SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 8, PAGE 216

THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION: HOW WILL IT AFFECT NON-EU ENTERPRISES?[1]

By: Manu J. Sebastian

INTRODUCTION

In a world where technology is ever changing and personal data is being processed and saved at every turn, corporations must be held accountable for the data they collect, store, and use.[2] The consumer truly does not understand the levels of data capture and retention that corporations employ, and the European Union's ("EU") government is on a mission to ensure that its citizens are protected because it believes personal data protection is a fundamental right

[1] In the summer of 2013, the author worked for Morgan Stanley Capital Investments (MSCI), a major international finance technology firm, in London. His long-term project focused on assisting their Europe, Middle East, and Asia Legal Department in proactively determining how the GDPR would affect the enterprise as a whole. He learned a great deal during his time at MSCI and is grateful to have had the opportunity to work so closely with the talented members of the team. Thank you to Jamie Pawliczek, Christopher Harte, Olga Pulickal, and Sunil Desaur. Secondly, the author would like to give further acknowledgement and thanks to Dean Christian Day of Syracuse University College of Law for his direction, encouragement and advisement and to Dean Aviva Abramovsky of Syracuse University College of Law for her support. Finally, the author would like to extend special thanks to Ms. Abigail L. Reese and the Sebastian Family for their support.

[2] *Data Protection Debate with Jan Philipp Albrecht & Pat Walshe*, VIEUWS (Oct. 17, 2013), http://www.vieuws.eu/ict/data-protection-debate-with-jan-philipp-albrecht-mep-pat-walshe-gsma/ [hereinafter *Data Protection Debate*].

that all people should enjoy.[3] The EU created the General Data Protection Regulation ("GDPR") in an attempt to protect data without detrimentally inhibiting cross-border data flow.[4]

The GDPR is in its final stages of adoption and corporations around the world are working to preemptively establish controls within their internal structures in order to be compliant.[5] These new changes will protect personal data on a level that has never before been seen, but it will come at a great cost to the consumer. The data that is being protected moves far beyond identification numbers and medical data. The GDPR seeks to protect names, phone numbers, addresses, economical data, cultural identity, racial origin, social identity, profiling data, and online identifiers such as IP address and location data, on top of the normal protections of health data and biological samples.[6] The regulation is based on the notion that every single person has the right to have his personal data protected and it protects all people in the EU.[7] These new changes make us ask a very important question: How exactly will Non-EU enterprises be affected?

The changes being proposed not only affect corporations based within the EU, but also affect any corporation that is looking to do business with a person in the EU.[8] International

---

[3] *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation): Compromise Amendments on Articles 1-29*, COM (2012) 0011 (Oct. 7, 2013) [hereinafter *Amended GDPR Art. 1-29*].

[4] *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard To the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Proposed GDPR*].

[5] *Data Protection Debate*, *supra* note 2.

[6] *Amended GDPR Art. 1-29*, *supra* note 3, art. 9.

[7] *Proposed GDPR*, *supra* note 4, at 19 ¶ 11.

[8] *Id.*

corporations have an economic need for transborder data flow.[9] As a result, most businesses will be affected, especially those within communications, finance, utilities, construction, medical, transportation, and business services.[10] Additionally, any international corporation that uses a credit card could be affected.[11] Non-EU corporations whose websites use EU Member States' currencies or EU Member States' languages will be viewed as targeting people in the EU.[12] The ramifications of the GDPR are great because it affects the entire global trading system and almost every international enterprise in the world.[13]

To illustrate these issues in the simplest way, we can consider any non-EU corporation that sells a product to a person in the EU. People who are the subject of the protected data are known as Data Subjects and all corporations that collect and process data are labeled Data Controllers ("Controllers") and Data Processors ("Processors").[14] The Data Subject in the EU would place a purchase with the international corporation (an "Enterprise") using their personal information including their name, telephone, and address. Because the EU resident is the buyer entering personal data, the buyer is known as the Data Subject.[15] The Enterprise would be the

---

[9] Press Release, Joint Statement on GDPR (Oct. 16, 2013), *available* at http://www.gsma.com/gsmaeurope/wp-content/uploads/2013/10/Joint-Association-Statement-on-GDPR-161013EP.pdf.

[10] EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY, THE ECONOMIC IMPORTANCE OF GETTING DATA PROTECTION RIGHT: PROTECTING PRIVACY, TRANSMITTING DATA, MOVING COMMERCE, U.S. CHAMBER OF COMMERCE (2013) [Hereinafter ECIPE] *available at* https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

[11] *Id.* at 5.

[12] *Proposed GDPR*, *supra* note 4, art. 3(2)(a); Briefing Paper on the Proposed General Data Protection Regulation (GDPR) from GSMA Europe, ETNO, ECTA and Cable Europe 4 (Sept. 2012), http://www.gsma.com/gsmaeurope/wp-content/uploads/2012/09/Briefing-Paper-on-Applicable-Law.pdf.

[13] U.S. CHAMBER OF COMMERCE, *supra* note 10.

[14] *See Proposed GDPR*, *supra* note 4.

[15] *Key Definitions of the Data Protection Act*, INFO. COMMISSIONER'S OFF., http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions (last visited Apr. 2, 2015).

Controller because it determines the purpose and manner in which the personal data is used.[16] As most of the Data Subject's information would be protected under the GDPR, any time the information is transferred to another enterprise or subsidiary within the supply chain, the initial Enterprise would have to ensure that the next enterprise that receives the information complies with the GDPR. These third party enterprises along the chain would be known as Processors since they process the data on behalf of the Controller.[17] Under the GDPR, the transaction would now require the seller to ensure that each entity involved in the supply chain, as well as enterprises like the customer service enterprise, the credit card machine enterprise, the credit card processing enterprise, the warehouse enterprise, the packaging enterprise, the transportation enterprise, and the delivery enterprise, to not only protect the Data Subject's data, but also have the Data Subject consent explicitly and specifically to each entity having his or her data.

Each enterprise involved in the simple transaction would have to be approved by a Data Protection Authority ("DPA").[18] The DPAs could be situated in a number of locations due to the fact that each enterprise involved could be from a different country and each country would have its own DPA. Non-EU entities would have to find some other way to be approved using some other compliance tool and with the way the GDPR is currently written, their options are extremely limited.[19] The amount of money that corporations would spend on the process of complying with the GDPR would squeeze many smaller international enterprises into solely domestic businesses or force them completely out of business.[20] Larger non-EU enterprises with

---

[16] *Id.*

[17] *Id.*

[18] *See Proposed GDPR*, *supra* note 4.

[19] *Id.*

enough income would be required to acquire data processing capacities within the EU.[21] Inevitably, enterprises will be compelled to pass the cost for the additional services associated with the transaction to the consumer, hindering international trade and raising the cost for the consumer.

The GDPR has the potential to completely stop the flow and portability of data between EU and Non-EU countries.[22] It has created a huge outcry from both corporations and government organizations and resulted in the proposal of almost 4,000 amendments to the initial General Data Protection Regulation.[23] While it is important to protect the data of all the Data Subjects in the world, this attempt to balance the increase in data protection and promote the free transborder flow of data portends to have dire consequences on corporations, especially American enterprises that do business in the EU.[24]

This article aims to explain the GDPR to the reader and analyze its effect on American and other non-EU enterprises, as well as its effect on international law and international commerce. It begins by briefly explaining the process of creating the GDPR and the regulation's history as it moves along the legislative path towards ratification. The article will then compare the GDPR and the initial 1995 Data Protection Directive to determine the changes between the two in order to identify the areas that American and non-EU enterprises must focus on to proactively prepare for the GDPR's ratification. The main effect on non-EU enterprises is the

---

[20] *ICC Comments On EU General Data Protection Regulation Issues*, INT'L CHAMBER OF COM. (Jan. 15, 2013), http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2013/ICC-comments-EU-Gen-DP-Reg-Issues/.

[21] ECIPE, *supra* note 10.

[22] *Id.*

[23] Memorandum from the Eur. Comm'n, LIBE Committee Vote Backs New EU Data Protection Rules (Oct. 22, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

[24] INT'L CHAMBER OF COM., *supra* note 20.

GDPR's territorial reach that now places all international firms under its jurisdiction. This article will compare the different compliance tools non-EU enterprises currently use in order to comply with the Data Protection Directive's requirements and discuss why the GDPR's removal of these tools will lead to dire consequences for everyone involved. Finally, this article will suggest possible alternatives to the current compliance tools in order to ease the transition of complying with the GDPR.

I. THE LEGISLATIVE PROCESS

The EU consists of twenty-eight different countries known as Member States.[25] It has a government consisting of three different branches: the European Parliament, the Council of the European Union, and the European Commission, together known as the EU Institutions.[26] The European Parliament is one of the legislative branches and consists of 732 elected representatives from the Member States based on population. [27] The Members of Parliament are elected for five-year terms and divided into specialized committees and delegations based on their knowledge and expertise. [28] The Council of the European Union is another legislative branch consisting of representatives from the governments of the Member States with its composition dependent on the subjects on the agenda. [29] The Presidency of the Council is held

[25] *EU Member Countries*, EUR. UNION, http://europa.eu/about-eu/countries/member-countries/index_en.htm (last visited Apr. 2, 2015).

[26] *Process and Players,* EUR-LEX, http://old.eur-lex.europa.eu/en/droit_communautaire/droit_communautaire.htm#2 (last visited Apr. 2, 2015).

[27] *Id.*
[28] *Id*.

[29] *Id.* Keep in mind that the Council of the European Union is not to be confused with the European Council. While the Council of the European Union is a legislative body, the European Council actually consists of the Heads of State of the Member States and the President of the European Commission. The President of the European Council, who is considered the President of the European Union as a whole, leads the European Council.

in a six-month rotation by each Member State.[30] At the time of the initial GDPR proposal, the Presidency was held by Ireland; it then went to Lithuania, then Greece, and will soon be turned over to Italy.[31] The European Commission is the executive branch of the EU and consists of one member from each Member State.[32] The members are appointed by the Council for a five-year term and approved by Parliament.[33]

The European Commission has the power to initiate most laws including the GDPR, which was proposed on January 25, 2012.[34] The EU Institutions pass laws in the form of directives and regulations.[35] Directives are broad statutes that allow each Member State to enforce the directive as they see fit and in accordance with their state laws.[36] Regulations are more rigid and uniform and do not allow Member States to interpret them.[37] As the GDPR is a regulation, Member States may not interpret it as they would with a directive. Rather, Member States must adhere to it directly once it is ratified.

The GDPR takes concepts from Directive 95/46/EC ("Data Protection Directive"), which is the current data protection directive passed in 1995,[38] and combines the Member States resulting patchwork of laws in an attempt to create a strict uniform law for the European Union

---

[30] *Id.*

[31] *Council of the European Union*, EUR. UNION, http://europa.eu/about-eu/institutions-bodies/council-eu/index_en.htm (last visited Apr. 2, 2015).

[32] *Process and Players*, *supra* note 26.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *EU Law: Regulations, Directives and Other Acts*, EUR. UNION, http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm (last visited Apr. 2, 2015).

[37] *Id.*

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

as a whole.[39] The Data Protection Directive was created to acknowledge the eight Mandatory Data Protection Principles.[40] Personal data must be:

> (1) [P]rocessed fairly and lawfully; (2) obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes; (3) adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed; (4) accurate and, where necessary, kept up-to-date; (5) not be kept for longer than is necessary for that purpose; (6) processed in accordance with the rights of data subjects under the Data Protection Act; (7) appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and (8) not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[41]

Since Member States were allowed to enforce the directive as they interpreted it, a patchwork of twenty-eight separate data protection laws derived from the Data Protection Directive.[42] The GDPR attempts to combine this patchwork into one unified law and further expand data protections.[43] The concept seems like a good idea on paper but its implementation is much more difficult and detrimental without proper transition, safeguard, and compliance tools.

Once the Commission created the GDPR proposal, it was sent to Parliament and the Council, as well as the Member States' national governments, for review.[44] Almost every entity

---

[39] *See Proposed GDPR*, *supra* note 4.

[40] *Data Protection Principles*, INFO. COMMISSIONER'S OFF., http://www.ico.org.uk/for_organisations/data_protection/the_guide/the_principles?hidecookiesbanner=true (last visited Apr. 2, 2015).

[41] *Id.*

[42] *LIBE Committee Vote on Data Protection Regulation*, VPH INST. (Nov. 11, 2013), http://www.vph-institute.org/news/libe-committee-vote-on-data-protection-regulation.html.

[43] *Id.*

[44] *EU Legislative Process Updates*, WILSON SONSINI GOODRICH & ROSATI, LLP, http://www.wsgr.com/eudataregulation/process-updates.htm (last visited Apr. 2, 2015).

that received the proposal proposed amendments to it. The Irish Presidency of the Council created a new draft incorporating a number of proposed amendments in May of 2013.[45] Four committees within the Parliament, the Legal Affairs Committee, the Internal Market and Consumer Protections Committee, the Industry, Research, and Energy Committee, and The Employment and Social Affairs Committee, submitted additional amendments to The Committee on Civil Liberties, Justice and Home Affairs ("LIBE").[46] LIBE had been delegated to create the final version that was voted on by Parliament.[47] A number of lobbyists from different organizations, including the International Chamber of Commerce ("ICC"), also requested to be heard and submitted their amendments as well.[48] Due to the influx of responses, LIBE postponed its vote on the proposed draft of the Regulation four times since it first received the initial proposal.[49]

When all was said and done, the LIBE committee found itself facing 4,000 proposed amendments, and on October 21, 2013, it finally released its own version of the Regulation, which compromised the 4,000 amendments into 104 amendments.[50] LIBE voted 49-1 to approve this version and it was presented to the rest of Parliament for a vote.[51] To date, the GDPR has gone through a number of further postponements and adjournments.[52] The Member States

---

[45] *Id*.

[46] *Legislative Observatory*, EUR. PARL., http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011%28COD%29&l=en.

[47] WILSON SONSINI GOODRICH & ROSATI, LLP, *supra* note 44.

[48] INT'L CHAMBER OF COM., *supra* note 20.

[49] WILSON SONSINI GOODRICH & ROSATI, LLP, *supra* note 44.

[50] LIBE Committee Vote Backs New EU Data Protection Rules, *supra* note 23.

[51] VPH INSTITUTE, *supra* note 42.

finally decided to adjourn its implementation until at least 2015 due to the controversy and disagreement surrounding the GDPR.[53]

II. DELTAS FROM DIRECTIVE 95/46/EC

The General Data Protection Regulation differs from the Data Protection Directive in that it: (1) shifts data protection powers from the Member States to Brussels and expands the EU's territorial reach;[54] (2) creates lead supervisory authorities as governmental regulatory agencies and the need for supervisory authorities within enterprises individually;[55] (3) forces greater accountability and responsibility on controllers and processors;[56] (4) defines consent and establishes the rights of data subjects;[57] and (5) specifies a time limit for breach notice and imposes high penalties in the form of monetary sanctions.[58]

A. Powers: The Shift of Control and Expanded Territorial Reach

Above all else, Data Protection will now be enforced through a regulation instead of a directive, meaning all Member States must adhere to the regulation as written with no room for

---

[52] *EU Data Protection Regulation Tracker*, HUNTON & WILLIAMS, http://www.huntonregulationtracker.com/legislativescrutiny/#ScrutinyEUCommission (last visited Apr. 2, 2015).

[53] Kenneth Mullen and Brian Dunefsky, *European Union: On Hold: EU Data Protection Reform Delayed* (Dec. 31, 2013), MONDAQ, http://www.mondaq.com/x/283634/data+protection/On+Hold+EU+Data+Protection+Reform+Delayed.

[54] *Radical Changes to European Data Protection Legislation*, ALLEN & OVERY (Jan. 2012), http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf.

[55] *Id.*

[56] *Id.*

[57] *Data Protection Debate*, *supra* note 2.

[58] *Id.*

interpretation.[59] The Commission will also have the power to adopt further legislation in order to rectify any issues that may be presented after the Regulation goes into effect.[60] In essence, Member States will relinquish control over data protection in their individual countries. The ratification essentially allows the EU Institutions to determine how data protection is handled throughout the EU as a whole. Since all three branches of the EU government, as well as the European Council, meet in Brussels, it is said that the power behind data protection will move from the Member States to Brussels[61].

Any enterprise that collects data from a person in the EU must adhere to the GDPR.[62] The Data Protection Directive only applied to Controllers within the EU and it only prohibited the transfer of data across borders to countries that did not have "adequate" data protections.[63] The GDPR now expands the territorial reach of the EU government by requiring any Controller, no matter where it is located, to adhere to the GDPR when dealing with a person within the EU.[64] It does not matter if the actual data processing takes place within the EU or outside of its boundaries.[65] This new requirement has the greatest effect on non-EU enterprises and instantly creates the need for all international non-EU enterprises to reconsider how they conduct business with anyone in the EU.

---

[59] Press Release, Council of the Eur. Union, 3260th Council Meeting of Justice and Home Affairs (Oct. 7-8, 2013), *available at* http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/138925.pdf.

[60] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[61] *Id.*

[62] *Amended GDPR Art. 1-29*, *supra* note 3, art. 3.

[63] Council Directive 95/46, *supra* note 38.

[64] *Amended GDPR Art. 1-29*, *supra* note 3, art. 3.

[65] *Id.*

2. Authorities: Data Protection Authority, the European Data Protection Board, and Data Protection Officers.

The Data Protection Directive mandated that Member States create a number of supervisory authorities within their individual states that would assist in the enforcement of the Data Protection Directive.[66] These supervisory authorities have become known as Data Protection Authorities ("DPAs").[67] The GDPR further clarifies the idea set forth in the Data Protection Directive by instituting the requirement of one lead supervisory authority for Controllers and Processors that have offices in more than one Member State or collect and process data of Data Subjects from more than one Member State.[68] As a result, an international enterprise within multiple jurisdictions now has the ability to use one national DPA to supervise all of its data processing activities throughout all of the enterprise's locations.[69] The main location will be determined by where the main processing activities take place, or in the case of a data processor, where the place of central administration is located within the EU.[70] This simplifies the burden on multi-national corporations *within* the EU, but still does not have any positive effect on non-EU enterprises.

The GDPR furthers the concepts of co-operation and consistency by creating the European Data Protection Board ("EDPB").[71] The EDPB has exclusive jurisdiction to enforce

---

[66] Council Directive 95/46, *supra* note 38, art. 28.

[67] *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation): Compromise Amendments on Articles 30-91*, COM (2012) 0011 (Oct. 17, 2013) [hereinafter *Amended GDPR Art. 30-91*].

[68] *Id.* art. 54a.

[69] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[70] *Amended GDPR Art. 30-91*, *supra* note 67, art. 54a.

[71] *Id.* art. 64.

the GDPR in a uniform fashion.[72] It will be comprised of one head of each DPA in each of the Member States, the European Data Protection Supervisor,[73] and led by a full-time Chair.[74] The Commission will still have the authority to participate in any of the EDPB's activities and meetings, but the EDPB will act independently and will not seek or take instructions from other bodies in the performance of its tasks.[75] The EDPB shall advise the European Institutions on any questions regarding the application of the GDPR, advise on recommendations and best practices,[76] and create a report every two years regarding data protection in the EU and third countries.[77] The EDPB will become the main EU authority and will oversee the exchange of knowledge and documentation between the DPAs worldwide,[78] including a register of all warnings, breaches, and sanctions that have been collected by the DPA.[79]

To enhance the idea of co-operation and consistency, the GDPR also requires all public authorities to have an independent Data Protection Officer ("DPO") dedicated to ensuring that the data the enterprise uses is protected and the processes used adhere to the GDPR.[80] The DPO will ensure the concept of privacy by design and utilize Privacy Impact Assessments to safeguard personal data. In addition to public authorities, all international enterprises that process the personal data of more than "5,000 Data Subjects in any consecutive 12-month period" or whose

---

[72] *Id.* art. 66; *see also* 3260th Council Meeting of Justice and Home Affairs, *supra* note 59.

[73] *Amended GDPR Art. 30-91*, *supra* note 67, art. 64.

[74] *Id.* art. 69.

[75] *Id.* art. 65.

[76] *Id.* art. 66.

[77] *Id.* art. 67.

[78] *Amended GDPR Art. 30-91*, *supra* note 67, art. 66.

[79] *Id.* art. 52.

[80] *Id.* art. 35.

core activities consist of processing special category data must also have a designated and independent DPO.[81] The concept of a DPO is not new, as the Data Protection Directive allowed enterprises with an independent data protection official to have more freedoms compared to controllers that did not have an independent data protection official.[82]

The major difference is that the GDPR now *requires* a DPO.[83] The effect of this requirement is that enterprises would be forced to create and finance a position within the enterprise's management staff that is accountable solely for the enterprise's data protection responsibilities.[84] In a time where technology can easily capture the information of 5,000 people in a matter of minutes with something so simple as an online form, any enterprise with a website would be forced to create an independent DPO position.[85] Before the GDPR, one person might have had a multitude of responsibilities in a smaller enterprise; now almost every enterprise must find and pay a data protection professional. This could put smaller international enterprises in a compromising situation, as they may barely be able to stay afloat let alone try to now find and employ an individual who is designated solely to protect data.

C. Accountability and Responsibility: Privacy by Design, Maintenance of Documentation, Privacy Impact Assessments, Legitimate Interests, and Shared Responsibility Between Controllers and Processors.

---

[81] *Amended GDPR Art. 1-29*, *supra* note 3, art. 6.

[82] Council Directive 95/46, *supra* note 38, art. 18(2).

[83] *Amended GDPR Art. 30-91*, *supra* note 67. art. 35

[84] *Proposed GDPR*, *supra* note 4. art. 37

[85] *Databases And Data Capture*, BBC, http://www.bbc.co.uk/schools/gcsebitesize/ict/databases/2databasesrev1.shtml (last visited Apr. 2, 2015); *see Top Ten Data Capture Tips*, ADMA, http://www.adma.com.au/connect/articles/top-ten-data-capture-tips/ (last visited Apr. 2, 2015); *see also Methods of Data Capture*, PROCESSFLOWS, http://www.processflows.co.uk/data-capture/methods-of-data-capture/ (last visited Apr. 2, 2015).

For corporations, data collection and processing begins at the creation of a data project. For example, when an enterprise uses a website to market its product to customers, each person that signs up will enter their information into the enterprise's website and this data will then be collected and processed. This endeavor is the enterprise's data collection and processing project. The GDPR requires that enterprises now consider data protection and privacy right from the beginning of the project's creation and inception, known as "privacy by design."[86] The project is designed around the concept of privacy. Privacy by design ensures that data protection is in the forefront of enterprises' data collection and processing efforts.

The Data Protection Directive required that Controllers and Processors notify supervisory authorities before "carrying out any wholly or partly automatic processing operation or set of such operations."[87] As technology advanced since the Data Protection Directive's implementation in 1995, this requirement to notify the DPA has become obsolete. Therefore, the GDPR no longer requires it.[88] In the initial proposal of the GDPR, the notification requirement was replaced with an obligation to maintain documentation of all processing operations.[89] The amended GDPR now only requires effective procedures and mechanisms that focus on identifying risks related to the protection of personal data.[90] This lesser requirement was done in the hopes of lessening the burdens on EU enterprises. Yet, once again, this leniency does not help non-EU enterprises.

---

[86] *Privacy By Design*, INFO. COMMISSIONER'S OFF., http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design (last visited Apr. 2, 2015).

[87] Council Directive 95/46, *supra* note 38, art. 18.

[88] *Proposed GDPR*, *supra* note 4, art. 18(2).

[89] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[90] *Amended GDPR Art. 30-91*, *supra* note 67, at recital ¶70.

To comply with this lesser requirement, entities must conduct data protection Privacy Impact Assessments ("PIAs").[91] PIAs are used to analyze "how personally identifiable information is collected, used, shared, and maintained."[92] Enterprises must identify and manage risks, avoid unnecessary costs, avoid loss of trust and reputation, inform media, advocacy groups, and regulatory agencies of the organization's communication strategy, and meet and exceed legal requirements that are set forth by the Data Protection Regulation.[93] PIAs work best when they are implemented at the beginning of the data collection process, especially when the project is in its design stages.[94] This allows the enterprises that utilize the PIA to identify and repair risks before it is too late.[95] PIAs are a proactive tool that ensures compliance with the GDPR. In addition to PIAs, the GDPR also requires a compliance review to be done at least once every two years or immediately when a change in risk presents itself.[96] The documentation from both the PIAs and the compliance reviews must be made available to the appropriate DPA.[97]

In the course of processing personal data, Controllers employ and use Processors to assist in the task. Processors will now be held accountable and have direct obligations just like Controllers.[98] For example, Processors must assist Controllers in Privacy Impact Assessments,

---

[91] *Id.* art. 33.

[92] *Privacy Impact Assessments*, FED. TRADE COMM'N, http://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments (last visited Apr. 2, 2015).

[93] *See Privacy Impact Assessment Handbook*, INFO. COMMISSIONER'S OFF., *available at* http://www.rogerclarke.com/DV/ICO-2007-V2.pdf (last visited Apr. 2, 2015).

[94] *Id.* at 5.

[95] *Id.*

[96] *Amended GDPR Art. 30-91*, *supra* note 67, art. 33a.

[97] *Id.*

implementing technical and organizational measures, maintaining documentation on processing activities, and keeping the Controller informed at all stages of the data processing.[99] Data Processors must also have prior permission before they appoint a sub-processor, which is a Processor that is employed by another Processor.[100]

According to the GDPR, enterprises must also show that there are "legitimate interests" for collecting and processing data.[101] They must explain the need for transferring data with legitimate reasons explicitly approved by the DPAs.[102] There are many legitimate reasons to collect data, such as the obvious need to know where to send a product to a consumer, but the need to transfer data is less obvious. Legitimate interests to transfer data would include data security or network services, preventing fraud, direct marketing, anonymising or pseudonymising data, or keeping data for historical, statistical, or scientific reasons. [103] The Controller and Processor must meet clear requirements, such as processing in a manner of "reasonable expectation."[104] Thus, they may only process personal data in a way that is reasonably expected by the Data Subject. Any transfer request to a third country requires authorization from the national DPA before the transfer can be processed, and the data subject must be notified of the request.[105]

---

[98] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[99] *Id.*

[100] *Id.*

[101] *Amended GDPR Art. 1-29*, *supra* note 3, art. 5.

[102] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[103] *Amended GDPR Art. 1-29*, *supra* note 3, art. 6.

[104] *Data Protection Debate*, *supra* note 2.

[105] Brian Tarran, *EU Civil Liberties Committee Backs 'Right to Erasure' of Data,* RES. (Oct. 22, 2013), http://www.research-live.com/news/government/eu-civil-liberties-committee-backs-right-to-erasure-of-data/4010672.article.

D. The Rights of the Data Subject: Consent Requirements, the Right to Access, and the Right to Erasure.

For the Data Subject, data collection and processing begins with consent. The Data Subject must give clear consent.[106] Clear consent is defined as consent that is freely given and specific.[107] It must be an informed and explicit indication of the Data Subject's wishes.[108] Also, consent must be given using a statement or by a clear affirmative action.[109] Consent must be limited to purpose and the consent will expire when the purpose for which consent was given ceases to exist or the "processing of personal data is no longer necessary for carrying out the purpose for which it was originally collected."[110] The ability to withdraw consent must be as easy as it was to actually give the consent.[111] The Data Subject may withdraw consent at any time and the Controller shall inform the Data Subject if the withdrawal of consent results in termination of services.[112] Data Subject's may also submit complaints free of charge to the DPA.[113]

A Data Subject has a "Right to Access" their protected data that is being processed.[114] Controllers and Processors must respond to any request within forty (40) calendar days.[115] The

---

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Amended GDPR Art. 1-29*, *supra* note 3, art. 7.

[111] *Id.*

[112] *Id*.

[113] *Amended GDPR Art. 30-91*, *supra* note 67, art. 52.

[114] *Amended GDPR Art. 1-29*, *supra* note 3, art. 12.

Data Protection Directive requires that each request inform the Data Subject as to whether data relating to the Subject is being processed, the purpose of the processing, the categories of data concerned, the category of recipients to whom data is disclosed, communication of the data processed, and information as to the logic involved in relation to automatic decisions.[116]

The GDPR expands the "Right to Access" by requiring additional information be presented, such as the period for which personal data will be stored, the existence of the right to request, the right to rectify, the right to erase, the right to object, the right to lodge complaints, and the consequences of the data processing.[117] Controllers may no longer charge a fee for the access request.[118] Also, the time to respond to the request will be lowered to one month and specific forms to request the data will be created.[119] However, Member States will be allowed to introduce exemptions as needed.[120]

The GDPR establishes the "Right to Erasure," which was formerly known as the "Right To Be Forgotten."[121] This right allows a Data Subject to request removal from a Controller or Processor's data capture system.[122] The data includes anything that the enterprise may have collected on their own or any data that the data subject posted "on the Internet themselves."[123]

---

[115] *Id.*

[116] Nigel Parker, *Unregulated Access – The Expanded Right of Access Under the Proposed Regulation*, ALLEN & OVERY 2 (Mar. 2012), http://www.allenovery.com/SiteCollectionDocuments/Unregulated%20access%20-%20The%20expanded%20right%20of%20access%20under%20the%20proposed%20Regulation.pdf.

[117] *Id.*

[118] *Id.*

[119] *Proposed GDPR*, *supra* note 4, art. 12.

[120] *Id.*

[121] Tarran, *supra* note 105.

[122] *Id.*

[123] *Id.*

The enterprise must also "forward the request to others where the data was replicated."[124] The concept seems valid in theory, but in practice it becomes almost impossible to truly erase a subject's data. The newest version of the GDPR presented by the LIBE committee attempts to address the Right to Erasure by allowing a number of exceptions that may assist Controllers while at the same time protect Data Subjects, but the entire concept has its flaws.[125]

Data disseminates at every turn and can become impossible to trace. Enterprises will not have access to public information listed on the Internet and cannot be held accountable for the deletion of that information.[126] Once the enterprise has erased a subject from its systems, the enterprise cannot keep track of the simple fact that the subject's information should have been erased. This leaves enterprises in a "catch-22" situation where they can be sanctioned for contacting someone that they should have erased, yet the enterprise has no way of knowing that the person was supposed to be erased if they cannot store that subject's particular data in order to keep track of those who should have been erased. Also, many enterprises keep servers backed up for multiple years for compliance and legal reasons. So, enterprises would now have to go through all of their backup files in order to ensure that the subject's data is deleted upon request.[127] If the data subject requests their information be deleted but then files a claim against the enterprise later on, the enterprise no longer has any of the data subject's information and will be unable to appropriately combat the claim against them. The intricacies of this concept create a huge financial burden on enterprises.[128]

---

[124] *Id.*

[125] *Amended GDPR Art. 1-29*, *supra* note 3, art. 17.

[126] Parker, *supra* note 116.

[127] *Id.*

[128] *Id.*

The LIBE committee's version of the GDPR attempts to quell this fear by allowing a restricted processing exception if the Controller shows they would need the data for "the purposes of proof."[129] Under the exception, the Controller or Processor would restrict the processing of personal data so that it is not the subject of normal data access.[130] Further, processing operations and personal data could no longer be changed in anyway.[131] This exception essentially invalidates the entire "Right to Erasure" concept as all enterprises could show a necessity to keep data for "the purposes of proof."[132] Therefore, the "Right to Erasure" should be amended to the "Right to Restriction." This would achieve the goal of protecting a Data Subject's personal data from being further disseminated and also assist the Controller in keeping a record of the Data Subject's personal data in order to protect the Controller from any claims that could arise.

E. Breach: Notice and Sanctions

If a breach occurs, the GDPR requires notification without undue delay to the DPA even if the breach was harmless.[133] Undue delay is presumed to be within seventy-two (72) hours and enterprises that do not comply will face sanctions.[134] A breach can be any event or action that would result in an adverse effect on personal data or privacy of a Data Subject including identity theft, fraud, physical harm, significant humiliation, or damaged reputation.[135] The notification

---

[129] *Amended GDPR Art. 1-29*, *supra* note 3, art. 17(4).

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Data Protection Debate*, *supra* note 2; *Amended GDPR Art. 1-29*, *supra* note 3, ¶67.

[134] *Data Protection Debate*, *supra* note 2.

must include a description of the breach including the types of data and number of Data Subjects concerned, the DPO's name and contact information, recommendations on how to mitigate the breach, a description of the consequence of the data breach, and the steps the enterprise has taken to address the breach.[136] The Controller/Processor must keep detailed documentation in regards to the breach including the surrounding facts, its effects, and the remedial action taken.[137]

The Controller must show the DPA that it has implemented sufficient technological protection measures to render the data unintelligible to those not authorized to access it.[138] If the Controller is unable to do so, the enterprise must also notify the Data Subject, whose personal data was breached, without undue delay.[139] The communication must be in comprehensive, clear, and plain language and include the same information that was sent to the DPA in the breach notification.[140]

Corporations can be punished for any inconsistencies through sanctions.[141] Sanctions will take into account the nature, gravity, and duration of incompliance, the intentional or negligent character of the infringement, the degree of responsibility, the previous breach history, the degree of cooperation with the DPA, the level of damage, the actions taken to mitigate the breach, the financial benefit gained or the loss avoided by breach, the degree of technical or organizational measures implemented to prevent breaches, and any other aggravating or

---

[135] *Amended GDPR Art. 1-29*, *supra* note 3, ¶67.

[136] *Amended GDPR Art. 30-91*, *supra* note 67, art. 31.

[137] *Id.*

[138] *Id.* art. 32.

[139] *Id*.

[140] *Amended GDPR Art. 30-91*, *supra* note 67, art. 32.

[141] *Id.* art. 79.

mitigating factors.[142] The possible sanctions include written warnings, regular and periodic audits, fines of €100,000,000, or up to five percent (5%) of their worldwide turnover.[143] These high and unfair monetary sanctions could easily cripple international enterprises if they are handed out arbitrarily.

III. TRANSFERS TO THIRD COUNTRIES OUTSIDE OF THE EU

The Data Protection Directive and the GDPR both prohibit the transfer of personal data outside of the EU to third countries that do not have "adequate" protections and safeguards.[144] Adequacy is determined by a number of factors including the third countries': (1) rule of law that allows effective administrative and judicial redress for Data Subjects; (2) independent supervisory authority with sufficient sanctioning powers; and (3) legally binding instruments and conventions with regard to personal data protection.[145] At the moment, the only countries outside of the EU that are considered to adequately safeguard personal data are Andorra, Argentina, Canada Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay.[146]

Other non-EU enterprises currently use compliance tools such as Safe Harbor, EU Model Clauses, and Binding Corporate Rules to comply with the current Data Protection Directive.[147]

---

[142] *Id.*

[143] LIBE Committee Vote Backs New EU Data Protection Rules, *supra* note 23.

[144] *Amended GDPR Art. 30-91*, *supra* note 67, art. 41.

[145] *Id.* art. 41(2).

[146] ECIPE, *supra* note 10.

[147] Jeremy M. Mittman, *EU Working Party Adopts Model Application Form for Binding Corporate Rules,* PROSKAUER (Mar. 8, 2007), http://privacylaw.proskauer.com/2007/03/articles/european-union/eu-working-party-adopts-model-application-form-for-binding-corporate-rules/.

These tools allow enterprises outside of the EU the ability to comply with the Data Protection Directive without creating unnecessary restrictions on them from a government that has limited jurisdiction over them.[148] Without these compliance tools, it would be nearly impossible for non-EU enterprises to conduct business and trade with people in the EU because the Data Protection Directive forbids the dissemination of personal data outside of the EU to any third party that does not have "adequate" data protection safeguards.[149]

The US-EU Safe Harbor Framework Agreement ("Safe Harbor") was created to respect the data protection established by the Data Protection Directive while still allowing uninterrupted flows of data between the United States and the EU.[150] The seven principles of Safe Harbor are notice, choice, onward transfer, access, security, data integrity, and enforcement.[151] The Safe Harbor principles directly correlate to the Data Protection Directives data protection principles.[152] American enterprises participating in Safe Harbor self-certify that they are providing "adequate protection" for transferring personal data from the EU to the US.[153] The

---

[148] *Id*.

[149] *Id.*

[150] Damon Greer, *Safe Harbor May Be Controversial in the European Union, But It Is Still the Law*, THE PRIVACY ADVISOR (Aug. 27, 2013), https://www.privacyassociation.org/publications/safe_harbor_may_be_controversial_in_the_european_union_but_it_is_still_the; W. Gregory Voss, *Preparing for the Proposed EU General Data Protection Regulation: With or Without Amendments,* A.B.A. (Nov. 19, 2012), http://apps.americanbar.org/buslaw/blt/content/2012/11/article-02-voss.shtml.

[151] *Federal Trade Commission Enforcement of the US-EU and US-Swiss Safe Harbor Frameworks*, FED. TRADE COMM'N (Dec. 2012), https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor.

[152] Amy Worley, *FTC Serious About Safe Harbor Framework Enforcement*, MONDAQ (Feb. 10, 2014), http://www.mondaq.com/unitedstates/x/291886/data+protection/FTC+Serious+About+Safe+Harbor+Framework+Enforcement.

[153] Belinda Doshi and Robyn Chatwood, *European Union: Is "Safe Harbor" No Longer Safe? EU to Review Regime for Personal Data Transfers to the US*, MONDAQ (Aug. 9, 2013),

process is a self-regulatory framework that is enforced by the U.S. Federal Trade Commission ("FTC").[154] There are more than 4,000 entities currently using the Safe Harbor program and over seventy (70) new applications every month.[155]

Safe Harbor only applies to enterprises under the jurisdiction of the FTC and the Department of Transportation ("DoT").[156] This means that enterprises within finance (banks, investment houses, credit unions, and savings & loans institutions), telecommunications, labor, non-profit, agriculture, and meat processing are not automatically eligible to use Safe Harbor as a compliance tool in regards to data protection.[157] It can be argued that Safe Harbor has helped to increase the interest in privacy protection in the U.S. since its inception, but the self-regulatory aspect has been under constant fire and criticism.[158] In fact, the European Parliament released a draft report and resolution that looks to establish a "European digital habeas corpus" that would suspend Safe Harbor.[159] Safe Harbor's demise would be detrimental to the 4,000 entities that use it, as well as the new enterprises looking to expand into the international market.

Incorporating EU Model Clauses within contracts is another way to comply with the Data Protection Directive.[160] They allow the transborder transfer of data and hold the parties involved

---

http://www.mondaq.com/x/256996/data+protection/Is+Safe+Harbor+No+Longer+Safe+EU+To+Review+Regime+For+Personal+Data+Transfers+To+The+US.

[154] Damon Greer, *Safe Harbor – A Framework that Works*, 1 INT'L DATA PRIVACY L. 143, 146 (2011).

[155] *Id.*

[156] *Eligibility for Self-Certification,* U.S. DEPT. OF COM., http://export.gov/safeharbor/ (last updated July 1, 2013).

[157] *Id.*

[158] *Safe Harbor – A Framework that Works*, *supra* note 154.

[159] Donald Aplin, *12 Companies Settle FTC Charges Of Falsely Asserting U.S.-EU Safe Harbor Compliance*, BLOOMBERG BNA (Jan. 27, 2014), http://www.bna.com/12-companies-settle-n17179881618/; *see also Draft Report On The Electronic Mass Surveillance of EU Citizens,* 2013/2188 (INI), (Dec. 23, 2013), *available at* op.bna.com/pl.nsf/r?Open=dapn-9f5kyk.

accountable.[161] Controllers must incorporate standard contractual clauses into their service agreements that are approved by the Information Commission.[162] The clauses are based upon the Mandatory Data Protection Principles.[163] Each clause must be entered exactly as written otherwise the Information Commission will not guarantee that adequate safeguards are provided and the effectiveness of the modification may be challenged.[164] Also, the data exporter and importer must accept liability for any breach and cross indemnify each other to ensure that one of them would be held responsible in case of a data breach.[165] Overall, these clauses are an attempt to protect data through contractual means and any deviation would be considered a breach of contract.[166] The downside behind EU Model Clauses is that they require hundreds of separate contracts in order for large companies to comply because each transaction would require a separate contract with an EU Model Clause.[167]

Binding Corporate Rules ("BCRs") are legally binding corporate codes of conduct that allow data handling systems to be EU-compliant.[168] An international enterprise uses BCRs to

---

[160] Memorandum from the Eur. Comm'n, Decision Updating the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Non-EU Countries PINCITE (Feb. 5, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/memo_10_30_en.pdf [hereinafter *Decision Updating the Standard Contractual Clauses*].

[161] *Id.*

[162] *Id.*

[163] *Model Clauses for Transferring Personal Data Overseas: An Overview*, PINSET MASONS LLP, http://www.out-law.com/page-8172 (last updated May 2010).

[164] *Model Contract Clauses: International Transfers of Personal Data*, INFO. COMMISSIONER'S OFF., http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/model_contract_clauses_international_transfers_of_personal_data.ashx (last visited Apr. 2, 2015).

[165] *Decision Updating the Standard Contractual Clauses*, *supra* note 160.

[166] *Id.*

[167] Memorandum from the Eur. Comm'n, Restoring Trust in EU-US Data Flows – Frequently Asked Questions (Nov. 17, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

create an internal data protection system that allows it to transfer data within the enterprise and among its partners and subsidiaries.[169] In order to use BCRs, the enterprise must have the rules approved by a DPA within a Member State.[170] Once it is approved in one Member State, the BCRs are forwarded to other DPAs in other Member States for approval.[171] The entire process is extremely complex, complicated, confusing, and time-consuming.[172]

BCRs can be an effective compliance tool, but they are very often costly to implement which would bar many small to medium size enterprises from using them.[173] There are only a few enterprises that possess the necessary income required to hire specialized law firms that can actually create and develop BCRs that are effective; enterprises such as General Electric, Hewlett Packard, Intel, Michelin, and Shell do not represent the entire international commerce community.[174] Also, BCRs only apply to transfers of data within one corporate group.[175] So, for non-EU firms to actually use them, they would need to establish an office within the EU.[176]

Almost all non-EU enterprises request the continued ability to use these compliance tools in order to comply with the GDPR, but the most recent amended version of the GDPR limits the

---

[168] Mittman, *supra* note 147.

[169] *Id.*

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] ECIPE, *supra* note 10, at 9.

[174] *See* K. Royal, *The ABCs of BCRs*, IAPP (May 13, 2013), https://www.privacyassociation.org/privacy_perspectives/post/the_abcs_of_bcrs; *see also List of Companies for Which the EU BCR Cooperation Procedure is Closed,* EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (last updated Feb. 20, 2015).

[175] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

[176] *Id.*

use of compliance tools.[177] The GDPR acknowledges and recognizes only BCRs as a tool to transfer data across borders into states outside of the European Economic Area ("EEA").[178] To require such strict data protection requirements and then allow only one form of compliance for non-EU enterprises creates a death grip on international commerce and stifles the international flow of data.

IV. GDPR'S EFFECT ON NON-EU ENTERPRISES

The GDPR will have the greatest effect on two major democratic powers: The United States and India.[179] Together, the European Union and the United States account for half of the world's GDP and 2.4 trillion EUR in bilateral investments.[180] The value of EU-India trade in 2011 was 79.9 billion EUR and India is one of the most prominent data processing destinations.[181] Other major trading partners affected by the GDPR would include Japan, Singapore, and Korea.[182] These countries all have privacy legislation that protects personal data, but the EU does not *recognize* them as countries with adequate safeguards like the ones created with the GDPR.[183]

---

[177] *See Proposed GDPR*, *supra* note 4.

[178] *Radical Changes to European Data Protection Legislation*, *supra* note 54.

[179] ECIPE, *supra* note 10.

[180] *Id.*

[181] *Countries and Regions: India*, EUR. COMM'N, http://ec.europa.eu/trade/policy/countries-and-regions/countries/india/ (last visited Apr. 2, 2015).

[182] ECIPE, *supra* note 10, at 8.

[183] *Id.*

For example, American data protection has a foundation based upon the Fourth Amendment of the Constitution and its protection from illegal search and seizure.[184] Instead of one general and uniform law across the states, data protection in America is accomplished using a patchwork of legislation, similar to the EU's current patchwork of laws stemming from the Data Protection Directive. [185] The United States uses privacy laws and regulatory compliance laws to achieve its goal of protecting citizens' data and applies different laws to different situations.[186] Comparatively, the American patchwork still is not as in depth as its European counterpart, but it does protect personal data.[187]

The United States has established a number of laws that each state must adhere to, such as the Federal Trade Commission Act ("FTC Act"), the Financial Services Modernization Act ("Gramm-Leach-Bliley Act"), the Health Insurance Portability and Accountability Act ("HIPAA"), the HIPAA Omnibus Rule, Security Breach Notification Rule, the Fair Credit Reporting Act, Fair and Accurate Credit Transaction, the Controlling of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"), the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, and the Computer Fraud and Abuse Act.[188]

---

[184] *Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States,* U.S. DEP'T. OF STATE, http://photos.state.gov/libraries/useu/231771/PDFs/Five%20Myths%20Regarding%20Privacy%20and%20Law%20Enforcement_October%209_2012_pdf.pdf (last visited Apr. 2, 2015).

[185] Ieuan Jolly, *Data Protection in United States: Overview*, LOEB & LOEB LLP (July 1, 2013), http://uk.practicallaw.com/6-502-0467#null; Cecile Martin, *Navigating the Patchwork: When is European Data Privacy Law Applicable to US Companies?*, PROSKAUER (Apr. 17, 2013), http://privacylaw.proskauer.com/2013/04/articles/online-privacy/navigating-the-patchwork-when-is-european-data-privacy-law-applicable-to-us-companies/.

[186] *United States Privacy Laws*, INFO. SHIELD, http://www.informationshield.com/usprivacylaws.html (last visited Apr. 2, 2015); *Regulatory Compliance: Security Policy and Organization*, INFO. SHIELD, http://www.informationshield.com/compliance.html (last visited Apr. 2, 2015).

[187] Richard Adhikari, *America's Perilous Patchwork of Privacy Laws*, TECHNEWSWORLD (Mar. 18, 2011), http://www.technewsworld.com/story/72092.html.

Additionally, many states have their own privacy laws, especially states like California, that attempt to patch the holes created by the federal laws.[189] These laws in combination with compliance tools like Safe Harbor should satisfy EU data protection standards adequately enough to allow data to flow transborder into the U.S.

V. THE EU-US DATA PROTECTION CONTROVERSY

The EU Institutions are unsatisfied with the United States' approach to data protection and after the most recent surveillance scandal, the Commission has released a list of thirteen data protection recommendations for the U.S.[190] These thirteen recommendations incorporate the data protection concepts of transparency, redress, enforcement, and access.[191]

The transparency and redress ideas help to protect EU citizens directly. The transparency concept requires the U.S. to ensure their enterprises publically disclose privacy policies, which include a link to the Department of Commerce Safe Harbor website, publish privacy conditions of contracts enterprises have with subcontractors, and clearly flag all enterprises that are not a part of Safe Harbor on the Department of Commerce Safe Harbor website.[192] The redress concept requires the U.S. to ensure its enterprises have links to alternative dispute resolution ("ADR") providers on their website that are readily available and affordable.[193] The Department

---

[188] Jolly, *supra* note 185.

[189] *United States Privacy Laws*, *supra* note 186; Jolly, *supra* note 185.

[190] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

[191] *Id.*

[192] *Id.*

[193] *Id.*

of Commerce must monitor the ADR providers to ensure they are abiding by rules that are set forth.[194]

The enforcement and access ideas help to police U.S. enterprises. The enforcement concept requires the U.S. to perform investigations to ensure enterprises are complying with Safe Harbor. [195] If an enterprise is found to be non-compliant a further specific investigation should be held one year later to ensure corrective measures were put in place.[196] The U.S. must also investigate any false claims of Safe Harbor compliance. When the Department of Commerce has doubts to an enterprise's compliance with any EU data protection standard, it must inform the appropriate EU DPA.[197] The access concept requires U.S. authorities to review privacy policies to ensure that exceptions to data protection standards for national security, public interest, and law enforcement are necessary and appropriate.[198]

The EU Institutions dispute the validity and self-regulatory nature of Safe Harbor and the actual reach of the FTC's enforcement powers.[199] However, just as a DPA would oversee and sanction an enterprise in the EU, the FTC has also served as a sufficient and aggressive enforcer of data protection in the United States. For instance, one major argument against Safe Harbor is that a number of companies have claimed to be Safe Harbor certified when in actuality they were not.[200] The FTC has charged twelve different enterprises for falsely asserting compliance with

---

[194] *Id.*

[195] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] Aplin, *supra* note 159.

Safe Harbor.[201] All twelve enterprises were previously certified under Safe Harbor but their certifications had lapsed.[202] The enterprises involved National Football League teams, as well as a major communications company.[203] The firms involved all had websites stating that they were current with their Safe Harbor compliance and therefore were all charged with making false claims.[204] Even though none of the charges alleged any substantial violations of the Safe Harbor data protection principles, the FTC has made a point to show that it respects EU data protection guidelines.[205]

The other main issue that the EU Institutions have with the U.S. in regards to data protection is that the EU citizen has no power to seek redress.[206] In the U.S., non-citizens seek judicial redress for wrongs committed against them in federal court.[207] Federal Courts hear cases involving laws and treaties of the U.S,[208] as well as hear cases involving subjects and citizens of foreign states.[209] People in the EU could file claims and seek damages against American

---

[200] *Is The Safe Harbor Program Still Safe?*, ALLEN & OVERY (Oct. 2, 2013), https://www.aohub.com/aoos/viewContent.action?key=Ec8teaJ9VaqLGpSUqS%2FLgl7eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JAvAvaah9lF21%0D%0ACiGG39vtfQ%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ%2FHLCIrtYuIY%3D&uid=frsvcLdHNrI%3D&popup=HxapDW%2FMKd4%3D&freersslink=true.

[201] Aplin, *supra* note 159.

[202] *Id.*

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

[207] *Jurisdiction Of The Federal Courts*, U.S. CTS., http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/Jurisdiction.aspx (last visited Apr. 2, 2015).

[208] *Id.*

[209] 28 U.S.C. § 1332(a)(2) (2014).

enterprises that violate U.S. laws that protect personal data.[210] The major issue is that U.S. laws do not protect EU citizens.

For example, the 1974 Privacy Act only protects U.S. citizens and permanent residents.[211] This means that even if an American enterprise violates the 1974 Privacy Act by illegally transferring an EU citizens personal data, the EU citizen will not be able to seek judicial redress in the American court system because they were not protected under the law. This is a valid concern but how can the EU expect the U.S., or any other third country for that matter, to create legislation that protects or controls citizens that are not under their jurisdiction?

VI. THE RIGHT TO CHOOSE – THE GDPR'S MISSING LINK

Until new data protection laws are ratified within the U.S. and other third countries, the EU Institutions should allow Data Subjects to consent as to whether or not they would allow a non-EU enterprise to process their data knowing that once it crosses the EU borders, it is not under the jurisdiction of the GDPR. This allows the Data Subject the "Right to Choose" how and where they want their personal data processed. Essentially, the GDPR's all-encompassing and widespread ban actually hinders the Data Subjects' rights. If the Data Subject wants his personal data to be processed by a non-EU firm, then that should be the Data Subject's uninhibited choice. This ability to consent truly allows uninhibited transborder data flow.

EU Model Clauses and BCRs are simply contractual statements to which enterprises agree. There is no magical power behind them. In the same respect, Safe Harbor is another form

---

[210] U.S. CTS., *supra* note 207.

[211] Restoring Trust in EU-US Data Flows – Frequently Asked Questions, *supra* note 167.

of contractual compliance. When enterprises utilize these compliance tools, they are simply entering into contracts with each other to be responsible for the safe processing and storing of data. If the EU Institutions are not willing to accept that other States can provide proper safeguards to personal data and enforce them amongst their respective enterprises, then the people in the EU should be allowed to decide whether or not they want to do business with enterprises outside of the EEA.

The GDPR has entire sections dedicated to clear consent and therefore should extend consent to include the "Right to Choose." International trade and commerce depends on transborder data flow and each person should have the "Right to Choose" how their own personal data will be processed. If the Data Subject does not want to have their data processed outside of the EEA, then it can refrain from giving consent or withdraw consent when notified that the data will be traveling outside of the EEA zone. The Data Subject has a number of rights and the "Right to Choose" is their most important one in regards to personal data protection.

CONCLUSION

The EU Institutions' push to protect the individuals fundamental right of privacy and personal data protection is understandable. There is a definite need for legislation that will allow a Data Subject the ability to control the use of his personal data. But, broad sweeping legislation is not the answer especially when the legislation attempts to force jurisdiction over other sovereign nations and their enterprises. In fact, the GDPR pushes the boundaries of the EU's international law without allowing proper compliance tools that allow enterprises to conform. The GDPR's attempt to use a "one size fits all" resolution to a worldwide problem will not work.

The GDPR must be further amended to allow a more widespread method of compliance or allow the Data Subject to make their own decisions on the protections of their own personal data.