European Commission Adopts EU-U.S. Data Privacy Framework: Developments That Could Impact Your Business

By Anna Mercado Clark and Paula P. Plaza

Phillips Lytle LLP

Anna Mercado Clark
Partner

Paula P. Plaza
Attorney

The General Data Protection Regulation (GDPR), a comprehensive European data protection law that has extraterritorial reach, permits the transfer of personal data from the European Economic Area (EEA), which includes EU countries, as well as Iceland, Liechtenstein and Norway, to other countries only under limited circumstances. U.S.-based companies may be subject to the GDPR. Non-compliance can result in fines potentially up to 20 million euros or 4% of gross global earnings, whichever is greater.

Cross-Border Data Transfers

Under the GDPR, personal data generally cannot be transferred from the EEA to countries without an adequacy decision from the European Commission (Commission) (i.e., a finding that the receiving country has adequate data protection). Absent an adequacy decision, cross-border data transfers may occur only if certain requirements are met, including but not limited to, appropriate safeguards, which can be achieved by, among other things, binding corporate rules, standard contractual clauses, or an approved certification mechanism. The U.S. does not have an adequacy decision, and earlier privacy frameworks (i.e., Safe Harbor and the Privacy Shield) created to facilitate routine cross-border data transfers were invalidated by the Court of Justice of the European Union.

The Recently Created EU-U.S. Data Privacy Framework

In March 2022, the EU and U.S. announced they had reached an agreement on a new transatlantic framework. The U.S. then adopted Executive Order 14086 (EO 14086) and a regulation establishing a Data Protection Review Court (AG Regulation). Updates were also made to the EU-U.S. Data Privacy Framework (DPF) that governs companies processing cross-border data transfers.

On July 10, 2023, the Commission adopted an adequacy decision which found that the DPF, along with the protections detailed in EO 14086 and AG Regulation, adequately protect personal data and permit cross-border data transfers from the EEA to certified organizations in the U.S. This decision means that personal data transfers under the DPF can occur without the need for further authorization.

The Impact on U.S. Companies

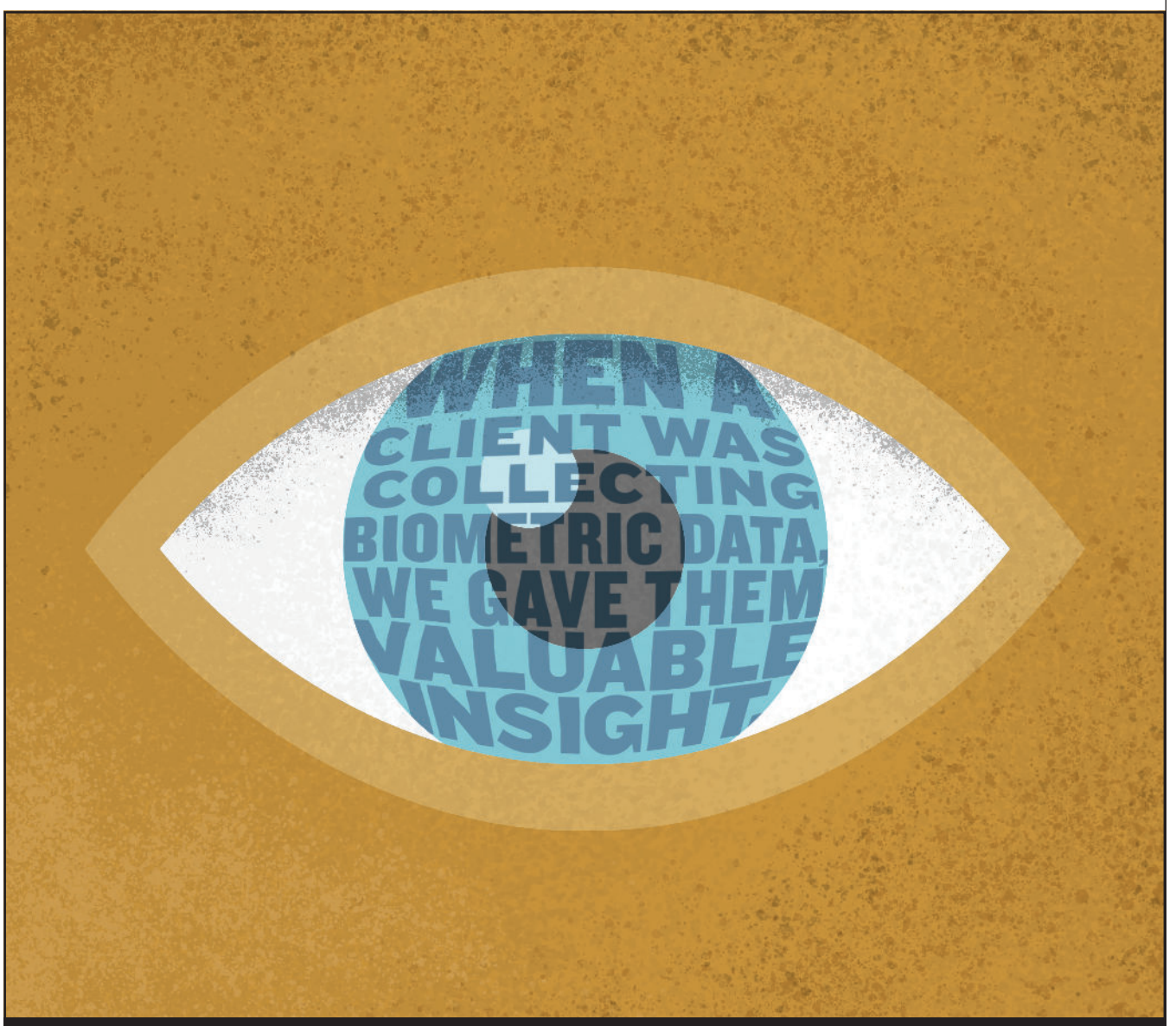
Eligible U.S. companies can participate in the DPF by certifying their commitment to comply with the privacy requirements outlined in the DPF Principles. These requirements include, but are not limited to, notifying individuals of their rights (including their right to access their personal data), limiting personal data to information relevant for achieving the purposes described for processing the personal data, and retaining personal data only for as long as it takes to achieve the purposes described for processing, subject to certain exceptions. As of July 17, 2023, eligible companies could self-certify their compliance with these DPF Principles. Companies that previously participated in the Privacy Shield have a three-month transitional period (i.e., a deadline of October 17, 2023) in which to comply with the new requirements, but can immediately rely on the DPF adequacy decision for cross-border personal data transfers without having to undergo the self-certification process set forth in the DPF.

First-time applicants should submit their draft privacy policy simultaneously with their self-certification to the U.S. Department of Commerce (DOC). The DOC will assess the submission for completeness and communicate updates to the applicants. Subsequently, the applicants should publish their privacy statements where necessary, and inform the DOC. Once these steps are completed, the DOC will add the applicants to its DPF list, authorizing them to conduct data transfers.

The Commission's adoption of the DPF confers certain efficiencies, but companies should stay vigilant regarding further guidance and developments, including potential legal challenges to the DPF. Companies should work with professionals who have the technical and legal expertise to guide them through the changing compliance landscape while considering their business needs.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, is a partner at Phillips Lytle LLP and leader of the firm's Data Privacy and Cybersecurity and e-Discovery Practice Teams. She can be reached at aclark@phillipslytle.com or (716) 847-8400 ext. 6466.

Paula P. Plaza, CIPP/E, is an attorney at Phillips Lytle LLP and member of the firm's Data Privacy and Cybersecurity and e-Discovery Practice Teams. She can be reached at pplaza@phillipslytle.com or (716) 847-8324.



Our deep knowledge of developing technologies and changing regulations helps keep you focused on staying compliant. That's The Phillips Lytle Way. Whether it is the collection and storage of biometric data, third-party risk management or data protection agreements, our Data Privacy and Cybersecurity Team knows how to keep you from being vulnerable. We are at the forefront of all this activity and have alerted clients of potential issues before laws were even implemented. We spot issues before they become issues. We can advise you on emerging regulations as well as privacy gaps that occur due to the remote workplace, supply chain databases, international vendors and employee error. Talk to us and learn why clients feel more secure working with Phillips Lytle.

Phillips Lytle LLP

Visit us at www.PhillipsLytle.com/DataSecurityLaw
Read our blog at DataSecurityAndPrivacyLawBlog.com

ONE CANALSIDE, 125 MAIN STREET, BUFFALO, NY 14203 (716) 847-8400
NEW YORK: ALBANY, BUFFALO, CHAUTAUQUA, GARDEN CITY, NEW YORK, ROCHESTER | CHICAGO, IL | WASHINGTON, DC | CANADA: WATERLOO REGION
Prior results do not guarantee a future or similar outcome. © 2023 Phillips Lytle LLP