GDPR: European Regulation with Global Reach

A Simplified but Sophisticated Overview for U.S. Companies

by Annmarie Giblin

CHUBB®

The GDPR provides protection for the personal data of EU residents wherever their data may travel and attempts to protect this personal data on a global basis.

Information has always been a valuable asset: protected, traded and stored since the dawn of the written word. In today's interconnected world, however, information is also a valuable commodity, with entire industries built around the collection, processing and extraction of value out of all types of information. By the same token, an underbelly of this industry has also emerged, focused on illegally obtaining this new perceived commodity and profiting from it. Cyber security incidents largely fuel this illegal taking and are a constant threat to industries and organizations of all sizes. While the cyber security incident itself will usually garner a lot of scrutiny and attention, the larger question of how and why the compromised information was obtained in the first place was historically overlooked. Over time, the protection of that information has been a focus of attention, and has prompted a variety of regulatory efforts.

The regulatory effort gaining the most attention recently has been the European Union's (EU) passage of the General Data Protection Regulation (GDPR). The GDPR not only takes a significant step forward in asserting and protecting the privacy rights of EU residents, but also requires increased security measures to protect their data.

Perhaps more importantly, the GDPR provides protection for the personal data of EU residents wherever their data may travel and attempts to protect this personal data on a global basis. The GDPR has been a significant media story in the EU since its passing, but has only recently, in the lead up to enforcement, received media attention in the U.S. However, on May 25, 2018, the GDPR became fully enforceable, including its international reach, which can touch organizations in the U.S. who deal with the personal information of EU residents. Thus, ready or not, any organization that deals with this information should be prepared.

This discussion paper provides a general overview of some of the more important sections of the GDPR, as well as some background on EU privacy regulations in general. It is important to note that the GDPR is massive, with 11 chapters and 99 articles.[1] A sufficient compliance plan will take time and thought to prepare, and should include input from experts from the legal, privacy and cyber security communities.

Before the GDPR: A Brief History of Privacy in the EU

On April 14, 2016, the GDPR was approved by the EU Parliament. It was published in the EU Official Journal on April 27, 2016, and became fully enforceable on May 25, 2018. Among other contributing factors, such as the rapidly changing technological landscape, two events helped to contribute to the enactment of the GDPR: the *Weltimmo* case in the EU Court of Justice and the collapse of the Safe Harbor Agreement between the EU and the U.S.[2]

First, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, Case C-230/14, highlighted the need for one EU general privacy regulation. Since 1995, the EU has followed the Data Protection Directive 95/46/EC (Data Protection Directive), which provided a general blueprint for EU Member States to follow when enacting their own privacy laws. The Data Protection Directive was established on October 24, 1995, and remained in full effect until the GDPR took over in May 2018. When it was enacted, the Data Protection Directive was described as the EU's "answer to the division of privacy regulations across the EU. Its major goals included the harmonization of data protection laws and the transfer of personal data to 'third countries' outside of the Union.'" [3]

Prior to the Data Protection Directive, each EU Member State had its own privacy laws. The only consistency between those laws was the fact that they were loosely based on the Organization for Economic Co-operation and Development (OECD) guidelines. The OECD guidelines[4] provided general principles on the protection of privacy and transfers of data, but were non-binding and the laws that were based on them "varied greatly even amongst different EU member states."[5] The Data Protection Directive was meant to remedy this by providing a more formal and cohesive blueprint for privacy regulation, while still allowing the Member States to enact their own individual laws.[6] Despite being more formal, the Data Protection Directive also ended up creating a patchwork of privacy laws across the EU, all with different applications and enforcement. This patchwork and the problems it created were highlighted by the *Weltimmo* case.

Specifically at issue in the *Weltimmo* case was whether or not a company had to comply with the privacy laws in one Member State where it did business, when it was in fact "established" or physically located in a different Member State. The EU Court of Justice provided a detailed analysis of how the term "established" had changed in light of the nature of online business and could no longer be limited to only include a physical location of a business. Indeed, the Court explained that:

> It is necessary to examine the specific nature of undertakings which operate exclusively via the internet, whose business model diminishes the importance of the concept of fixed establishment and also has a bearing on the extent of the human and material resources. In some circumstances, an agent who is permanently present, equipped with little more than a laptop computer, can constitute a sufficient structure for the purposes of engaging in the effective and real exercise of an activity with a sufficient degree of stability.[7]

The EU Court of Justice in *Weltimmo* held that organizations that have such a sufficient structure in a Member State, "such as the presence of human and technical resources…" must comply with the privacy laws of that Member State, regardless of whether or not it is actually physically established in that State.[8] The *Weltimmo* case highlighted not only the uneven nature of the privacy laws across the EU, but provided an example of how many organizations were forum shopping by being physically "established" in a Member State with more favorable privacy laws, while still doing business in other Member States and using their establishment to avoid compliance with that State's laws.

Second, the collapse of the Safe Harbor Agreement highlighted the need for more oversight into third country transfers. The Safe Harbor Agreement allowed data transfers between the EU and the U.S. in accordance with the regulations of the Data Protection Directive. Specifically, the Data Protection Directive provided that the processing of data in third countries was only allowed if there were "guarantees to ensure that the rights and obligations provided for in [the] directive are respected in practice."[9] In order to facilitate such transfers, adequacy decisions were issued to certify that transfers to certain third countries and organizations were in compliance with the directive. On July 26, 2000, the EU Commission issued adequacy decision 2000/520/EC, better known as the Safe Harbor Agreement, which provided "a legal basis for the transfer of personal data from the European Union to undertakings established in the United States that adhere to the safe harbor principles."[10] It allowed U.S. companies to self-monitor and self-certify that they were in compliance with EU privacy regulations when it came to the handling and processing of the personal data of EU residents. This was very important for U.S. companies that did business in the EU as it allowed them to transfer data out of the EU to their main locations in the U.S. Without the Safe Harbor Agreement, U.S. organizations would have had to have implemented another legal ground in order to legally transfer the data, which would generally require more effort, greater sophistication, and/or complexity than certifying under the Safe Harbor Agreement. Thus, the Safe Harbor Agreement was an important tool for U.S. organizations that needed to transfer such data.

The Safe Harbor Agreement lasted 15 years and was ultimately brought down by a complaint made by Maximillian Schrems. On June 25, 2013, Schrems lodged a complaint with the EU commissioner claiming "that the law and the practices of the US offer no real protection of the data kept in the United States against State surveillance."[11] Schrems argued that following the revelations made by Edward Snowden in May 2013 concerning the activities of the U.S. intelligence services, in particular those of the National Security Agency, it was impossible for the U.S. or any U.S. organization to comply with the Data Protection Directive, thereby rendering the Safe Harbor Agreement useless.[12] After working its way through the Courts, the case was presented to the EU Court of Justice, which agreed with Schrems and, on October 6, 2015, declared that the Safe Harbor Agreement was invalid.[13]

Since the Safe Harbor Agreement provided the legal justification for data transfers between the EU and the U.S. for data in many U.S. organizations, its collapse was troubling. Thus, in order to allow the flow of data once again, the Privacy Shield Framework (Privacy Shield) was created to take its place.

Privacy Shield is very similar to the Safe Harbor Agreement with some notable upgrades. Specifically, it provides for more detailed and enhanced data privacy principles to be adhered to and "contains commitments from U.S. national security officials, as well as letters from U.S. government officials, concerning the protections afforded by Privacy Shield to data from EU citizens."[14] Privacy Shield also provides several avenues of recourse against organizations that do not adhere to the privacy principles. Specifically:

- An EU data subject can complain directly to the U.S. organization, which must have a complaint mechanism in place in order to comply with the Privacy Shield.

- The EU data subject can also submit a complaint to its local Data Protection Authority or bring a legal action in its home Member State against the U.S. organization.
- They can also complain to the U.S. Department of Commerce and the Federal Trade Commission or to a special arbitration panel created to deal with such disputes.
- The EU data subjects can bring a legal action in the U.S. courts.[15]

On June 12, 2016, Privacy Shield was deemed adequate by the EU Commission and is still in effect today.[16]

The Privacy Shield underwent its first annual review in September 2017.[17] After spending two days reviewing the framework, the EU Commissioner for Justice, Consumers and Gender Equality, Vera Jourová, stated that the discussions were fruitful and declared that the "Privacy Shield can be a win-win for the EU and the U.S., if implemented correctly."[18] On October 18, 2017, the EU Commission released its first annual report on the functioning of the EU-U.S. Privacy Shield.[19] The report concluded that "the Privacy Shield continues to ensure an adequate level of protection for the personal data transferred from the EU to participating companies in the U.S.," but also listed several recommendations to "ensure the continued successful functioning of the Privacy Shield."[20]

After reviewing the EU Commission's report, on November 28, 2017, the Article 29 Data Protection Working Party issued its own report on the findings of the review.[21] The Article 29 Data Protection Working Party's report was much more critical of the Privacy Shield than the EU Commission's report. In their report, the Article 29 Data Protection Working Party "identified a number of significant concerns" that they concluded needed to be addressed and, as a result, called "upon the Commission and the U.S. competent authorities to restart discussions."[22] The Article 29 Data Protection Working Party threatened to bring the Privacy Shield Adequacy decision, which is the formal legal basis for the Privacy Shield, to the national courts if their concerns were not addressed.[23] To date, no formal proceedings have been brought.

Similar to the Data Protection Directive, the GDPR will continue to regulate data transfers to third party countries and also has a provision for issuing adequacy decisions. Additionally, the GDPR allows prior adequacy decisions, such as the Privacy Shield, to remain in effect unless repealed, amended or replaced by commission decree.[24] Thus, the Privacy

Shield will continue to be in effect under the GDPR as it has been deemed adequate by the EU Commission after its first review, but its future status remains in peril as long as the formal concerns of the Article 29 Data Protection Working Party are unresolved.

GDPR

It is important to remember that the GDPR is overall a privacy regulation and, while it does mandate cyber security protections, its focus is the collection, use and disposal of the personal information of EU residents.

U.S. organizations that deal with the personal data of EU residents in the U.S. should either already be certified under Privacy Shield or have some other mechanisms in place to ensure compliance with the EU Data Protection Directive. As noted previously, this is important so that any data transfers out of the EU to the U.S. do not violate EU law. Beyond Privacy Shield, organizations can use, among other things, Binding Corporate Rules, model contract clauses and obtained consent of the EU data subjects to ensure legal data transfers.[25] Programs that are currently in compliance with the Data Protection Directive, however, likely still need upgrades to be in compliance with the GDPR.

Important General Provisions

The GDPR only applies to "the processing of personal data" in the EU and the personal data of data subjects who are in the EU, regardless of whether or not the processing is undertaken there.[26] It does not apply to non-personal data and, in fact, the EU is currently exploring new regulations to address the privacy concerns of non-personal data.[27] Personal data is defined as "any information relating to an identified or identifiable natural person (data subject)..."[28] A data subject is identifiable if they can be "identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, generic, mental, economic, cultural or social identity of that natural person."[29] Processing is defined as an operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, organizing, storing, using, altering and erasing.[30] A data breach is defined as "a breach in security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."[31]

The GDPR applies to controllers and processors of personal data. Controllers are defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data..."[32] Processors are defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[33] In simpler terms, an organization or business that defines how to collect and use personal data is considered a controller; a company hired under specific written instructions to collect, organize or otherwise manipulate the data is a processor. Both the controller and the processor are responsible for ensuring that the processing and security of the data is in compliance with the GDPR.[34]

Transfers to third countries such as the U.S. and international organizations are only allowed if the provisions of the GDPR are complied with by both the controller and the processor. As noted previously, the GDPR allows for "adequacy decisions," which are required to be reviewed every four years.[35] Adequacy decisions can also be made as to individual organizations, regardless of what country the organization is in.

Personal Privacy Principles

The GDPR mandates six principles to follow when processing the personal data of data subjects. Demonstrated compliance with these principles must be maintained as well. The six principles are:

1. 1Personal data should only be processed lawfully, fairly and in a transparent manner.
2. Personal data should only be collected for a specific and legitimate purpose and not further processed for any other purpose.[36]
3. Only the personal data that is adequate, relevant and limited to what is necessary for its purpose should be collected.
4. Personal data collected should be accurate and up to date, and reasonable steps must be taken to ensure that inaccurate data or data not related to the legitimate purpose for processing be erased.
5. Personal data should not be kept longer than necessary for the purpose of why it is being processed.
6. Personal data must be processed in a way that ensures the appropriate security of the data.[37]

Additionally, the processing of data must be lawful. The GDPR mandates that processing will be lawful ONLY if one or more of the six grounds apply:

1. The data subject gives specific consent.[38]
2. Processing is necessary for the performance of a contract to which the data subject is a party or to comply with the data subject's request to enter into a contract.
3. Processing is necessary to comply with a legal obligation that the controller has.

4. Processing is necessary to protect the vital interests of the data subject or another person.
5. It is necessary to perform a task in public interest.
6. It is necessary for the purpose of a legitimate interest pursued by the controller or by a third party, except when such interests are overridden by the interests or a fundamental right and freedom of the data subject, especially when the data subject is a child.[39]

The GDPR prohibits the processing of special categories of personal data that reveal racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health or sexual orientation, or information about a data subject's sex life, unless one of the other conditions is met. For example, if the data subject has given explicit consent or makes this information public, then it can be processed.[40] Unless other grounds apply, personal data concerning criminal convictions can only be processed under official authority.[41]

Rights of the Data Subject

Additionally, the GDPR provides for the enhancement of the rights of data subjects with regards to their personal data. There are a few fundamental rights that must be respected:

1. **Right of access** – the data subject has the right to request information from an organization, such as what type of data it has on the data subject, which must be provided free of charge and in an easy-to-read format. Additionally, the following information must be provided, usually by means of a privacy notice to the data subject when directly collecting the data from them:
   a. Identity and contact information of the controller and data protection officer
   b. The purpose(s) and the legal basis for the processing
   c. If the processing is based on a "legitimate" interest of the controller, then the legitimate interest must be provided
   d. The recipients or category of recipients of the data, if any
   e. Whether or not the controller intends to transfer the data to a third country or international organization, and the existence or absence of an adequacy decision
   f. The period of time that the data will be stored
   g. If processing is based on consent, the right to withdraw the consent
   h. The right to lodge a complaint with a supervisory authority
   i. If the processing is necessary because of a contract, then it must be communicated as to whether or not the data subject is required to provide the data and the possible consequences of not providing the data
   j. The existence of automated decision-making processes and meaningful information about the logic involved, as well as the significance and envisaged consequences of the processing
   k. Whether or not the controller intends to further process the data for a purpose other than the purpose for which the personal data was first collected[42]

When the information has not been obtained from the data subject directly, then the controller must provide all of the above information to the data subject as well as where the data originated and whether or not it was publically available.[43]

2. **Right to rectification** – The data subject has the right to have their information corrected if inaccurate, including having incomplete data completed.[44]
3. **Right to be forgotten (right to erasure)** – The data subject can request that their personal information be erased by the controller. Even when the data subject doesn't specifically request it, the controller also has the obligation to erase the data, without delay, when certain situations arise, such as the data being no longer necessary for the reason it was collected or processed, or if the data subject withdraws their consent.[45]
4. **Right to restrict processing** – The data subject can also restrict the processing of their data by the controller.[46]
5. **Right to data portability** – The data subject has the right to receive their personal data from the controller in a "structured, commonly used and machine-readable format" and can send their information to a new controller.[47]
6. **Right to object to profiling, automated decision-making and processing under legitimate interests grounds** – The data subject has the right to object at any time to the processing of their personal data when the processing is based on some legitimate interest of the controller or necessary for public trust, including profiling, and when it is processed for direct marketing purposes.[48] The controller cannot use an automated process to make a decision on a data subject when that decision produces some type of legal effect or similar consequence for the subject, except under specific circumstances.[49]

Security Obligations

The controller and the processor must implement the "appropriate technical and organizational measures to ensure a level of security appropriate to the risk…"[50] Such measures should include, where appropriate, data encryption, the

ability to restore availability and access to data in the event of an incident, and a process for regularly testing, assessing and evaluating the security measures.

When new technologies or high risk processing activities are used to process data, the controller must carry out a data protection impact assessment prior to the processing to determine the potential impact to the protection of the personal data. The assessment must contain specific information as outlined in the regulation. Large scale processing of special categories of data, systemic monitoring of a publicly accessible area and automated processing in particular require a data protection assessment.[51]

When a data protection impact assessment indicates that the processing will result in a high risk to the protection of the data, without efforts taken by the controller to mitigate that risk, the controller must consult the supervisory authority before using the process and then wait for a written decision with advice about using the process. Additionally, Member States may require consultation and the obtaining of prior authorization from the supervisory authority when the processing concerns public interest or is related to social protection and public health.[52]

Personal Data Breach Notification

In the event of a personal data breach, the controller "shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."[53] The processor must notify the controller without undue delay of a personal data breach.[54] The information can be provided in phases where necessary and the breach must be documented by the controller in order to allow the supervisory authority to verify compliance with the regulation.[55]

The notification to the supervisory authority must contain at least the following information:

1. A description of the nature of the personal data breach, including, where possible, the categories of data and approximate number of records and data subjects involved.
2. The name and contact information of the data protection officer.
3. A description of the likely consequences of the breach.
4. A description of the measures taken or that will be taken by the controller to address the breach, including actions to potentially mitigate the adverse effects.[56]

The controller must also notify the data subject without undue delay when the breach is likely to result in a high risk to their rights and freedoms.[57] If the controller has implemented security measures that render the personal data unintelligible, such as encryption, or if the security measures otherwise ensure that there is not a high risk to the rights and freedoms of the data subject, then the data subject does not have to be notified.[58]

The term "undue delay" is used frequently with regards to the notification of a personal data breach. Although vague, this term is not defined and the only guidance provided is the addition of "not later than 72 hours."[59] Indeed, it is very likely that 72 hours will become the actual deadline for notification, but application and formal interpretation of what constitutes "undue delay" may be fleshed out more by the supervisory authority once the GDPR is fully enforceable. The notification to the data subject must be in clear and plain language and contain at least the following information:

1. The nature of the personal data breach.
2. The name and contact information of the data protection officer.
3. A description of the likely consequences of the breach.
4. A description of the measures taken or that will be taken by the controller to address the breach, including actions to potentially mitigate the adverse effects.[60]

Data Protection Officer

The controller and the processor must have a data protection officer where the processing is:

- Carried out by a public authority.
- At its core, a type that requires systemic monitoring of data subjects on a large scale.
- Deals with a large scale of special categories and personal data related to criminal convictions.[61]

If any of the above three situations do not apply, then a controller and processor can designate a data protection officer, but it is not mandatory. Member States can make it mandatory. The data protection officer can be a staff member or can be an outside consultant.[62]

Where there is a data protection officer, that person must be involved in all issues related to the protection of personal data. The data protection officer must be allowed to operate without influence, cannot be punished for performing their tasks and must report to the highest level of management. Further, the data protection officer must be qualified and have "expert knowledge of data protection law and practices…"[63]

Where the controller or processor is not based in the EU, then they must designate in writing a representative in the EU.[64] The representative has to be established in one of the Member States where the EU data subjects whose data is being processed or whose behavior is being monitored is located.[65] The representative must have authority to be contacted by the supervisory authority and data subjects on all issues related to data processing.[66] The controller and processor are still legally responsible for all data processing issues.[67]

General Rules for Transfers to Third Countries

Any transfer of personal data to a third country outside of the EU or to an international organization shall take place only if the conditions of the GDPR are complied with. This includes onward transfers of that information from a third country or organization to another third country or organization.[68] This means that all transfers of covered data to a third country or international organization, regardless of who is making the transfer, must comply with the regulation.

As noted previously, transfers can be based on an adequacy decision such as Privacy Shield.[69] Where there is no adequacy decision, then a transfer can only happen where the controller and the processor have provided the appropriate safeguards. The safeguards can be provided for by contract between the controller and the processor and the third country or international organization, or with binding corporate rules.[70] There are a few exceptions that allow data transfers without these safeguards, such as when the specific consent of the data subject is obtained or if the transfer is necessary to defend or exercise a legal claim.[71]

Remedies, Liabilities and Sanctions

Every data subject has the right to lodge a complaint with a supervisory authority.[72] The data subject also has the right to bring a legal action against the controller or processor where they believe that their rights have been infringed upon in violation of the GDPR.[73] The data subject can also subrogate their rights to a legal action and a complaint to a nonprofit that handles such cases.[74] Data subjects are entitled to receive compensation from the controller or processor when they have "suffered material or non-material damage" as a result of a violation of the regulation.[75] The GDPR does not define what constitutes material or non-material damage.

A controller is liable for the violations committed by the processor. When the controller and the processor are both involved and responsible for a violation, then both "shall be held liable for the entire damage in order to ensure effective compensation of the data subject."[76]

Additionally, under the Privacy Shield, EU residents have several avenues of recourse against a company in the U.S., such as making a formal complaint with the FTC or the Department of Commerce or bringing a lawsuit in the U.S. against the company. Further, the FTC is also tasked with enforcing compliance and recently issued three separate law enforcement actions against U.S. organizations that made false claims about their participation with Privacy Shield.[77]

Administrative fines can also be imposed. If one or more provisions of the regulation are violated, then the fine shall not exceed the highest fine amount allowed. The following criteria will be used to determine the amount of the individual fine:

1. The nature, gravity and duration of the infringement, including the number of data subjects affected and the level of damage they suffered.
2. The intentional or negligent character of the infringement.
3. Any action taken to mitigate the damage.
4. The degree of the responsibility of the controller and processor taking into account the security measures they put in place.
5. A history of previous violations.

6. The degree of cooperation with the supervisory authority.
7. The categories of personal data affected.
8. How the supervisory authority found out about the violation, including whether the controller or processor notified the supervisory authority about it.
9. Whether there was a code of conduct and if it was followed.
10. Whether or not there were any prior reprimands.
11. Any other aggravating or mitigating factors, such as financial benefits or losses, etc.[78]

Violations can range from up to $10 million EUR or up to 2 percent of the total worldwide annual turnover, whichever is higher; or $20 million EUR or up to 4 percent of the total worldwide annual turnover, whichever is higher. There are specific categories of violations that are subject to each category. An example of a violation that can trigger the lower amount is failing to properly keep records of the data processing,[79] while failing to follow the rules on transfers to third party countries or international organizations can trigger the higher fine.[80]

Non-compliance with an order by the supervisory authority with regards to a reprimand or a warning about a violation of the regulation is also subject to fines up to $20 million EUR or up to 4 percent of the total worldwide annual turnover, whichever is higher.[81] Each Member State can lay down rules on other applicable penalties for violations that are not subject to administrative fines.

Conclusion

The GDPR gives regulators the power to enforce in the context of accountability – data protection by design, failure to conduct a data protection impact assessment, DPOs and documentation. If a business can't show that good data protection is a cornerstone of their practices, they're leaving themselves open to a fine or other enforcement action that could damage bank balance or business reputation.[82]

Full compliance with the GDPR is an enormous task that requires significant investment in time and resources, including a commitment to the continued cost of compliance. For U.S. companies that fall within the purview of the GDPR, compliance should be a top priority. With the proper preparation and support, compliance is achievable and will be in the organization's best interest overall. Ignoring the GDPR and not striving for compliance may be a huge and costly error for those organizations that are within its reach.

The GDPR provides for the enhancement of the rights of data subjects with regards to their personal data.

[1] Council of European Union. General Data Protection Regulation (GDPR). http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

[2] EU General Data Protection Regulation, "How did we get here?" eugpr. http://www.eugdpr.org/how-did-we-get-here-.html

[3] EU General Data Protection Regulation, "How did we get here?" eugpr. http://www.eugdpr.org/how-did-we-get-here-.html

[4] The OECD guidelines, (September 1980).

[5] EU General Data Protection Regulation, "How did we get here?" eugpr. http://www.eugdpr.org/how-did-we-get-here-.html,

[6] European Parliament and of the Council, (October 1995), http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[7] *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, Case C-230/14, Opinion of the Advocate General, ¶34, (June 2015). http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=req&docid=165232&occ=first&dir=&cid=820251, (accessed August 29, 2017).

[8] *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, Case C-230/14, Opinion of the Advocate General, Section V. conclusion, item (1), (June 2015), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=req&docid=165232&occ=first&dir=&cid=820251, (accesses August 29, 2017).

[9] Directive 95/46/EC of the European Parliament and of the Council, ¶20, October 24, 1995, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, (accessed August 30, 2017).

[10] *Schrems v. Data Protection Commissioner*, Case C-362/14, Opinion of the Advocate General, ¶ 2, (September 2015). http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=564712, (accessed August 29, 2017).

[11] *Schrems v. Data Protection Commissioner*, Case C-362/14, Opinion of the Advocate General, ¶ 25, (September 2015), http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=564712, (accessed August 29, 2017).

[12] *Schrems v. Data Protection Commissioner*, Case C-362/14, Opinion of the Advocate General, ¶ 25, (September 2015) http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=564712, (accessed August 29, 2017).

[13] *Schrems v. Data Protection Commissioner*, Judgment of the Court (Grand Chamber), October 2015, (2015/C 398/06), http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2015.398.01.0005.01.ENG, (accessed August 29, 2017).

[14] Weiss, Martin A. and Archick, Kristin, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, May 19, 2016: p. 9-10, https://fas.org/sgp/crs/misc/R44257.pdf, (accessed August 29, 2017).

[15] EU-U.S. Privacy Shield, EU Commission, "Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection", July 2016, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf,

[16] https://www.privacyshield.gov/Program-Overview, (assessed August 30, 2017).

[17] European Commission-Statement, "Joint Press Statement from US Secretary of Commerce Ross and Commissioner Jourová on the EU-U.S. Privacy Shield Review," September 21, 2017, http://europa.eu/rapid/press-release_STATEMENT-17-3342_en.htm, (assessed October 13, 2017).

[18] European Commission, "Daily News," September 21, 2017, "http://europa.eu/rapid/press-release_MEX-17-3405_en.htm, (assessed October 13, 2017).

[19] EU-U.S. Privacy Shield - Press Release, "First review shows it works but implementation can be improved," http://europa.eu/rapid/press-release_IP-17-3966_en.htm, (accessed December 19, 2017).

[20] Id.

[21] EU-U.S. Privacy Shield - First Annual Join Review, November 28, 2017, EU Article 29, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, last visited on 12/20/17.

[22] EU-U.S. Privacy Shield - First Annual Join Review, November 28, 2017, EU Article 29, p.4, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, last visited on 12/20/17.

[23] Id.

[24] GDPR, Article 45, 2018.

[25] EU commission, "Data Protection," http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm, (accessed August 31, 2017)
Brown, E. Jane, Small Companies and Those Not Certified Under the Safe Harbor Face Hidden Costs in the EU/US Privacy Shield Certification Process (blog). http://www.beyondiplaw.com/2016/10/12/small-companies-and-those-not-certified-under-the-safe-harbor-face-hidden-costs-in-the-euus-privacy-shield-certification-process/

[26] GDPR, Article 2 and 32, 2018.

[27] "Building a European Data Economy," Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, January 10, 2017, https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy, (accessed October, 15 2017).

[28] GDPR, Article 4(1), 2018.

[29] GDPR, Article 4(1), 2018.

[30] GDPR, Article 4(2), 2018.

[31] GDPR, Article 4(12), 2018.

[32] GDPR, Article 4(7), 2018.

[33] GDPR, Article 4(8), 2018.

[34] GDPR, Article 24, 28, and 30, 2018.

[35] GDPR, Article 45, 2018.

[36] GDPR, Article 6(4), (The GDPR does provide an analysis tool to use when the data is to be processed for another purpose besides the legitimate purpose it was originally collected for), 2018.

[37] GDPR, Article 5, 2018.

[38] GDPR, Article 8, (When the processing is based on consent, the controller has to be able to demonstrate that the data subject has actually consented. If the consent is in writing, it must be separate from any other writing, and be in clear and plain language. The data subject has the right to withdraw consent at any time, and it must be just as easy to withdraw consent as it was to give it). 2018.

[39] GDPR, Article 6, 2018.

[40] GDPR, Article 9, (The data can also be processed if it is necessary for carrying out the obligations or exercising rights of the controller in an employment or social context or if authorized by some other law; it is being processed to protect the data subjects rights; necessary for the establishment, exercise or defense of a legal claim; necessary for substantial public interest; necessary for medical purposes; or necessary for public interest and done in compliance with relevant laws; necessary for scientific purposes). 2018.

[41] GDPR, Article 10 and 11, 2018.

[42] GDPR, Article 13, 2018.

[43] GDPR, Article 14, 2018.

[44] GDPR, Article 16, 2018.

[45] GDPR, Article 17, 2018.

[46] GDPR, Article 18, 2018.

[47] GDPR, Article 20, 2018.

[48] GDPR, Article 21, 2018.

[49] GDPR, Article 22, 2018.

[50] GDPR, Article 32, 2018.

[51] GDPR, Article 35, (Additionally, the supervisory authority will establish a list of operations which require an assessment and the operations that do not). 2018.

[52] GDPR, Article 36, 2018.

[53] GDPR, Article 33, 2018.

[54] Id.

[55] Id.

[56] GDPR, Article 33, 2018.

[57] GDPR, Article 34, 2018.

[58] GDPR, Article 34, (The controller can also provide a public notification to the data subjects affected when individual notification would involve a disproportionate effort). 2018.

[59] GDPR, Article 33, 2018.

[60] Id.

[61] GDPR, Article 37, 2018.

[62] Id.

[63] Id.

[64] GDPR, Article 27, 2018.

[65] Id.

[66] Id.

[67] Id.

[68] GDPR, Article 44, 2018.

[69] GDPR, Article 45, 2018.

[70] GDPR, Article 46 and 47, 2018.

[71] GDPR, Article 49, 2018

[72] GDPR, Article 77, 2018

[73] GDPR, Article 79, 2018.

[74] GDPR, Article 80, 2018.

[75] GDPR, Article 82, 2018.

[76] GDPR, Article 82(4), (However, the controller and processor can bring contribution actions against each other to recover any amounts that they overpaid). 2018.

[77] Fair, Lesley. FTC cases affirm commitment to Privacy Shield (blog). https://www.ftc.gov/news-events/blogs/business-blog/2017/09/ftc-cases-affirm-commitment-privacy-shield.

[78] GDPR, Article 83, 2018.

[79] GDPR, Article 83(4), (also, failing to properly obtain a child's consent to processing; failing to have proper security controls in place; failing to properly notify a data breach to the supervisory authority and the data subject; failing to conduct a data protection impact assessment when necessary and failing to have a data protection officer when mandated). 2018.

[80] GDPR, Article 83(5), (also, failing to follow the basic principles of processing, including obtaining consent; violating the data subjects rights; failing to follow related member state law and failing to comply with an order limiting processing or the suspension of data flows). 2018.

[81] GDPR, Article 83(6), 2018.

[82] Denham, Elizabeth. GDPR and accountability (blog), https://ico.org.uk/about-the-ico/news-and-events/news- and-blogs/2017/01/gdpr-and-accountability/

About the Author

Annmarie Giblin is Senior Counsel in the Office of General Counsel for Chubb with a focus on Cyber Liability, where she is tasked with the rapidly changing regulatory, legal and insurance complexities concerning cyber liability across Chubb's global footprint. She is also a frequent speaker and author on this subject. She has conducted continuing education programs for the Financial Services industry, spoken on panel discussions with other cyber security experts and briefed senior staffers of sitting United States Senators on this topic. Before joining Chubb, Annmarie was a litigation attorney, spending more than 10 years in private practice. She received her Bachelor of Arts from the University at Albany, SUNY and her JD from St. Johns University School of Law.
Annmarie can be contacted at Annmarie.Giblin@chubb. com.

Chubb. Insured.℠

www.chubb.com/cyber

06/2018