FOLEY

FOLEY & LARDNER LLP

Privacy Shield – Rejected. GDPR – Accepted: What This Means to Your Organization and What You Should Consider Doing Now

By Michael K. Chung, Chanley T. Howell, Steven M. Millendorf, and Aaron K. Tantleff
15 April 2016

Legal News: Privacy, Security & Information Management

The European Union Article 29 Working Party (Article 29) issued an opinion on the proposed EU-U.S. Privacy Shield framework agreement (Privacy Shield) earlier this week, stating that although the Privacy Shield was a "great step forward," the Article 29 group identified several areas in which it found the Privacy Shield to be unacceptable, including that it permits the U.S. to carry out "massive and indiscriminate" bulk surveillance of European Union citizens. On the other hand, just a day later on April 14, 2016, European Parliament provided final approval for the new EU General Data Protection Regulation (GDPR), after four years of work between the member states.

While many U.S. organizations will be disappointed to learn of the Article 29 group's rejection of the Privacy Shield, as it does not provide "adequate protection" to EU residents, it should not come as a surprise. The Article 29 group continued to raise concerns over the possibility of "massive and indiscriminate" bulk collection by U.S. authorities of EU personal data. However, the Article 29 group raised other concerns as well, tipping their hat to the concern that, unless these issues are addressed, a similar challenge could be brought against the Privacy Shield as was brought against Safe Harbor in the European Court of Justice, thus invalidating the Privacy Shield.

What You Should Start Doing Today to Prepare for GDPR and Privacy Shield

GDPR will apply to almost all organizations who monitor or process the personal data of European citizens, without any regard to the physical location of the processor or controller. Although the penalties for non-compliance with GDPR will not be enforced until mid-2018, organizations that collect or process the personal data of EU citizens may have a lot of work to do to be ready. Likewise, although the Privacy Shield has encountered some roadblocks to its adoption, it seems likely that it will be adopted in some form and companies considering the Privacy Shield have some preparation to do before they can adopt it. We recommend that companies consider the following to prepare for GDPR and Privacy Shield:

- Perform a data inventory to understand what personal data your organization collects, how it is processed, where it is stored, how it is protected, and who may have access to it. Put processes in place to conduct Privacy Impact Assessments if your organization may be engaging in high-risk processing (it is likely that you will need to perform such an assessment if your organization handles any of the particular special categories of personal data).
- Begin drafting or revising your written information security policies to ensure the appropriate technical, administrative, and physical measures to protect personal data and employ proper

training for all your employees. Ensure that procedures are in place to continually monitor compliance with these policies prior to, during, and after processing of personal data. Begin performing a gap assessment and consider participation in certification programs.
- Maintain detailed records of the processing performed on personal data.
- Review your product development process to ensure that privacy risks are considered early in the process and that your products and services only collect and maintain the minimum amount of personal data necessary for the proper performance of the products and services.
- Review and update privacy policies to ensure they are easily accessible, written in clear and plain language, and include full disclosure of your data collection and processing. Privacy Shield also requires that you implement, and your privacy policy describes, methods for individuals to have their complaints addressed.
- Review and revise your methods of obtaining consent from data subjects to ensure that specific, informed, unambiguous opt-in consent is provided before processing data.
- Review your ability to comply with the data subject's right to be forgotten and new data portability rights. You must be able to erase personal data and transfer the data to another provider when technically feasible.
- Review your cyber-incident response plans and update if necessary to be able to implement notification to Supervisory Authorities within 72 hours of a breach.
- If you are using BCRs or SCCs for trans-Atlantic data flows, you should review them for compliance with the new requirements of GDPR. Draft addendums to SCCs and other contracts as necessary to address the onward transfer restrictions of the Privacy Shield. This includes ensuring that downstream entities comply with limitations on purpose and meet all of the Privacy Shield requirements, including remediating any unauthorized processing by the downstream entity.
- Begin to search for qualified Data Protection Officers (DPO). Under GDPR, organizations that regularly or systematically gather personal data as part of its core activities, or that process large amounts of sensitive personal data, will need to appoint a DPO who has the authority and independence to inform the organization of their obligations under GDPR, monitor compliance, train the organization's internal staff, and conduct internal audits. The DPO will also act as the organization's point of contact for data subjects' inquiries, withdrawals of consent, right to be forgotten requests, and other related rights.
- Review insurance policies for scope and limits of coverage. Consider if your policy includes global or enterprise coverage, what types of data issues are covered, and the potential for increased costs and liabilities under GPDR and the Privacy Shield.

Companies should be aware that GDPR shifts the issue of privacy and personal data protection even further from an information technology issue to a Board of Directors and C-suite issue. GDPR will have a tremendous impact on the day-to-day operations, costs, and potential liabilities of the company that demands board level attention. Furthermore, under Sarbanes-Oxley in the United States, public companies may need to disclose GDPR's increased operational costs and potential for high liabilities to their investors.

Impact to Your Business

The rejection by the Article 29 group puts the U.S. Department of Commerce and the EU Commission, who jointly proposed the Privacy Shield after almost two years of negotiations, in a difficult situation. The decision leaves U.S. organizations with significant uncertainty on how to continue to provide services to EU residents and puts these organizations at risk to further enforcement actions by European Data Protection Authorities. However, the Privacy Shield was not necessarily an easy solution for many organizations, including those thinking of registering for the Privacy Shield, if and when it is adopted. In addition, Privacy Shield may be invalidated by the European Court of Justice for similar reasons that Safe Harbor was invalidated. While the Privacy Shield, if and when adopted, would be one of the permissible methods to transfer personal data

between the U.S. and the EU, the decision to join is one that every U.S. organization should not take lightly, as it is just one of several mechanisms to provide for trans-Atlantic data transfers, such as the EU Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). Although both are more complex as compared to the Privacy Shield, their relative certainty may be the best option for trans-Atlantic data flow at this time. However, the adequacy of each of these methods is also expected to be reviewed by the Article 29 group following the approval of the Privacy Shield by the European Commission. Furthermore, companies will almost certainly need to repeat some efforts to put these methods in place to comply with the upcoming GDPR.

Although GDPR is intended to harmonize data protection in all 28 member states of the EU, there are certain provisions of the new regulation left to local laws (for example, in the area of processing health information and the age of consent), which will lead to continued complexity for compliance by all organizations. Although it will not be required to be fully compliant with GDPR for two years, organizations need to become familiar with the provisions of GDPR and begin planning for implementation now, because once GDPR is enforced, violations for non-compliance with could result in penalties up to four percent of the organizations worldwide revenue or 20 million Euros, whichever is greater.

Details of the Article 29 Working Party Decision

In the highly-anticipated press conference on April 13, 2016, Chairwoman Falque-Pierrotin indicated that while Privacy Shield was a “major improvement” compared to the now invalidated Safe Harbor framework, the Article 29 group believes there is still work to do and urged the EU Commission to resolve the concerns. The announcement described a number of issues with the Privacy Shield proposal:

- The documents and annexes provided by the U.S. government were “rather complex” and not always consistent, making it difficult for the Article 29 group to understand the proposal as a whole. Chairwoman Falque-Pierrotin indicated that it would have been better if it was simpler and less complex to understand.
- The purpose limitation was not clear and may have permitted reuse of personal information for a large amount of purposes and transfers.
- There is no express discussion of what the permissible scope of data retention is and therefore it remains unclear what an organization’s obligations data retention and destruction obligations are.
- Too many avenues for individual recourse that are too difficult for end users to navigate.
- Because the Privacy Shield is built on the old Data Protection Directive, there needs to be some capability of adjusting the framework for the new GDPR.
- The six exceptions for bulk surveillance (including an undefined “counter terrorism” purpose) provide too much of a possibility for massive, indiscriminate surveillance.
- The independence and authority for enforcement of the new Ombudsman is questionable.

Chairwoman Falque-Pierrotin indicated that surveillance and the ombudsman were the most significant concerns for the Article 29 group. With regard to surveillance, she described that the “massive and indiscriminate” bulk data collection by the U.S. government had not been addressed, and there was still an unacceptable possibility for such collection that the Privacy Shield did not fully address.

In describing the new role of an Ombudsman, Chairwoman Falque-Pierrotin expressed the concerns that, while the creation of this new role is a major step forward, there are still concerns that the Ombudsman may not be a truly independent authority with the effective powers to enforce the Privacy Shield. The Ombudsman, as currently proposed, would be appointed by, and would report to, the U.S. Secretary of State.

Next steps for Privacy Shield

While this decision calls the future of the Privacy Shield into question, it does not necessarily mean its end. The Article 29 group's decision is advisory in nature, and the European Commission will still wait to hear from the Article 31 Committee before rendering its final decision. The Article 31 Committee is comprised of representatives from each of the EU member states and is widely expected to decide in favor of the Privacy Shield. Such a decision is likely to follow meetings scheduled on April 29 and May 19, where the Committee will discuss the details of the Privacy Shield arrangement.

Following the recommendation of the Article 31 Committee, the EU Commission and U.S. Department of Commerce may resume talks to further work on the Privacy Shield and address the Article 29 group's concerns. On the other hand, both the Article 29 group's and the Article 31 Committee's recommendations are purely advisory, and the EU Commission may still approve the Privacy Shield as is or with modifications, if any. It is unclear whether the Commission would implement the Privacy Shield despite a rejection by the Article 29 group. However, there is a lot of speculation that it may be the case, given the significant pressure from the U.S. government, and organizations on both sides of the Atlantic. During a debate on the finalization of GDPR, EU Justice Commissioner Vera Jourova, who has been deeply involved in the negotiation of the Privacy Shield, indicated that the commission will "study the opinion and address concerns in the final decision." However, a decision to adopt the Privacy Shield without addressing the most important concerns of the Article 29 group is almost certain to meet legal challenges in front of the the Court of Justice of the European Union (CJEU), the same court that invalidated Safe Harbor over similar fears about mass surveillance in the U.S. by the NSA. Chairwoman Falque-Pierrotin confirmed that such a recourse to the CJEU "is always an option." This potential, which would lead to even greater uncertainty for both European and U.S. organizations, may put significant pressure on both the European Commission and the U.S. Department of Commerce to address the issues in writing prior to the European Commission final decision.

Next steps for GDPR

The GDPR will first be published in the EU Official Journal (expected sometime in June), and will be officially considered enforceable 20 days following the publication. There will be a two year implementation period following the in force date, which will require that organizations be fully compliant sometime in mid-2018.

FOR MORE INFORMATION ON THIS TOPIC, REGISTER TO ATTEND THE FOLOWING WEB CONFERENCE ON WEDNESDAY, APRIL 27, 2016, FROM 12:30 P.M. - 1:30 P.M. GREENWICH MEAN TIME (7:30 A.M. - 8:30 A.M. U.S. CENTRAL TIME)

Unveiling the Impact of the EU-U.S. Privacy Shield and GDPR

Leading to the biggest data protection shake up in the last 30 years, the European Parliament has approved the new General Data Protection Regulation (GDPR) which would be enforceable in 2018 and creates significant new obligations, establishes new enforcement mechanisms and new data protection rights for EU residents. In addition, the European Commission and the U.S. Department of Commerce issued a draft of the new EU-U.S. Privacy Shield (Privacy Shield) set to replace the invalidated Safe Harbor framework. While Privacy Shield has been rejected by the Article 29 Working Party, it is possible that some form of Privacy Shield will soon be adopted. Privacy Shield and GDPR will likely influence data protection for the next 30 years.

Click here to register.

Legal News Alert is part of our ongoing commitment to providing up-to-the-minute information about pressing concerns or industry issues affecting our clients and our colleagues. If you have any questions about this update or would like to discuss this topic further, please contact your Foley attorney or the following:

Aaron Tantleff
Chicago, Illinois
312.832.4367
atantleff@foley.com

Chanley Howell
Jacksonville, FL
904.359.8745
chowell@foley.com

Steve Millendorf
San Diego, CA
858.847.6737
smillendorf@foley.com

Michael Chung
Los Angeles , CA
213.972.4601
mchung@foley.com