COMPLIANCE WITH THE EU'S GENERAL DATA PROTECTION REGULATION AND US DISCOVERY LAW

By: Miriam C. Beezy and Stephanie A. Lucas

I. INTRODUCTION

On May 25, 2018, the General Data Protection Regulation ("GDPR") will become binding legislation for all businesses established outside the EU who control or process data if (1) the processing activities relate to the offering of goods or services to EU data subjects as well as (2) activities profiling EU data subjects' behavior while those data subjects are in the EU.[1]This new law will fundamentally alter the type of data processing and retention practices that US companies have traditionally held. Importantly, the GDPR will expose US companies to severe penalties in the absence of compliance with the regulation's strict rules. Complicating matters further, the US has recently enacted revised discovery obligations that impose sanctions for a party's failure to preserve electronic data.[2] Based on the GDPR's impending enforcement date and the new US discovery rules, US companies must now analyze their data processing and retention practices to ensure compliance with both the GDPR and US discovery obligations. Failure to comply with these sets of laws will lead to substantial penalties with GDPR violations penalizing US data controllers for up to EUR twenty million or four percent annual global turnover gross revenue and US discovery violations resulting in severe penalties to offending parties. [3]

Just next year, US companies will be confronted with the changing landscape of global data protection enforcement and the considerable shift in compliance and enforcement of data processing and retention policies.[4] This changing landscape has caused trepidation for many multinational respondents with a recent survey indicating that participants believe that GDPR "fines are inevitable according to 53% of UK respondents, 62% of German respondents and 58% of US respondents, while 63% of all respondents believe the proposed GDPR will make it harder for US companies to compete in Europe, and 70% think the new legislation will favor businesses based in Europe."[5] Undoubtedly, there is a great deal of uneasiness about how multinational businesses can comply with the GDPR while maintaining compliance with their domestic country's set of laws. However, companies must respect both domestic and GDPR regulations to ensure the least likelihood of sanctions while abiding by data privacy concerns of individuals.

This article aims to illustrate the GDPR's imminent data processing and retention changes for US companies and to aid US companies in the compliance of both the GDPR and the recently enacted US discovery law. In particular, this article addresses the GDPR's basic rules of compliance, the basic rules of the new US discovery law, and how US companies can process data effectively while remaining

---

[1] Giangi Olivi, *Technology's Legal Edge, Analysis: What to Expect From the Privacy Shield and the General Data Protection Regulation (GDPR)*, https://www.technologyslegaledge.com/2016/02/analysis-what-to-expect-from-the-privacy-shield-and-the-general-data-protection-regulation-gdpr/.

[2] Alan Klein and Kimberly G. Lippman, *Spoilation of Electronic Information Under Amended Federal Rule 37(e)*, http://www.thelegalintelligencer.com/home/id=1202778281178/Spoliation-of-Electronic-Information-Under-Amended-Federal-Rule-37e?mcode=1202615324341&curindex=3&slreturn=20170120152613.

[3] Jonathan Millard and Tyler Newby, *EU's General Data Protection Regulation: Sweeping Changes Coming to European and U.S. Companies*, http://apps.americanbar.org/litigation/committees/technology/articles/spring2016-0516-eu-general-data-protection-regulation.html.

[4] Alex van der Wolk and Sotirios Petrovas, *The EU General Data Protection Regulation: A Primer for International Business*, https://www.mofo.com/resources/publications/the-eu-general-data-protection-regulation-a-primer-for-international-business.html.

[5] ComputerWeekly.com, *EU Data Protection Regulation*, http://www.computerweekly.com/guides/Essential-guide-What-the-EU-Data-Protection-Regulation-changes-mean-to-you.

compliant with both sets of laws. Although the laws provide a framework for conformity, this article strives to provide greater clarity on what concrete steps US companies can take now to ensure their data processing and retention policies will be compliant by May 25, 2018.

II. PRIOR DATA PRACTICES IN THE EUROPEAN UNION

The European Union has traditionally been more protective of privacy rights for individuals than the US counterpart. This protective nature is best evidenced by numerous pieces of European legislation enumerating the individual's right to protection of their personal information. Although the European Union has enacted a myriad of legislation regarding individual privacy rights, the Privacy Shield and the GDPR have garnered considerable attention for US companies due to the legislation's sweeping effects. While this article will primarily address the intersection between US discovery obligations and compliance with the GDPR, an analysis of the Privacy Shield is critical to understand the sweeping effects that the GDPR will have on multinational companies, companies doing business in the EU or having customers located in the EU.

A. THE PRIVACY SHIELD

The EU-US Privacy Shield framework was designed by the US Department of Commerce and the European Commission to ensure US companies complied with EU data protection requirements when transferring European individual's personal data from the European Union to the United States.[6] In particular, "the privacy shield [was] a proposed framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States." [7] Notably, the Privacy Shield provides US companies a means to transfer personal data between the EU and the US while ensuring EU individuals the necessary safeguards for US data processing and retention.

To comply with the Privacy Shield, US companies are required to self-certify to the Department of Commerce that their data retention and processing policies are compliant and publicly commit to comply with the Privacy Shield's framework.[8] Once US companies have publicly committed to comply with the Privacy Shield, US companies receiving personal information of European Union members are required to take steps to ensure they comply with the requirements of the Privacy Shield.[9] Some of these requirements include ensuring US companies provide quick responses to individual EU members regarding their data processing and retention policies.[10] Also, the Privacy Shield requires US companies to outline a mechanism to quickly and effectively address privacy complaints or risk facing FTC investigation or investigation by a Privacy Shield panel.[11] If US companies do not comply with the Privacy Shield requirements, US companies processing EU member personal information and data will face harsh sanctions of exclusion from business with other EU members.[12] Additionally, the Privacy Shield also binds the US government by requiring the US to bolster its monitoring and enforcement of US company compliance for companies that receive EU member personal information.[13] In sum, the Privacy Shield presents a breadth of regulations and potential sanctions for US companies that control the

[6] *Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework*, Department of Commerce, https://www.commerce.gov/news/fact-sheets/2016/07/fact-sheet-overview-eu-us-privacy-shield-framework.
[7] Stephanie Hadley, *Preparing for Business with Europe: the Age of Privacy Shield and GDPR*, https://www.klogixsecurity.com/blog/preparing-for-business-with-europe.
[8] Department of Commerce, *supra* note 6.
[9] Hadley, *supra* note 7.
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*

processing and retention of data of EU individuals while holding the US government accountable for US company compliance.

Although European and US officials agree the Privacy Shield was a step in the right direction, the legislation raises serious issues of adequacy and compliance with data processing and retention. European privacy authorities have critiqued the Privacy Shield as being inadequate based on the lack of enforceable guidelines for compliance as well as the lack of a truly independent authority for challenges to US companies' data practices.[14] Thus far, the Privacy Shield has not faced direct legal challenges from opponents post-enactment. However, the Privacy Shield will be reviewed by the European Commission and the US Department of Commerce in June 2017 to assess the effectiveness of the Shield's safeguards and address any outstanding issues with the principles.[15] Based on the breadth of critiques of the Privacy Shield's effectiveness, salient issues will likely be discussed during the review and legal challenges addressing the intersection between the Privacy Shield and the GDPR will inevitably surface.

B. HOW THE GDPR DIFFERS FROM THE PRIVACY SHIELD

Although the Privacy Shield imposed a data processing and retention framework for US companies' interaction with EU individual's personal information, the GDPR reaches beyond the intersection between US and EU data practices. Importantly, the GDPR is not limited to EU and US data practices, but applies to all international companies who process or retain the data of EU individuals. The stricter GDPR compliance requirements will bind all international (including US-based) companies and inevitably cause companies to reorganize their data retention and processing practices.

Other notable differences between the Privacy Shield and the GDPR include the GDPR's breadth in addressing a variety of issues such as data breach notifications, an individual's right to removal of records, harsh monetary sanctions, and appointment of data protection officers.[16] Although the Privacy Shield has not been explicitly preempted by the GDPR, US companies should begin retention practices that comply with the GDPR as those practices will necessarily encompass the requirements of the Privacy Shield and avoid the GDPR's harsh penalties.

III. BASIC RULES OF THE GDPR

The GDPR provides a basic framework for how companies can comply with its stringent requirements. In particular, the GDPR enumerates the basic rules regarding compliance, territorial reach, legal bases for processing, and a myriad of other requirements with which companies processing and retaining European data must comply. This article discusses each of those requirements in turn.

A. TERRITORIAL REACH

One of the most important aspects of the GDPR is the sweeping territorial reach that the regulation will have on companies established and operating outside of the EU. Previously, European privacy legislation was limited to those entities that controlled the use of the data or had some establishment or equipment for data processing in the EU.[17] However, the sweeping scope of the GDPR now "applies directly to any entity that processes personal data about EU residents in connection with (1) the offer of goods or services in the EU; or (2) the monitoring of behavior in the EU."[18] Based on these broad categories, it is

[14] European Parliament Resolution on Transatlantic Data Flows, 2016/2727(RSP).
[15] John Farrell, *EU-US Privacy Shield: Set for Review in June 2017*, http://www.williamfry.com/newsandinsights/news-article/2017/01/26/eu-us-privacy-shield-set-for-review-in-june-2017.
[16] *Id.*
[17] Millard and Newby, *supra* note 3.
[18] *Id.*

difficult to imagine how a multinational company's activities, or any business transacting business with the EU, could avoid the GDPR's reach.

In considering whether a company offers goods or services to EU data subjects, there are no definitive criteria to determine whether goods or services are "offered" to EU data subjects to expose a company to the GDPR's territorial reach.[19] Specifically, a "combination of factors may lead to the determination that the company is targeting EU individuals, such as the ability to order goods and services in an EU language, providing payment options in EU currencies, and providing local content." [20] Although mere accessibility to a company website will not trigger the GDPR's territorial reach, offering potential EU customers international-friendly services as a matter of convenience could blur the line between providing mere accessibility and the offering of goods.

Furthermore, since the GDPR governs data processing activities that monitor the behavior of EU data subjects, companies tracking EU data subjects for big data purposes will likely be within the regulation's territorial reach. In considering the monitoring of EU data subjects, a business will be considered to "monitor the behavior" of individuals in the EU when the business specifically monitors behavior that *takes place* in the EU.[21] Although this geographical limitation on tracking behavior limits the reach of the GDPR, the tracking and profiling of individuals in the EU on the internet is also considered monitoring to trigger the territorial reach of the GDPR.[22] Therefore, multinational businesses that employ tracking technologies and targeted advertising on their websites are likely to fall within the purview of the GDPR's territorial reach and be subject to the regulation's requirements.

B. ENFORCEMENT BY DATA PROTECTION AUTHORITIES

The GDPR will be primarily enforced by European data protection authorities (DPAs) acting as independent agencies with fining and investigatory powers.[23] Although DPAs have traditionally enforced EU data protection laws, the GDPR will provide DPAs with more tasks and greater powers.[24] Specifically, under Article 52, DPAs will be required to monitor compliance, promote awareness, advise governments, provide information to individuals, handle complaints, cooperate with other authorities, conduct investigations, draft standard contracts for data transfers, draft requirements for privacy impact assessments, encourage certification mechanisms, and fulfill any other task related to data protection.[25]

Additionally, under Article 53, DPAs will have many powers under the GDPR such as "access to equipment and premises and corrective powers such as binding orders and bans on processing, administrative fines, and suspension of cross-border transfers." [26] One of the most important explicit powers given to the DPAs is to fine the companies that violate the GDPR. [27] "Data protection authorities will also be able to enforce penalties against the local representative of a non-EU data processor or controller, effectively giving those authorities indirect jurisdiction over non-EU data processors."[28] With GDPR violations of up to EUR twenty million or four percent annual global turnover gross revenue, DPAs carry significant authority over US companies who control and process EU individual's data. [29]

---

[19] Olivi, *supra* note 1.
[20] Van der Wolk and Petrovas, *supra* note 4.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Millard and Newby, *supra* note 3.
[29] *Id.*

C. EXPANSION OF PERSONAL DATA DEFINITION

The GDPR's expanded definition of personal data implicates the territorial reach and rights of individuals under the regulation. The GDPR defines personal data to include "unique online identifiers, including IP addresses and mobile device identifiers, and geo-location data about a subject."[30] Additionally, the GDPR's personal data definition also includes unique biometric data (i.e., fingerprints and retina scans) and genetic data.[31] Based upon this expanded definition, US companies who process data not traditionally considered personal data (i.e., geo-location data) would potentially need to comply with the enhanced individual's rights with respect to the newly defined personal data. For companies evaluating whether their collection of data is considered personal data under the GDPR, companies must carefully analyze the specific types of data they process and collect. Once companies have determined whether they collect personal data of EU data subjects, companies will be able to build a framework for ensuring compliance with the GDPR and the processing of this newly defined personal data.

D. LEGAL BASES FOR PROCESSING

Compared to prior EU privacy legislation, the GDPR is more restrictive concerning the permissible processing of EU individual's personal data. In particular, the GDPR restricts the permitted processing of personal data to when a company has a legal basis or "good reason" to do so.[32] An acceptable form of a "legal basis" to process personal data includes obtaining the consent of the individual from whom the personal data is derived.[33] Other "good reasons" to process personal data include the necessity to perform a contract as well as processing the personal data for compliance with a legal obligation.[34]

Additionally, a company may have a legal basis to process the personal data of an EU resident when the legitimate interest of the company in processing the data outweighs the privacy rights of the individuals.[35] To ascertain this balance, data controllers will have to balance their legitimate interests against the "fundamental rights and freedoms of the individual."[36] The balancing of the data processor's interests versus an individual's privacy rights will likely be a point of contention between as both the individual and the data processor will value their interests above the other.

1. CONSENT

The GDPR considers obtaining the consent of the individual from whom the personal data is derived to be an acceptable form of a legal basis to process personal data.[37] In ascertaining whether an individual has given affirmative consent, data controllers and processors should take into account the individual's age and capacity to give consent. The GDPR sets the standard age for consent from minor individuals at 16 years old.[38] However, the GDPR also allows member states to give discretion over permissible ages for

---

[30] *Id.*
[31] *Id.*
[32] Van der Wolk and Petrovas, *supra* note 4.
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] Lawrence Ryz and Tracey Stretton, *EU Data Protection Gains A Sword To Go With Its Shield*, http://www.theediscoveryblog.com/2016/03/09/discovery-implications-eu-data-protection-regulation/.
[37] Van der Wolk and Petrovas, *supra* note 4.
[38] *Eye on Discovery- Five Steps to take Now to Prepare for the General Data Protection Regulation,* Consilio, http://www.consilio.com/resource/eye-discovery-five-steps-take-now-prepare-general-data-protection-regulation/.

consent based on the member state in which the individual is located.[39] Also, if the company processes sensitive data or data relating to children (individuals under the age of 13 to 16 depending on the member state), potential further restrictions apply (explicit consent and parental consent, respectively).[40] Therefore, to ensure compliance with the GDPR and the new consent requirements, companies will need to evaluate the jurisdictions of the member states in which they operate to identify the necessary age for individuals to give proper consent to their data processing.

After establishing the age of the individual giving consent, companies must obtain the proper form of consent from the individual. Specifically, the consent an individual gives to processing of personal data must be "informed, specific, evidenced by a statement or affirmative conduct (silence or inactivity is insufficient) and in the case of sensitive personal data, be explicit." [41] In ascertaining what constitutes consent from the individual, the GDPR makes clear that "silence, pre-ticked boxes or inactivity do not constitute adequate forms of consent."[42] Therefore, data controllers and processors must implement more overt practices to obtain the individual's affirmative consent. Additionally, the company cannot require consent from the individual as a provision of the service unless the consent is necessary to the performance of the contract.[43] Also, the individual must retain the right to revoke consent at any time without detriment to the individual.[44] These requirements for affirmative consent and free revocation essentially require companies to have individuals effectively "opt-in" to data processing and easily "opt-out" without any negative residual effects. Therefore, data controllers and processors must evaluate how they have previously obtained individual's personal information and data and how they plan to ensure compliance under the regulation.[45] Although many organizations have previously relied on procedures allowing the individual to opt-out of data collection procedures, these organizations may need to obtain a new form of consent from these individuals to comply with the GDPR's requirements.[46]

E. ENHANCED INDIVIDUAL RIGHTS

With the expanded definition of personal data, the GDPR also provides EU individuals with enhanced and powerful rights on how companies may retain and process their personal data. Data controllers will be required to provide greater transparency to individuals about how they collect the individual's data and how the collected data will be used at the time of collection.[47] Also, data controllers will be required to notify individuals of their right to file complaints to the data controller's privacy authority officer, and the right of EU individuals to "receive data that has been collected about them in a structured and commonly used machine-readable format."[48] This information can most easily be disclosed to the individual in a well-written privacy policy that discloses the "identity and contact information of the controller, the purpose of data collection and processing, and third parties to whom the data will be transferred."[49]

The GDPR also requires data controllers to hold data only for the period of time absolutely necessary and not change use of the data from the purpose for which it was originally collected from the individual. [50] This is a potential issue for data controllers who seek to use personal data of individuals for big data purposes. However, the GDPR contains an exception to this restrictive rule. The GDPR allows a change

[39] *Id.*
[40] Van der Wolk and Petrovas, *supra* note 4.
[41] Millard and Newby, *supra* note 3.
[42] *Id.*
[43] Van der Wolk and Petrova, *supra* note 4.
[44] Millard and Newby, *supra* note 3.
[45] Consilio.com, *supra* note 38.
[46] *Id.*
[47] Millard and Newby, *supra* note 3.
[48] *Id.*
[49] *Id.*
[50] Computerweekly.com, *supra* note 5.

in the use of the data from the purpose it was originally collected, if the purpose is not "incompatible" with the original purpose.[51] Under Article 6(3a), some factors to assess incompatibility include "the link between the purposes for which the data were collected and the intended new purposes; the relationship between the individual and the company; the nature of the personal data; the 'possible consequences' for individuals; and the existence of safeguards such as encryption or pseudonymization."[52] Therefore, the analysis of the permissible usage of data will likely be a fact-specific inquiry requiring careful consideration of the original and renewed purposes of the data collection and processing.

1. PROFILING

Another enhanced individual right under the GDPR is the requirement for data controllers to notify EU individuals if controllers use personal data for "profiling."[53] Profiling is defined as the automated processing of personal data and use of that personal data to "evaluate certain personal aspects relating to a natural person." [54] If a data controller uses personal data for profiling, that profiling cannot be based on special categories of personal data (i.e., racial, ethnic, or religious information) without explicit consent. [55] However, profiling may be permissible if such processing "is necessary for reasons of substantial public interest."[56] When a data controller profiles individual's data, the controller will be required to secure personal data, implement technical and organizational safeguards to avoid errors and correct data inaccuracies, and minimize the risk of profiling's "discriminatory effects." [57] Importantly, the GDPR gives individuals being profiled the right to request profiling data about themselves and either object to or demand that such profiling be stopped.[58]

2. RIGHT TO BE FORGOTTEN

Additionally, data controllers will be required to inform EU individuals about the individual's "right to be forgotten." [59] This right to be forgotten requires data processors to inform individuals about their right to deletion and correction of data concerning themselves. However, Article 17(3) limits this expansive individual right. A data controller may be exempt from the individual's right to be forgotten if the data "processing is deemed necessary for the exercise of freedom of expression, compliance with a legal obligation, public interests such as public health, scientific or historic research, or the establishment or defense of legal claims."[60] Therefore, the right to be forgotten is expansive in scope, but data controllers have several potential exemptions to waive this requirement.

3. DATA PORTABILITY

Individuals may be able to request that data be transferred between companies directly and not through a third party data processor.[61] However, even upon the individual's request, companies do not need to implement technically compatible systems to facilitate the direct transfer of personal data to another company. [62] The request for direct data transfer by an individual only applies to personal information that was "obtained on the basis of consent or as necessary for the performance of a contract, but not where

[51] Van der Wolk and Petrova, *supra* note 4.
[52] *Id.*
[53] Millard and Newby, *supra* note 3.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] Millard and Newby, *supra* note 3.
[60] Van der Wolk and Petrova, *supra* note 4.
[61] *Id.*
[62] *Id.*

information was obtained on other grounds (e.g., compliance with a legal obligation)."[63] Therefore, data controllers must abide by these enhanced data portability rights, but only under these limited circumstances.

4. NEXT STEPS BASED ON INDIVIDUAL RIGHTS

Based on these enhanced individual rights, a data controller's processing methods are likely to trigger individuals' rights to control information collection and dissemination. Therefore, data controllers, including US companies, should begin to review how data flows through their organizations to determine how difficult it would be to comply with an individual's request to provide or delete their information.[64] Since some companies disperse personal data of individuals across various systems, vendors, third parties, and applications, it is important to map out how a company's data is stored and who has access to it.[65]

After analyzing the flow of personal data from an organization, the organization must then create a procedure for easily searching for, segregating, and deleting this personal information when an individual invokes their rights under the GDPR.[66] Companies should take the time before May 25, 2018 to ensure their compliance with these enhanced individual rights and mitigate any potential risk of noncompliance under the coming regulation.

F. DIRECT LIABILITY FOR PROCESSORS

The GDPR's obligations primarily focus on entities that are data controllers "who make decisions regarding how personal data are collected, used and shared." [67] However, the GDPR also introduces obligations for data processors. Data processors are entities that are responsible for processing the data without directing the collection or control of the data.[68] Under the regulation, data processors will be subject to direct liability and will need to comply with requirements relating to cross-border transfers, security, and recording their processing activities.[69] Additionally, regardless of whether the data processor is located within the EU or another jurisdiction, the data processor will be subject to obligations such as "implementing appropriate technical and organizational measure[s] with respect to personal data, [and] notifying the data controller of a data breach and potentially appointing a data protection officer."[70] This direct liability is a sharp departure for data processors that traditionally were contractually liable only to the data controller but not subject to enforcement from a data regulator. [71] Under the regulation's imposition of additional data processor powers and obligations, it is recommended that data controllers require audit rights and an approval system for the potential appointment of sub-processors working on the data controller's behalf.[72]

G. ORGANIZATIONAL REQUIREMENTS

Under the GDPR, data controllers and processors will face changes in organizational requirements based on their data processing and retention practices. Specifically, data controllers and processors will be

[63] *Id.*
[64] Consilio.com, *supra* note 38.
[65] *Id.*
[66] *Id.*
[67] Van der Wolk and Petrova, *supra* note 4.
[68] *Id.*
[69] *Id.*
[70] Millard and Newby, *supra* note 3.
[71] *Id.*
[72] *Id.*

required to develop and maintain data protection policies and the documentation describing such policies.[73]

1. PRIVACY IMPACT ASSESSMENTS

Article 33 of the GDPR requires data controllers and processors to conduct data protection impact assessments (more frequently known as a Privacy Impact Assessment ("PIA")) if the proposed data processing "is likely to result in a high risk to the rights and freedoms of individuals."[74] These PIAs would evaluate the data controller or processor's proposed data processing and the susceptibility to risk that such data processing presents.[75] Additionally, the PIA would evaluate the data processor or data controller's potential safeguards to mitigate the risk of such data processing.[76]

Specifically, Article 33(3) of the GDPR requires the PIA to include a "systematic description of the processing operations, their purposes, and the interests pursued by the company; an assessment of the necessity and proportionality of the processing; a risk assessment with regard to individual rights; and the safeguards and accountability measures that are envisaged."[77] Also, Article 28 will require companies to "maintain a record detailing, among other things, the purposes of processing; categories of individuals; potential data recipients within and outside the EU; appropriate safeguards for transfers; and security measures."[78] The detail and importance of retaining records and PIAs is emphasized because such records must be provided to the Data Protection Authorities upon request to demonstrate compliance with the GDPR and avoid potential sanctions.[79] Therefore, detailed and organized PIAs can help data controllers and processors evade the GDPR's harsh sanctions.

2. DATA PROTECTION OFFICERS

The GDPR will require the appointment of a position known as the data protection officer (DPO) in certain circumstances. The GDPR requires data processors and controllers to appoint a DPO when a company's "core processing activities require regular and systematic monitoring of individuals on a large scale, or where its core activities consist of the processing of sensitive data on a large scale."[80] Due to the DPO's limited application for most companies, it is unlikely that many companies will be required to appoint a mandatory DPO. [81] Nevertheless, data controllers and processors need to evaluate their data practices to determine whether their organization will ultimately require a DPO to ensure compliance with the GDPR. A recent study by the International Association of Privacy Professionals estimates that the GDPR's requirement for a DPO will require the appointment of approximately 28,000 DPOs over the next two years in Europe alone.[82]

If a DPO is required for a data controller or processor, the DPO will have the responsibility of overseeing the controller's or processor's compliance with the GDPR based on their data retention policies and record keeping.[83] Understandably, these DPOs will need to have expert knowledge on data protection practices and laws to ensure the company is in compliance with the regulation.[84] A DPO appointed for

---

[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] Van der Wolk and Petrova, *supra* note 4.
[78] *Id.*
[79] *Id.*
[80] Millard and Newby, *supra* note 3.
[81] Van der Wolk and Petrova, *supra* note 4.
[82] Computerweekly.com, s*upra* note 5.
[83] Millard and Newby, *supra* note 3.
[84] Consilio.com, *supra* note 38.

one company may also be appointed for the group of company affiliates. [85] Therefore, data controllers and data processors that are required to appoint a DPO and have several affiliates will only be required to appoint one DPO.[86] Because the appointment of a DPO will require company recruitment and re-organization efforts, one of the next steps an organization should take in preparation for GDPR compliance is to seek legal advice as to whether the company's data processing requires the company to appoint a DPO.[87]

3. LOCAL REPRESENTATIVE REQUIREMENT

Under Article 25 of the GDPR, companies who "regularly collect or process personal data from EU citizens on a large scale" will be required to appoint local representatives within the EU member states in which they do business.[88] This Article 25 requirement will bring non-EU data processors within the regulatory purview of EU data protection authorities and ensure global compliance with non-EU based companies. [89] However, this local representative requirement is limited and unlikely to apply to companies that have few contacts with EU individual's personal information. If a company only processes data occasionally, processes data related to criminal convictions and offenses, and based on the nature, context, scope, and purpose of processing, the data processing is unlikely to be a risk for the rights and freedoms of individuals, and does not process special categories of data (defined under Article 9(1)), the company will not be required to appoint a local representative in those EU countries. [90] Therefore, it is important for companies to take the time to analyze what types of data they currently process to assess whether appointment of a local representative is required.

H. DATA BREACH RESPONSE

According to Article 31, the GDPR will introduce a breach notification duty throughout the EU and uniformity in data breach responses.[91] Specifically, when a data breach occurs, data controllers will be required to notify supervisory authorities (the DPAs) of "a data breach that is likely to result in a risk for the rights and freedoms of the data subject within 72 hours of discovery of the breach."[92] Also, the potentially affected individuals of a data breach must be notified of the breach without undue delay if the data breach "presents a high risk for the rights and freedoms of individuals."[93] However, if the data breach only presents *some* risk for individuals, only the data protection authority will need to be notified and not the individuals. [94] The information provided with the data breach notification must include the cause and nature of the breach (if known) and recommendations for how the potentially affected individuals can mitigate the risks of the breach.[95] Notably, the burden to prove the absence of risk in a data breach will be on the data processor. [96]

Some hurdles with the GDPR's data breach notification requirement include the challenges with notifying individuals during the required 72-hour time frame when the investigation into the breach can take substantially more time. [97] Other hurdles include ensuring data controllers have the proper identification

[85] Van der Wolk and Petrova, *supra* note 4.
[86] *Id.*
[87] Consilio.com, s*upra* note 38.
[88] Millard and Newby, *supra* note 3.
[89] *Id.*
[90] *Id.*
[91] Van der Wolk and Petrova, *supra* note 4.
[92] Millard and Newby, *supra* note 3.
[93] *Id.*
[94] Van der Wolk and Petrova, *supra* note 4.
[95] Millard and Newby, *supra* note 3.
[96] *Id.*
[97] *Id.*

and response infrastructure to respond within this time frame after a breach occurs. Based on the ambiguity of what constitutes a "high risk" for individuals affected by a data breach, the GDPR is necessarily broader and vaguer than US state data breach notification statutes.[98] Therefore, US data controllers will likely issue more data breach notifications under the GDPR than they traditionally would under US state law.[99]

IV. THE INTERACTION BETWEEN US DISCOVERY LAW AND THE GDPR

The GDPR will inevitably result in tension with US companies who seek to comply with US discovery obligations while maintaining compliant data processing and retention policies for EU individuals. Although there has been a long standing tension between EU legislation regarding privacy rights and US e-discovery obligations, the GDPR and "various EU country-specific data privacy laws make even more challenging when faced with collection, processing, review, and production tasks along the e-discovery lifecycle."[100] Companies should be mindful of enforcing data retention policies to be in accord with both the GDPR and the US discovery obligations to ensure they will not be subject to penalties under either law.

With respect to penalties, US companies will face penalties for non-compliance with the GDPR as well as sanctions for non-compliance with new US discovery rules. To alleviate these potential conflicts in data retention and discovery, attorneys will need to carefully plan their data collection and data requests during the early stages of litigation to avoid a conflict between a US court order and the stringent GDPR requirements.[101] Comparing the GDPR's heavy fines with US court sanctions, an increasing number of US companies may decide to pursue early settlements or risk sanctions in the US to avoid the steep fines for GDPR violations.[102] This cost-benefit analysis of choosing settlement versus pursuing litigation may be an attractive option for companies facing litigation that is not considered a serious threat to the company or its way of doing business.[103] The cost benefit analysis should be based on the conflicts between US discovery and specific GDPR provisions which are further examined below.

A. NEW FEDERAL RULES OF CIVIL PROCEDURE FOR DISCOVERY

Examination of the new Rule 37(e) is required to understand the conflict between the GDPR requirements and e-discovery obligations. In December 2015, the rule makers amended Rule 37(e) of the Federal Rules of Civil Procedure.[104] The Amended Rule 37(e) imposes sanctions for a party's failure to preserve

---

[98] *Id.*
[99] *Id.*
[100] Moncure, Del Piero, McKenna, *The General Data Protection Regulation's Key Implications for E-Discovery*, http://www.insidecounsel.com/2016/11/23/the-general-data-protection-regulations-key-implic.
[101] Millard and Newby, *supra* note 3.
[102] Van der Wolk and Petrova, *supra* note 4.
[103] Moncure, Del Piero, McKenna, *supra* note 100.
[104] FRCP 37(e) (2015), available at: https://www.law.cornell.edu/rules/frcp/rule_37
Rule 37(e) was amended in December 2015 and now states:

> FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

electronic data in certain circumstances.[105] This amended rule seeks to preserve potentially valuable electronic data for discovery purposes for anticipated or ongoing litigation. Under the amended rule, a court may enforce sanctions against a party who does not comply with the preservation of the electronically stored information. Specifically, in evaluating whether to enforce sanctions under Rule 37(e), "a court must balance the severity of sanctions against the intent of the spoliator and any prejudice borne by other parties."[106] The effect of this amended Rule 37(e) has pushed party's preservation practices to the forefront of litigation "with cases focusing on reasonable steps to preserve, intent to deprive another party of relevant [electronically stored information (ESI)] and the inherent power of the court to administer sanctions."[107]

The committee notes to the amended rule address proportionality as an important factor in evaluating the reasonableness of preservation of electronic data. [108] However, courts have generally struggled with Rule 37(e)'s removal of the "reasonably calculated to lead to the discovery of admissible evidence" language and the amended rule's additional emphasis on proportionality.[109] Over the course of 2016, about 56 percent of e-discovery judicial opinions examined the amended Rule 37(e) and emphasized proportionality and the scope of discovery as compared to 35 percent in 2015. [110] Based on this increased attention and examination of proportionality for ESI discovery productions, companies must now balance the types and breadth of data they collect against the new rule's obligation to preserve, collect and review relevant ESI for cases.[111] As courts continue to interpret the new discovery rules and permissibility of e-discovery practices, companies will find it vital to stay current on judicial opinions to assist with formulating company polices.[112]

B. CONSENT AND LEGAL BASES FOR PROCESSING

One of the accepted "legal bases" for processing personal data under the GDPR includes obtaining the consent of the individual from whom the personal data is derived.[113] However, obtaining consent from data subjects with respect to e-discovery data processing can be a cumbersome process. Data subjects can give affirmative consent to e-discovery of their personal data only if they are given sufficiently detailed notice for them to make an informed choice.[114] However, under the GDPR, even if the data subject has given affirmative and informed consent for discovery data processing, the data subject's consent to this e-discovery data processing can be withdrawn without consequence to the subject at any time.[115]

---

[105] Klein and Lippman, *supra* note 2.
[106] *Id.*
[107] *2016 Ediscovery Case Law: New FRCP Amendments Drive 60 Percent Increase in Proportionality Opinions*, https://www.krollontrack.com/resources/press/details/64997/2016-ediscovery-case-law-new-frcp-amendments/.
[108] Comment to FRCP amendment (2015), available at: https://www.law.cornell.edu/rules/frcp/rule_37
"Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms. It is important that counsel become familiar with their clients' information systems and digital data — including social media — to address these issues. A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime."
[109] Michelle Lange, *6 Months of Case Law Under the New FRCP*, The Ediscovery Blog, http://www.theediscoveryblog.com/2016/06/16/6-months-of-case-law-under-the-new-frcp/.
[110] Krollontrack.com, *supra* note 107.
[111] *Id.*
[112] *Id.*
[113] Van der wolk and Petrovas, *supra* note 4.
[114] Ryz and Stretton, *supra* note 36.
[115] *Id.*

Additionally, a company may have a legal basis to process the personal data of an EU resident when the legitimate interest of the company in processing the data outweighs the privacy rights of the individuals.[116] "A company's legitimate interest is currently and is likely to continue to be the most common justification for carrying out an e-discovery exercise."[117] However, in balancing their legitimate interests for data processing, US companies complying with US discovery obligations should provide individuals with comprehensive notice about "how their personal data is to be processed, that personal data is only processed within the scope of that notice and that their rights (i.e., to be able to access or correct personal data or object to the processing) are preserved." [118] Therefore, companies relying on this "legitimate interest" should carefully describe the business' interests in processing the data and fully inform the affected individual.

C. RIGHT TO BE FORGOTTEN AND DATA PORTABILITY RIGHTS

Under the GDPR, individuals can request to have their personal data deleted and/or request a transfer of their personal data to another institution. [119] For e-discovery purposes, personal data is likely to be in any email or document that is handled during pre-trial discovery or produced in response to a regulatory inquiry.[120] Therefore, companies involved in US litigation will almost positively possess personal data of European individuals in their potential discovery productions. With the right to be forgotten and data portability rights under the GDPR, companies who comply with the GDPR will inevitably lose control and custody over the information they retain, even potentially during litigation or a government investigation.[121] This lack of control over the retention and processing of personal data will inevitably bring conflict "between U.S. requirements regarding the preservation of potentially relevant evidence and the EU data subject's right to have data deleted."[122]

If an organization is required to comply with an individual's data transfer or deletion requests under the GDPR's right to be forgotten, a US judge will inevitably face a confrontation over whether to enforce the US discovery obligations or accept the defense of compliance with European law. In all likelihood, a US judge will be more likely to respond favorably to a company preserving potentially relevant information in litigation proceedings as opposed to a company abiding by the GDPR's deletion of data.[123] Because US civil litigation is based on the principle that expansive pre-trial discovery and a developed record serve to narrow the legal issues, cutting to the heart of the dispute, US judges will likely not excuse a litigation party from defying US discovery laws in order to comply with European laws.[124]

D. PRIVACY IMPACT ASSESSMENT OBLIGATIONS

The GDPR also requires certain companies to develop and maintain PIAs to analyze their scope of data processing and mitigate potential data risks. These PIAs contain a trail of information of the company's data transfers, deletions, and processing for the company.[125] If a company inadvertently deleted potentially relevant data in a pending investigation or litigation matter, a US judge could feasibly require the company to turn over the PIA to demonstrate the data trail showing how the lost data was originally collected.[126] Therefore, a company's GDPR compliant PIA could become a shield for the company to

---

[116] Van der wolk and Petrovas, *supra* note 4.
[117] Ryz and Stretton, *supra* note 36.
[118] *Id.*
[119] Moncure, Del Piero, McKenna, *supra* note 100.
[120] Ryz and Stretton, *supra* note 34.
[121] Moncure, Del Piero, McKenna, *supra* note 100.
[122] *Id.*
[123] *Id.*
[124] Ryz and Stretton, *supra* note 36.
[125] Moncure, Del Piero, McKenna, *supra* note 100.
[126] *Id.*

explain why some data was removed or deleted based on the European data subject's enhanced individual rights. [127] On the other hand, if a company's PIA did not provide enough information or was not thorough enough, the lack of information produced in a discovery request for the PIA could exact additional sanctions under the new discovery rules.[128] To balance a GDPR compliant PIA with a demanding discovery preservation rule, US companies should carefully plan their PIA documentation and data trails to delineate clear compliance with European data subject requests for deletion or revocation of consent.

E. DPO REQUIREMENT

Under the GDPR, a DPO will be a required position for organizations processing certain forms of data. The GDPR requires data processors and controllers to appoint a DPO when a company's "core processing activities require regular and systematic monitoring of individuals on a large scale, or where its core activities consist of the processing of sensitive data on a large scale."[129] Although the appointment of a DPO will incur an additional expense for relevant companies, US companies with a DPO in their compliance or legal department can lend greater advocacy and education for US judges and regulators.[130] A DPO could serve as an excellent advocate before US judges with respect to a business' need for data deletion for compliance under the GDPR.[131] If a DPO is able to explain in an expert and comprehensive manner the company's requirement to follow certain data deletion practices to comply with the GDPR, US judges may be more likely to find a resolution for the conflict between the company's compliance with the GDPR and US discovery rules of electronic data preservation. [132] The DPO could also educate and advocate to US judges the most efficient and feasible means of accommodation for companies when laws governing GDPR data and US discovery inevitably conflict.[133] Although appointment of a DPO adds to compliance costs, a DPO can serve as a valuable asset to companies needing an expert in the field to develop and advocate for the propriety of their data processing policies.

F. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

The GDPR stringently regulates the transfer of EU individual's personal data to countries outside the EU. Article 48 of the GDPR "expressly states that orders or judgments by non-EU courts and administrative authorities requiring transfer or disclosure of personal data are not a valid basis for transferring data to third countries."[134] However, Article 48 also states that orders or judgments by non-EU courts and administrative authorities will be recognized if they are based on international agreements or treaties between the EU or member state and the third country.[135] Examples of these recognized agreements include the Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters.[136] Therefore, companies litigating in US courts will be required to rely upon an appropriate international treaty or other acceptable basis for transferring and disclosing personal data of EU residents during litigation.[137] Although these options may be problematic under US discovery rules, compliance with the GDPR through these means will be required to avoid the staggering penalties that the GDPR enforces.[138]

---

[127] *Id.*
[128] *Id.*
[129] Millard and Newby, *supra* note 3.
[130] Moncure, Del Piero, McKenna, *supra* note 100.
[131] Moncure, Del Piero, McKenna, *supra* note 100.
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *Id.*
[138] *Id.*

The GDPR will permit transfer of personal data to countries outside the EU if the outside country has an "adequate" level of data protection. [139] The GDPR also will permit transfer of personal data to other nations through standard contractual clauses and binding corporate rules.[140] The GDPR approves two other safeguards for the transfer of personal data: codes of conduct and certification.[141] "A code of conduct is a self-regulatory mechanism that demonstrates adherence to information privacy standards, including international data transfers." [142] This code of conduct may be "drafted by a DPA, member state, European Data Protection Board, the European Commission, or other associates or bodies that represent data controllers or data processors." [143] Certifications, the other safeguard, may be developed by the European Data Protection Board at the Union level. [144] These two alternative safeguards for the transfer of personal data may give US companies an alternative to the Regulation and allow for sector-specific adequacy "(e.g., a country may be considered adequate for financial information but not health information)."[145] Therefore, if a US company wants to avoid the headache of complying with international treaties to transfer European data for litigation proceedings, a US litigant is entitled to several different and more accessible options such as contractual clauses and codes of conduct.

G. MORE OBLIGATIONS ON SERVICE PROVIDERS ACTING AS DATA PROCESSORS

The GDPR's direct liability for data processors will likely affect US data processors who serve as e-discovery service providers. Specifically, e-discovery service providers and/or law firms who serve as e-discovery service providers will be subject to GDPR penalties if those entities cannot meet the GDPR's heightened standards. Therefore, e-discovery service providers may be wary of continuing data processing obligations under the GDPR based on the regulation's demanding requirements.

However, an e-discovery data processor who demonstrates compliance with these heightened GDPR standards can also take advantage of the increased demand from US litigants. Based on the requirement for strict compliance with data processing and retention policies, a well-versed e-discovery data processor can be an invaluable asset for parties in litigation aiming to comply with US discovery laws. Therefore, compliant e-discovery data processors "will likely be recognized as preferred providers within the industry," and provide valuable data processing techniques to US companies involved in litigation.[146]

V. CONCLUSION

The May 25, 2018 enforcement of the GDPR will inevitably cause US data controllers and processors to undergo significant planning and restructuring of their data practices. Moreover, complying with the amended US discovery rules will inevitably conflict with the GDPR's demanding requirements. To alleviate the tension in complying with these laws, businesses moving forward should take the time to determine what type of data they have collected about EU residents. [147] After determining the type of data collected, they should trace the flow of data collection, both inside the company and to any third-party data processors, including vendors and the company's law firms. [148] Also, businesses should evaluate their current data transfer mechanisms and procedures and ensure such systems are compliant with both sets of

[139] Consilio.com, *supra* note 38.
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] Moncure, Del Piero, McKenna, *supra* note 100.
[147] Consilio.com, *supra* note 38.
[148] *Id.*

rules.[149] Moving forward, the world of regulations addressing data practices will inevitably converge and conflict and multinational entities and entities having an EU reach will need to be flexible in adapting their practices to ensure compliance with these diverse sets of laws. The accompanying checklist summarizes what companies can do to prepare for compliance with the GDPR and US discovery law.

[149] *Id.*

Checklist to Comply with the EU'S General Data Protection Regulation (GDPR) and US Discovery Law

- ☑ Determine whether your company processes data of activities relating to (1) the offering of goods or service to EU individuals or (2) processes data profiling the activities of EU individuals while they are in the EU.

- ☑ Determine who your company's European Data Protection Authority would be for enforcement and compliance issues.

- ☑ Determine what type of personal data your company is collecting. Specifically, does you company collect geo-location, biometric, or sensitive personal data? If so, you are likely within the GDPR's reach.

- ☑ Determine your basis for processing of EU individual's personal data. Is it for a legal basis, a legitimate interest of the company, and/or did you obtain consent from the individual?

- ☑ Determine what type of consent you previously obtained from EU individuals regarding the processing of their personal data. Was it affirmatively given and explicit? If the consent obtained does not comport with GDPR requirements, you may need to obtain a renewed form of consent.

- ☑ Determine whether your data processing activities constitute profiling under the GDPR to trigger notification of your profiling activities to EU individuals.

- ☑ Determine how data flows through your company to discern how difficult it would be to comply with an individual's request to move or delete their information.

- ☑ Create and analyze a private impact assessment to discern your company's proposed data processing, susceptibility to risks, and planned safeguards to mitigate such risks. A more carefully analyzed PIA will help companies potentially avoid US discovery law sanctions if proof of deletion or movement of data complies with the GDPR and is evidenced in the PIA framework.

- ☑ Analyze whether your company's core processing activities require (1) regular and systematic monitoring of individuals on a large scale or (2) consist of processing sensitive data on a large scale. If you determine your company's activities satisfy either of these inquiries, you may need to appoint a Data Protection Officer.

- ☑ Analyze whether your company regularly collects or processes personal data from EU citizens on a large scale. If so, you may be required to appoint an EU local representative in the EU member states in which your company does business.

- ☑ Implement the proper infrastructure to be able to notify affected individuals and the Data Protection Authorities within 72 hours of a data breach.

- ☑ Determine what type of consent from EU individuals will be required to comply with US discovery data retention obligations. EU individuals must be given as much disclosure as possible for companies to obtain their informed and affirmative consent.

- ☑ Mitigate the risks in discovery proceedings of an EU individual exercising their right to deletion and portability of their personal data. Because an individual can exercise these rights and revoke consent at any time, companies should assess discovery productions accordingly.