Privacy Shield Agreement

WHAT WILL U.S. COMPANIES HAVE TO DO TO COMPLY WITH THE EU PRIVACY SHIELD AGREEMENT?

On February 2, 2016, the EU Commission and U.S. Department of Commerce reached an agreement on a program called the EU-U.S. Privacy Shield ("Privacy Shield") that establishes a new framework for the transfer of personal data for commercial purposes from the EU to the U.S. The Privacy Shield replaces the Safe Harbor Program ("Safe Harbor"), which the European Court of Justice ("CJEU") struck down last October in the Schrems case over concerns that U.S. companies were not adequately protecting the personal information of EU citizens.

The Privacy Shield imposes stronger obligations on U.S. companies to protect the personal information of EU citizens and stronger monitoring and enforcement mechanisms by the U.S. Department of Commerce and Federal Trade Commission ("FTC"). It also requires greater transparency on how U.S. companies use personal data and offers multiple avenues to address concerns EU citizens may have regarding U.S. companies' compliance with the Privacy Shield.

The Privacy Shield has yet to go through several stages of review, including review by the EU Data Protection Regulators, Member States and the College of EU Commission. The process will take several months. In the meantime, companies that are thinking about participating in the Privacy Shield should review its text to familiarize themselves with the new compliance requirements and better understand how this new framework will impact their business. Some of these obligations and other important aspects of the Privacy Shield are discussed below.

Corporate Commitment

Joining the Privacy Shield is completely voluntary. U.S. companies must decide if they want to participate in the Privacy Shield framework or use other methods of transatlantic data transfers, such as the EU Model Clauses or Binding Corporate Rules. Under the Privacy Shield, U.S. companies must annually register on the Privacy Shield List and self-certify their compliance with certain EU data protection principles and subject themselves to oversight by the U.S. Department of Commerce and the FTC. U.S. companies must also publicly commit to comply with the Privacy Shield's requirements. Only then may EU companies share personal information of EU citizens with U.S. companies without violating the EU restrictions on transfers of personal data outside the EU.

E. Martín Enriquez
Partner
303.628.9585 direct
menriquez@lrrc.com

Richard K. Clark
Partner
303.628.9531 direct
rclark@lrrc.com

Disclosure

Please note that the information provided in this article does not constitute legal advice and is not intended to be and should not be construed as legal advice. Readers with questions specific to the issues raised in this article should consult with qualified legal counsel.

Lewis Roca Rothgerber Christie LLP will continue to monitor developments and progress on the Privacy Shield and we will provide updated information as it becomes available. In the meantime, if you have any questions about the Privacy Shield, please feel free to reach out to E. Martín Enriquez or Dick Clark.

www.lrrc.com

Importantly, once a U.S. company publicly commits to comply with the Privacy Shield, the company's commitment will become enforceable under U.S. law. U.S. companies that wish to self-certify under the Privacy Shield will need to audit their current privacy practices to determine if their practices meet the new stringent Privacy Shield requirements. As discussed below, changes may include updating privacy policies, security measures, and data handling protocols (particularly government access). Failure to comply with the Privacy Shield requirements could result in sanctions or exclusion from the framework.

Stronger Compliance Obligations for U.S. Companies

Under the Safe Harbor, U.S. companies had to comply with certain Privacy Principles when transferring and processing personal data from the EU to the U.S. in support of transatlantic commerce. These Privacy Principles include: Notice; Choice; Security; Data Integrity and Purpose Limitations; Access; Accountability for Onward Transfers; Recourse, Enforcement, and Liability. The Privacy Shield relies on the same Privacy Principles but imposes stringent compliance requirements than those imposed under the Safe Harbor. These requirements are discussed below.

U.S. companies must include in their privacy policy a declaration of the company's commitment to comply with the Privacy Principles. If the privacy policy is available online, it must include a link to the Department of Commerce's Privacy Shield website.

U.S. companies must inform individuals of their right to access their personal data, the requirement to disclose personal information in response to lawful request by the government, which enforcement authority has jurisdiction over the organization's compliance with the Privacy Shield, and the organization's liability in cases of onward transfer of data to third parties.

U.S. companies must limit personal information to the information relevant for the purposes of processing.

In order to transfer personal information to a third party acting as a controller, the U.S. company must (1) comply with the Notice and Choice Privacy Principles; and (2) enter into a contract with a third party controller that (i) provides that such data may be only process for limited and specified purposes consistent with the consent given by the individual, and (ii) the controller will provide the same level of protection as the Privacy Principles.

In order to transfer personal information to a third party acting as an agent, the U.S. company must (1) transfer such data only for limited and specified purposes; (2) ascertain that the agent is obligated to provide the same level of privacy protection as the Privacy Principles; (3) take reasonable steps to ensure the agent processes the personal information in a manner consistent with obligations imposed by the Privacy Principles; (4) upon notice, take reasonable steps to stop and remediate unauthorized processing; and (5) provide, upon request by the Department of Commerce, a summary or representative copy of the relevant privacy provisions of its contract.

U.S. companies participating in the Privacy Shield framework that handle HR data from EU citizens must also commit to cooperate with the relevant Data Protection Authorities ("DPA") in the investigation and resolution of any complaints, including agreeing to comply with recommendations from the DPA that the company needs to take specific action to comply with the Privacy Principles.

Importantly, the obligations under the Privacy Shield framework extend to companies that withdraw from the framework. If a U.S. company leaves the Privacy Shield and it chooses to keep the information, it must annually certify to the Department of Commerce its commitment to apply the Privacy Principles to information received under the Privacy Shield framework or provide "adequate" protection by another authorized means. An alternative authorized means of protection includes, for example, using a contract that incorporates the EU Model Clauses.

Remedies for Affected Individuals

The Privacy Shield provides certain rights and legal remedies to EU citizens. First, U.S. companies must have in place a process to address and resolve complaints about mishandled personal information of EU citizens.

All complaints have to be resolved within 45 days. Second, an alternative dispute resolution mechanism, free of cost to the individual, must be available in the U.S. for individuals to pursue unresolved claims of non-compliance.

EU citizens will also be able to obtain aid from their local DPA, which will work with the FTC or the Department of Commerce to ensure complaints are properly investigated and resolved. If the DPA submits a complaint to the Department of Commerce, the Department has committed to review complaints and facilitate their resolution within 90 days. Also, the FTC has committed to work with DPA to provide enforcement assistance, which could include information sharing and investigative assistance under the U.S. Safe Web Act.

Ultimately, if a complaint cannot be resolved by these mechanisms, at the request of the EU citizen, U.S. companies will have to submit the complaint to binding arbitration. The so called "Privacy Shield Panel" will make binding decisions against participating U.S. companies.

U.S. companies will be required to update their online privacy policies to explain how people can access these services, including a link to the website of their chosen dispute resolution provider.

In sum, compliance with the Privacy Shield will require a commitment of considerable resources by U.S. companies.

U.S. Government Assurances

The U.S. government has given the EU written assurance that any access by public authorities for national security purposes will be subject to defined limitations, safeguards, and supervision. An Ombudsperson within the Department of Commerce—independent from the national security agencies—will be appointed through whom EU citizens will be able to submit complaints or inquiries regarding possible access to personal information by U.S. intelligence services. Additionally, under the Judicial Redress Act, EU citizens will have access to U.S. courts to enforce privacy rights related to the transfer of personal information to the U.S. for law enforcement purposes.

Interim Compliance

Because the Privacy Shield has not yet been adopted, U.S. companies that received personal data of EU citizens under the Safe Harbor will need to use alternative mechanisms to comply with data sharing requirements of the Data Protection Directive 95/96/EC ("Directive"). The Directive regulates the export of personal data outside of the European Economic Area ("EEA") and prohibits EU companies from transferring personal data to companies outside the EEA unless those companies ensure adequate protection for the data (such as under the Privacy Shield). The Directive is implemented through the local laws of the Member States. The relevant DPA could, if it sees fit, launch enforcement actions against companies that have not implemented alternative, compliant data transfer mechanisms.

A U.S. company can continue receiving personal data by entering into certain standard forms of contracts known as EU Model Clauses or adopting so-called Binding Corporate Rules. Failure to comply with the Directive could result in the relevant DPA imposing monetary fines and sanctions, such as prohibiting future transfers of personal information (because the Directives are implemented through the laws of the Member States, the privacy laws of the Member State from which the data will be exported should be consulted).