shield is decidedly vague:

> Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles . . . . Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances. Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards.[67]

While Privacy Shield sanctions might not be severe, GDPR penalties could be the death of a company. As such, it is in the financial interest of Privacy Shield members to ensure that they are GDPR compliant as well.

---

[64] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 33 (EC).

[65] Int'l Trade Admin., *EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, PRIVACY SHIELD FRAMEWORK (2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [hereinafter *Privacy Shield*].

[66] *See* Int'l Trade Admin., *Privacy Shield Framework: Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=OVERVIEW (last visited Oct. 1, 2018).

[67] *Privacy Shield*, *supra* note 65 (footnote omitted).

3. Data Subjects' Rights

As previously discussed, data subjects have three major rights under the GDPR: the right to give consent before their personal data is collected or used, the right to access their personal data, and the right to be forgotten (the right to have their personal data erased).[68] Under the Privacy Shield, the right to access personal data and the right to be forgotten do not exist.[69] It does include the right to consent, but only for "sensitive information," which is defined as "personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual."[70] Since May 2018, Privacy Shield members must ensure that they are obtaining consent for much more than the collection of sensitive information, or they could fall victim to GDPR penalties.

4. Implementation

Recall that the GDPR requires data controllers to implement its provisions from the very beginning of the business (privacy by design).[71] The Privacy Shield, on the other hand, lacks such a requirement.[72] The Privacy Shield does, however, contain a provision requiring implementation generally.[73] Since the GDPR has been enacted, businesses intending to collect and use the personal data of EU citizens are no longer able to hold off on establishing personal data security measures, even though the Privacy Shield does not require immediate implementation.

5. Breach Notification

While the GDPR requires notification of a data breach to be made to the relevant supervisory authority within seventy-two hours,[74] the Privacy Shield

---

[68] SeeUnity, *supra* note 21.

[69] *See Privacy Shield*, *supra* note 65.

[70] *Id.*

[71] *See* SeeUnity, *supra* note 21.

[72] *See Privacy Shield*, *supra* note 65.

[73] *See id.*

> In order to enter the Privacy Shield, an organization must . . . fully implement [the Principles]. An organization's failure to comply is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts.

Id.

[74] SeeUnity, *supra* note 21.

contains no such requirement.[75] The Privacy Shield Principles are silent as to any breach notification requirements.[76] This is perhaps the largest discrepancy between the GDPR and the Privacy Shield—and one that could cost a company a significant amount of money if it assumed that compliance with the Privacy Shield meant compliance with the GDPR.

6. Scope

Because the GDPR is a regulation, companies are required to comply if they collect and use the personal data of EU citizens.[77] On the other hand, a U.S. company bringing itself within the ambit of the Privacy Shield is completely voluntary.[78] While some contend that joining the Privacy Shield is a way to achieve GDPR compliance,[79] others suggest that foregoing the Privacy Shield altogether and focusing on GDPR compliance might be best:

> [D]espite possible preparations being made for compliance with the Privacy Shield, some commentators say that "[organizations] shouldn't be overly distracted by Privacy Shield, as there are far more significant changes on the horizon for [organizations] processing personal information," such as implementing changes required for compliance with provisions of the GDPR by 2018. [C]ompanies in the United States subjected to the GDPR have a lot for which to prepare. This makes it necessary for companies to keep the requirements of the GDPR in perspective when weighing whether to pursue the Privacy Shield.[80]

7. Potential Privacy Shield Updates

While the Privacy Shield does not currently live up to the GDPR, that is not to say that it never will; the EU Commission reviews the Privacy Shield

---

[75] *See Privacy Shield*, *supra* note 65.

[76] *See id.*

[77] *See* Allen & Overy, *supra* note 20, at 8.

[78] *See Privacy Shield Program Overview*, *supra* note 54.

[79] *See* Fugairon, *supra* note 62; *and GDPR vs. Privacy Shield*, *supra* note 63.

[80] Sherri J. Deckelboim, *Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying the EU-U.S. Privacy Shield Framework and How the Framework Will Impact Privacy Advocates, National Security, and Businesses*, 48 GEO. J. INT'L L. 263, 295–96 (2016) (quoting Mark Thompson & Ewan Donald, *Privacy Shield: What to Expect and Why Businesses Must Act Now*, COMPUTER BUS. REV. (Mar. 22, 2016), http://www.cbronline.com/blogs/cbr-rolling-blog/privacy-shield-what-to-expect-and-why-businesses-must-act-now).

annually for adequacy.[81] Despite requests that they ensure the Privacy Shield reflects the GDPR,[82] the EU Commission deemed the Privacy Shield adequate in its first annual review in October 2017.[83] With the GDPR having gone into effect in May 2018, the EU Commission will likely feel even more pressure at the next annual review to align the Privacy Shield framework with the GDPR. In the meantime, U.S. companies may want to focus their resources on GDPR compliance and opt out of joining the Privacy Shield, since being a part of it will no longer ensure compliance with the European Union's personal data security requirements.

B. Legal Implications for Georgia Businesses

While the Privacy Shield is less strict than the GDPR, Georgia data protection law pales in comparison to even the Privacy Shield; Georgia law is extremely lax compared to the GDPR. Because the United States views privacy differently than the European Union, personal data protection is not a high priority for many states. The *only* statutory law in Georgia regarding protection of consumers' personal data is found in title 10, chapter 1, section 912 of the Code of Georgia, requiring notification of a breach to be made quickly and without unreasonable delay. While such a vague time frame could mean weeks or months, as of May 2018, "quickly and without unreasonable delay" means within seventy-two hours of learning of the breach if that breach involves the personal data of EU citizens.

Most notably, the Georgia data breach notification law is silent as to enforcement, and case law citing the statute is sparse.[84] Therefore, Georgia businesses might be aware of the statute yet choose not to comply with it. In practice, many Georgia businesses are likely nowhere near GDPR compliance.

IV. CONCLUSION

Given the weighty potential penalties under the GDPR, Georgia companies conducting business in the European Union—intentionally or unintentionally—must ensure they are complying with more than Georgia

---

[81] *See* European Comm'n, *First Annual Review of the EU-U.S. Privacy Shield* (Oct. 18, 2017), http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619.

[82] Shehana Cameron Perera & Nikita Saini, *Privacy Shield Updates*, LEXOLOGY (June 22, 2017), https://www.lexology.com/library/detail.aspx?g=98c72bcb-2df2-44af-be59-a298255c0d6c.

[83] Hunton Andrews Kurth LLP, *EU Commission Releases Report on First Annual Review of the EU-U.S. Privacy Shield Framework*, LEXOLOGY (Oct. 18, 2017), https://www.lexology.com/library/detail.aspx?g=c015daae-008a-4ecf-9f32-9207fb390348.

[84] *See* GA. CODE ANN. § 10-1-912 (West 2007).

law. If those businesses are already members of the Privacy Shield, they may have a head start towards GDPR compliance. But "a proper response to the GDPR is not just about compliance – it requires a system-level, organization-wide response."[85] Therefore, companies must act quickly to ensure they will not be destroyed as a result of mishandling the personal data of EU citizens.

[85] Tim Walters, *Privacy Shield and GDPR: Sorting out the Business Obligations*, DIGITAL CLARITY GROUP (Feb. 9, 2017), http://www.digitalclaritygroup.com/gdpr-privacy-shield-sorting-out-business-obligations/.

V. APPENDIX

Appendix A: Privacy Shield vs. GDPR Infographic [86]

[86] *Privacy Shield vs. GDPR Infographic*, TRUSTARC, resources/privacy-research/privacy-shield-vs-gdpr-infographic/ (last visited Oct. 2, 2018).