GDPR, PART I: HISTORY OF EUROPEAN DATA PROTECTION LAW

Jay F. Kramer & Sean B. Hoar

In today's global marketplace, organizations must comply with an increasingly complicated set of international laws and regulations. This article is the first in a seven-part series which seeks to explain, in plain English, the critical compliance requirements of the European Union's forthcoming General Data Protection Regulation (GDPR). While this series will focus on a number of the most significant "need to know" features of the GDPR, future editions of this series will also compare how the GDPR will affect commerce among and between three of the world's most significant markets: the United States, the European Union, and China.

Part 1: A brief history of European data protection law and why it's important to understanding the GDPR

What is the GDPR and why is it important?

The forthcoming GDPR[1] is a new European regulation intended to strengthen and unify data protection for all individuals within the EU. It applies to all EU member states, and will become fully effective on May 25, 2018. This new regulation will replace the currently controlling European Data Protective Directive 95/46/EC and is significant because it *expands the territorial reach* of European data protection laws beyond "data controllers" and "data processors" to those entities who:

- offer goods or services *to* European residents; or
- monitor the behavior of European residents (if that behavior occurs in Europe).

This new regulation, therefore, will apply to many international corporations who either do business within the EU, or transact in the data of EU citizens.

How is a history of European data protection relevant to understanding the GDPR?

Understanding the history of European efforts to protect the data of its citizens can be helpful in two important ways. First, it can help practitioners understand how the GDPR's new standards change the compliance requirements of the existing European framework. Second, an understanding of the history of data protection efforts around the globe will serve as a broad foundation for understanding what will inevitably be evolving data privacy and data protection efforts in the U.S. and other countries.

An early but important effort: the 1980 OECD Guidelines

From the outset, it's helpful to recognize that the principles behind this new GDPR are *not new*. The principles embodied in the GDPR actually go all the way back to World War II, when leaders of a war-torn Europe realized that the best way to ensure ongoing peace and prosperity was to encourage broader

1 The official title of the regulation is "Regulation (Europe) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data," as published in the Official Journal of the EU.

international cooperation and reconstruction[2]. To aid in that effort, in 1945 the Organisation for Economic Co-operation and Development (OECD) was born.

In 1980, thirty five years after its founding, the OECD (which by that time included the U.S. and several other European countries) issued a set of international data privacy and protection guidelines known as the "*Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*." These guidelines established several important principles of data protection and privacy that we see reflected in today's GDPR, including the following:

- The purpose of data collection should be relevant to its use;
- Data should be protected against loss and unauthorized access;
- Individuals should have the right to know what data is collected about him or her;
- Individuals should have the right to access any data related to him or her; and
- An individual should be able to challenge the retention of data, or amend or erase data about him or her.

The OECD guidelines quickly became the global standard for fair information practices, but their power to influence data handling practices within OECD member states was limited because the OECD guidelines were just that – *guidelines*. In other words, despite their value in declaring important data protection principles, the OECD guidelines were still a *non-binding* and *voluntary* framework.

As European nations sought to develop implementing measures to comply with this framework, several individual and at times conflicting privacy laws were passed by OECD member states. This led to a great deal of confusion regarding how to comply with what became a patchwork of regional privacy requirements.

The EU's 1995 Data Protection Directive 95/46/EC

In 1995, the European Union attempted to solve some of the problems caused by the mosaic of European privacy laws resulting from the OECD framework. To do so, the European Commission (EC) promulgated a new "directive" which was now binding upon EU member states[3]. This directive, known as the *Data Protection Directive 95/46/EC*, required each EU member state to adopt privacy laws that are "equivalent" to one another. It also directed that data could only be exported to third party countries that could ensure "an adequate level of protection" for European citizens' data through their domestic laws or through international commitments that had been made.

Which countries were deemed to have "adequate" protections for privacy under the Directive?

In furtherance of the directive, the EC recognized a limited number of third party countries deemed to have an "adequate" legal framework for the protection of EU citizens' data[4]. Those countries included Andorra, Argentina,

2 *See http://www.oecd.org/about/history/*

3 According to Article 288 of the Treaty on the Functioning of the European Union, a directive is binding upon each member state, but leaves to the national authorities of each state the choice of "forms or methods" to achieve the intended result. By contrast, a "regulation" within the EU is binding *in its entirety*, is directly applicable to all member states, and *does not* require any implementing measures – it is self-executing.

4 http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay. These countries could therefore transfer the data of EU citizens without any additional approval. Significantly, the EC did not find the protections afforded by U.S. law to be "adequate."

The U.S. response and evolving efforts to comply with the directive

The "Safe Harbor" framework

On July 26, 2000, the EC approved a "Safe Harbor" framework developed by the U.S. Department of Commerce. This framework established a set of fair data information practices to which participating organizations agreed to abide. To comply with the requirements of the directive, organizations participating in the framework also agreed to enhanced enforcement and oversight by two U.S. regulatory agencies: the Federal Trade Commission (FTC)[5] and the Department of Transportation (DOT).

The Schrems decision and the invalidation of the Safe Harbor framework

In 2013, Austrian lawyer Max Schrems filed a complaint against Facebook to prohibit Facebook's transfer of personal data from Ireland to the U.S. The suit was brought in the wake of several disclosures made by Edward Snowden, including the specific allegation that Facebook USA participated in the National Security Agency's PRISM surveillance program.[6] Schrems based his complaint on the directive's mandate that data not be transferred to non-EU countries, unless the company transferring the data can guarantee "adequate protection." On September 23, 2015, the EC ruled in Schrems' favor, declaring the Safe Harbor agreement invalid, and holding that individual data protection authorities were permitted to suspend data transfers to third countries if those countries violated EU rights.

On October 6, 2015, the Court of Justice of the EU further ruled that the Safe Harbor framework was invalid for several reasons: it allowed for government interference of the directive's protections, it did not provide legal remedies for individuals who seek to access data related to them or to have their data erased or amended, and it prevented national supervisory authorities from appropriately exercising their powers.

Back to the drawing board: the EU-U.S. Privacy Shield Framework

On July 12, 2016, U.S. Secretary of Commerce Penny Pritzker and EU Commissioner Věra Jourová announced the approval of the *EU-U.S. Privacy Shield Framework* as a valid legal mechanism to comply with EU requirements when transferring personal data from the EU to the U.S. The Privacy Shield replaced the U.S.-EU Safe Harbor Framework, and the Department of Commerce began accepting Privacy Shield compliance certifications on August 1, 2016[7].

---

5 The FTC established jurisdiction to oversee compliance with the Safe Harbor framework through a determination that non-compliance constituted an "unfair and deceptive trade practice."

6 According to the NSA, the U.S. Intelligence Community relied on Section 702 of the Foreign Intelligence Surveillance Act to compel providers to facilitate surveillance on specific foreign targets located outside the U.S. for the purpose of acquiring critical intelligence on issues ranging from international terrorism to cybersecurity. For more information, see https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.html

7 As of October 31, 2016, the department stopped accepting all U.S.-EU Safe Harbor certifications.

Under the Privacy Shield framework, U.S. companies are required to certify compliance with seven primary data security principles, including the responsibility to:

1. Respond to complaints within 45 days;
2. Provide a response with assessment of the merits and potential solutions;
3. Designate an independent dispute resolution body in the EU or the U.S.;
4. Respond promptly to requests for information from Department of Commerce;
5. Provide information to the FTC when requested;
6. Cooperate with Data Protection Authorities (DPAs); and
7. Submit to regular compliance reviews.

Participating organizations must also agree to enhanced monitoring and enforcement requirements through national or local DPAs, and an expanded role for U.S. regulatory authorities, including the U.S. Department of Commerce, the FTC, and the DOT.

A shift from self-certification under the Privacy Shield to the new GDPR

On January 25, 2012, the EC announced it would attempt to unify data protection law across a unified EU via proposed legislation called the "General Data Protection Regulation." The EC's objectives for this new legislation included:

- the harmonization of 27 national data protection regulations into one unified regulation;
- the improvement of corporate data transfer rules outside the EU; and
- the improvement of user control over personal identifying data.

On April 27, 2016, after four years of negotiation, final legislative approval was obtained for the GDPR,[8] and after a two year transition period, the regulation will become fully enforceable on May 25, 2018. The GDPR will supersede the former data protection directive known as Directive 95/46/EC.

To what will the GDPR apply?

The GDPR addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by *unifying* regulations within the EU. The GDPR codifies into law many additional requirements for the handling and protection of data including stricter conditions for consent, a broader definition of sensitive data, new provisions on protecting children's privacy, mandatory breach reporting obligations, and the inclusion of the "right to be forgotten."

8 See http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/

Additional protections: the EU-U.S. Umbrella Agreement and U.S. Judicial Redress Act

The EU-U.S. Data Protection and Privacy Agreement or the "Umbrella Agreement"

Despite the enhanced requirements imposed by the EU-U.S. Privacy Shield Framework, lingering concerns about U.S. government surveillance programs led the European Commission to negotiate and adopt an additional data protection agreement known as the EU-U.S. *Data Protection and Privacy Agreement,* otherwise known as the *"Umbrella Agreement"*[9]. This agreement entered into force on February 1, 2017, and layered on an additional data protection framework for personal data transferred for the purpose of prevention, detection, investigation, and prosecution of criminal offenses, including terrorism.

The U.S. Judicial Redress Act

To finalize implementation of the Umbrella Agreement, EU negotiators insisted that EU citizens be extended the privacy rights and remedies available to U.S. persons within the U.S. Accordingly, in anticipation of the full implementation of the Umbrella Agreement, on February 24, 2016, the U.S. Congress passed the U.S. Judicial Redress Act (JRA), to extend the benefits of the U.S. Privacy Act to Europeans.

Significantly, the JRA extends some, but not all of the protections in the Privacy Act to records shared by EU and other designated countries with U.S. law enforcement agencies, including records shared under the Umbrella Agreement. The JRA also affords persons who are the subject of those records – including citizens of EU member states – access to certain civil remedies and other U.S. court proceedings for violations of those protections.

Despite the adoption of the Umbrella Agreement and the passage of the JRA, there are still a number of exceptions, definitional limitations, loopholes, and other hurdles a citizen of an EU country must clear before he/she can actually seek redress under the law.

Conclusion

In the 241 year history of the U.S., Americans have cultivated a national identity based on the ideas of individualism and a free market economy with limited government interference. This is reflected in the U.S.' "sectoral" approach to data privacy and data protection. U.S. law and policy has addressed certain data privacy and data protection concerns, but only in very specific ways to address the specific needs of individual sectors of the U.S. economy.

For example, to protect the health care sector in the U.S. the *Health Insurance Portability and Accountability Act of 1996* was enacted to provide data privacy and security to medical information.[10] In 1999, the *Gramm-Leach-Bliley Act* was passed to protect data within the financial sector by requiring financial institutions to explain information-sharing practices to their customers and to safeguard sensitive data.[11] In addition, 48 separate state data breach notification statutes have been passed to reflect the legislative judgment of 48 individual states regarding manner and means by which data breach notifications should be made.[12]

---

9 See http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf

10 See Pub.L. 104–191, 110 Stat. 1936

11 See Pub.L. 106–102, 113 Stat. 1338

12 See http://lewisbrisbois.com/privacy/US.

These examples illustrate that there is no overarching federal data privacy or data protection framework currently in existence within the U.S. When contrasted with the evolving series of European frameworks, directives, and regulations described above, the significance of the newly enacted GDPR becomes evident. To some, the requirements of the GDPR may be seen as onerous or unnecessary, but when compared with the prior patchwork of European law and policy in this area, at the very least, the GDPR will facilitate a more uniform international effort regarding data protection and compliance. So although it is too early to decide whether the GDPR's reporting, compliance, and enforcement provisions will function as intended, it is likely that other global regulations will soon follow the GDPR.

The world is becoming "connected" at an alarming rate,[13] and for global policy makers to keep up with this connected world, international data privacy and protection regimes must be aligned to insure the various personal, governmental, and financial interests of citizens are honored and respected within connected nations across the globe. The GDPR may be the first of many international efforts in this arena.

13 According to a recent analysis by Gartner, Inc., 8.4 billion devices will be connected to the Internet by the end of 2017, and that number will grow to 20.4 billion by 2020.