by Daniel A. Cotter

Privacy in the European Union: A data safekeeping revolution

» The European Union was at the forefront of privacy regulations in the 1990s and is taking a lead role currently.
» The Safe Harbor protections will be revisited and new guidance will evolve.
» Companies should review their existing privacy practices and notices for potential updates.
» Changes implemented by the EU General Data Protection (GDP) Regulation likely will spread to other countries, including the U.S.
» Companies must review relevant contracts to make sure any privacy language is included in notices.

In 1995, the European Union (the EU) brought to the forefront the issues of privacy and the individual's right to protection of their sensitive information, when it adopted "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (the EU Data Protection Directive). A version of the EU Data Protection Directive was implemented in each EU country. The EU's history of strong commitment to privacy and human rights law is reflected in the EU Data Protection Directive, which was the first major privacy law of its kind. The U.S. Congress subsequently enacted the Health Insurance and Portability and Accountability Act of 1996 and, in 1999, Congress passed the Gramm-Leach-Bliley Act, which governs privacy obligations for financial institutions.


Cotter

On January 25, 2012, the EU introduced a new privacy regulation, known as the General Data Protection Regulation (the EU GDP Regulation), that will supersede the EU Data Protection Directive in March 2018.[1] However, companies should review the new EU GDP Regulation and start to consider how their privacy programs might need to change, even if they are US-only companies. As was the case in 1995, the EU may be on the forefront of more restrictive privacy regulations than the U.S.

A version of the EU Data Protection Directive was implemented in each EU country.

The U.S. Safe Harbor

On July 26, 2000, the EU issued European Commission's Decision 2000/520/EC "on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the U.S. Department of Commerce" (the U.S. Safe Harbor). The Safe Harbor Privacy Principles

(the Principles) were developed between 1998 and 2000, and were designed to put in place systems to prevent accidental disclosure of private information from companies in the EU or U.S. The Principles included seven requirements:

1. **Notice** – Individuals must be provided information about their data and how it is being collected and used.
2. **Choice** – Individuals must have the ability to opt out of the collection and transfer of data to third parties.
3. **Onward transfer** – Transferring data to third parties may only occur if the third party to whom the data will be transferred also adheres to the Principles.
4. **Security** – Reasonable efforts must be made by the recipient of private information to protect it against loss.
5. **Data integrity** – Data must have integrity (i.e., be relevant and reliable for the purpose for which it was collected).
6. **Access** – Individuals must have the ability to access information about themselves and correct or delete it.
7. **Enforcement** – There must be effective means of enforcing the Principles.

US companies that complied with the Principles and appropriately answered a series of questions could self-certify compliance and thereby be eligible for the U.S. Safe Harbor and safely transfer EU data to the U.S.

Invalidation of the Safe Harbor

On October 6, 2015, the Court of Justice of the EU declared the U.S. Safe Harbor framework invalid, citing the "massive and indiscriminate surveillance" conducted by the U.S.[2] The Court of Justice's decision left many US companies with little guidance or protection for their EU data practices. On February 29, 2016, the European Commission published a series of documents detailing the new Privacy Shield framework. The draft was published and is currently "under review," meaning the Privacy Shield will not become effective until this review is completed. The Privacy Shield framework requirements are detailed in the EU-U.S. Privacy Shield Principles (the Privacy Shield Principles).[3] Although the Privacy Shield Principles follow the same seven requirements found in the old Safe Harbor Principles, there are significant differences between the U.S. Safe Harbor framework and the new Privacy Shield framework.

Although the specific differences are beyond the scope of this article, the new Privacy Shield framework provides for significantly enhanced notice obligations. US companies wishing to avail themselves of the Privacy Shield will have to inform individuals about 13 aspects of the company's privacy practices, including:

1. Participation in the Privacy Shield, with a link to the listing of all US companies that have self-certified compliance with the Privacy Shield Principles (i.e., the Privacy Shield List).
2. What types of data the company collects and which subsidiaries or affiliates of the company also adhere to the Privacy Shield Principles.
3. Commitment to strictly adhere to the Privacy Shield Principles for all EU data collected.
4. The purposes for which the company collects and uses the data.
5. The independent dispute resolution body to which complaints and disputes will be submitted for resolution.

The Privacy Shield Principles are substantially more detailed and onerous than the notice requirements provided for in the Safe Harbor Principles.

Significant changes were also made to consumers' choices. Individuals are given the

ability to prevent their personal information from being disclosed to third parties. For sensitive information (defined as "personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual"), the individual must affirmatively permit either the disclosure of sensitive information to a third party, or the use of this information for purposes substantially different from the original collection purpose. The broad definition of sensitive information, as well as the obligations on a US company participating in the Privacy Shield, make compliance with these obligations more burdensome than compliance with the Safe Harbor Principles. EU individuals also have enhanced redress options at their disposal.

If the Privacy Shield becomes effective, US companies will have additional compliance obligations to be able to avail themselves of the Privacy Shield safe harbor protections.

The EU GDP Regulation

The EU GDP Regulation is a second privacy initiative by the EU that is designed to address the changes that have taken place in data security and information flow over the last 20 years. The EU GDP Regulation will replace the EU Data Protection Directive in its entirety. One advantage of the EU GDP Regulation is that one single law will apply to all 28 EU countries. Currently, each country within the EU had to approve the EU Data Protection Directive and so, like the states' enactment of model laws in the U.S., each EU country had the ability to have slight differences from the EU Data Protection Directive.

The EU GDP Regulation implements some significant changes from the current EU Data Protection Directive, including:

- There will be a one-stop shop, with a lead regulator appointed to enforce the EU GDP Regulation.
- The EU GDP Regulation framework has significantly higher fines and penalties for non-compliance.
- Organizations must have a data protection officer (the DPO), who will be monitored by the regulator overseeing the organization. This is a significant change in reporting order.
- Controllers and processors of data have a higher accountability level.
- Explicit consent must be obtained from the consumer to use and transfer data.
- A right to erasure of data exists for the subject of the private information.

Preparing for the EU GDP Regulation

As noted, the EU GDP Regulation will likely lead to changes in other privacy rules and regimes, including in the U.S. (a number of countries in the last 12 to 18 months have established privacy rules and regulations, some of which impose stringent compliance standards). Over the next 12 to 18 months, the EU will start to issue implementing regulations. Companies should do a number of things to prepare for the enhanced privacy rules and the resultant privacy obligation enhancements that will be enforceable in the near future, including the following.

Review current privacy policies and practices

- What data are you collecting? Does any of it involve EU citizens? Other countries?
- Are you providing goods or services to EU citizens?
- Are you monitoring behaviors of EU citizens?
- What is your practice on consent for use of data? Are you obtaining explicit consent?

- Note that in the U.S., recent changes implemented by the Telephone Consumer Protection Act (the TCPA), require opt-in explicit consent for use of data.

Review your compliance program

- Do you have one in place?
- The EU GDP Regulation requires that you have a program in place to show compliance.

Consider how the DPO position will fit within your organization

- What skill sets and experience will the person in this position need?
- Who will the DPO report to internally?

Review your policy notices

- The terms of any relevant contract your organization has with a third party addressing potential use of consumer information must be explicitly set forth in your privacy notice.
- Any cross-border data transfers must be disclosed in the notice.
- The legitimate interests for use of data and sharing must be explicitly set forth in the notice.
- Data retention periods must be set forth in the notice.
- Consider whether the uses of information and protections described in your current privacy notices match how you are using the information. Some regulators within the United States are beginning to enforce violations of organizations' privacy notices.

Review your contract provisions

- Companies with multiple contractual provisions on confidentiality and privacy will need to consider streamlining the contract language to avoid having a privacy notice that is overly cumbersome.

Review your data breach notification procedures

- Companies must report any breaches to the supervising authority within 72 hours of being discovered.
- If not reported within 72 hours, the organization must provide a reasoned justification for the failure to make a report to the supervising authority.

Conclusion

As the EU GDP Regulation moves towards full implementation, we expect that privacy rules and practices in the United States and around the world will undergo significant review and changes. Whether a US-domiciled company is doing business in the EU or not, some of the concerns addressed by the EU GDP Regulation will likely be incorporated into United States privacy rules and regulations. Around the world, China, Russia, Canada, and Latin American countries are implementing strict data localization rules that require data to be kept in the country promulgating the rules. Companies would do well to refresh their review of privacy practices, procedures, and notices, regardless of where they are collecting data. Changes in practices implemented by the TCPA, as well as other privacy laws and regulations, make a fresh review of privacy policies and procedures a best practice for companies of any kind. ✳

The article contains the author's opinions and is not to be attributed to Butler Rubin or any of its clients or The Chicago Bar Association.

1. European Council of the European Union, press release: "Data Protection: Council agrees on a general approach" June 15, 2015. Available at http://bit.ly/general-approach
2. Grant D. Petersen, Simon J. McMenemy, and Hendrik Muschal: "European Court of Justice invalidates European Commission's Safe Harbor Decision" *Lexology*, October 16, 2015. Available at http://bit.ly/euro-court
3. U.S. Department of Commerce, letter to Commissioner Jourova. February 23, 2016. Available at http://bit.ly/Jourova

Daniel A. Cotter *(dcotter@butlerrubin.com) is Partner at Butler Rubin Saltarelli & Boyd LLP in Chicago and Immediate Past President of The Chicago Bar Association.*