SQUIRE PATTON BOGGS

Privacy Shield Package Released; EU Determination of "Adequacy" Next

The United States and the European Union today released a 128-page package of "EU-U.S. Privacy Shield materials," which flesh out the Framework agreed to on February 2. Called the "Privacy Shield Package" in the transmittal letter from US Secretary of Commerce Penny Pritzker, the package is founded on a series of "EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce."

Before organizations can rely on the Privacy Shield, a number of steps remain to be implemented, including submission of the package to Article 29 Working Party (comprising national data protection authorities) for an opinion and discussion with Member States and the European Data Protection Supervisor. These stakeholders may have concerns about the substance and enforceability of the package. Ultimately, the European Commission will need to formally adopt the adequacy decision before it takes effect. Even then, the Privacy Shield may be challenged before the European Court of Justice, as Safe Harbor was last year. Thus, it is difficult to predict when the approval process will be complete, and organizations can rely on the Privacy Shield. Until such time, consent, model clauses and BCRs remain viable options.

The Principles

In order to rely on the Privacy Shield to effect transfers of personal data from the EU, an organization "must self-certify its adherence to the Principles to the" Commerce Department or its designee. To be eligible to do so, an organization must, among other things, be subject to the investigatory and enforcement powers of the Federal Trade Commission, the Department of Transportation or another statutory body that will "effectively ensure compliance with the Principles." Such certification is voluntary, but once made, "effective compliance is compulsory." Self-certification must be done annually.

The basic Principles address (a) notice requirements, (b) individual "opt-out" mandate, (c) accountability for onward transfer, (d) data security, integrity and purpose limitations, (e) individual access, (f) individual recourse, and (g) enforcement and liability.

A series of Supplemental Principles address (a) sensitive data, (b) journalistic exceptions, (c) secondary liability (e.g., non-liability for organizations that "merely transmit, route, switch or cache information"), (d) performing due diligence and conducting audits, (e) the role of the DPAs, (f) details of the self-certification process, (g) verification of organizations privacy practices, (h) details on the right of individual access, (i) application to human resources data, (j) requirement for contract when data transferred only for processing purposes ("onward transfers"), (k) dispute resolution and enforcement (including details on recourse mechanisms, remedies and sanctions, FTC action, import of persistent non-compliance, (l) timing of "opt-out" choice, (m) handling of travel information, (n) data for pharmaceutical research, medical products and other purposes, (o) public record and publicly available information, and (p) access requests by public authorities.

The Privacy Shield is to be administered in the US by the International Trade Administration of the Department of Commerce (ITA), and the package includes a letter from the ITA describing the Commerce Department's commitments (a) ensuring that the Privacy Shield operates effectively and (b) relating to the new arbitral model relating to dispute resolution under the Privacy Shield.

US Agency Commitments

Also included as part of the package are letters from the following US agencies:

- Federal Trade Commission and Department of Transportation, describing their respective enforcement of the Privacy Shield;
- Office of Director of National Intelligence, regarding safeguards and limitations applicable to US national security authorities;
- Department of State, describing the commitment to establish a new Privacy Shield Ombudsman for submission of inquiries regarding US signals intelligence practices; and
- Department of Justice, regarding safeguards and limitations on US Government access for law enforcement and public interest purposes.

Next Steps and Uncertainties

As noted above, and acknowledged by Secretary Pritzker in her transmittal letter, the next step is for the EU to review and make a determination of "adequacy." There is no specific deadline for this determination to be made. Opinions issued by the EU Article 29 Working Party (which comprises the national data protection authorities of EU member states) will be central to an EU determination on whether Privacy Shield would adequately protect EU citizens' personal data that is transferred to the US.

The Article 29 Working Party expects to complete its review by the end of March. The EU Commission's draft adequacy decision would then need to be adopted by the EU Commission and approved by the Article 31 Working Group (representing EU Member states) before it became law. Any material changes would require further negotiation with the US authorities.

Current Options: Consent, Model Clauses and BCRs

In the meantime, until this process is completed, model contract clauses, consent and binding corporate rules appear to remain viable options. Their longer term viability through implementation of the Privacy Shield could depend on how the Article 29 Working Party views the adequacy of the Privacy Shield in relation to the applicable EU rules and the principles laid down by the European Court of Justice in the Schrems case.

The new framework will introduce a detailed set of new obligations and procedures that will require prior Safe Harbor participants to consider their options. For example, under the new framework, businesses have 45 days to resolve complaints from EU citizens regarding the use of their personal information and will be subject to various requirements and options in this regard. As a last resort, unresolved cases may be subject to an enforceable arbitration mechanism. Additionally, companies may commit to comply with advice from European DPAs, which will be mandatory for companies processing EU human resources data in the US.

Finally, it is important to recognize that this announcement is the beginning and not the end of a process. Furthermore, even if the EU Commission adopts a decision finding that the US ensures an adequate level of protection under the new framework, there is still the prospect its decision could be challenged before national data protection authorities, national courts and the European Court of Justice – just as occurred in the case of the Privacy's Shield's predecessor, the Safe Harbor framework.

Contacts

Ann J. LaFrance
E ann.lafrance@squirepb.com

Philip R. Zender
E philip.zender@squirepb.com

France

Stéphanie Faber
E stephanie.faber@squirepb.com

Germany

Andreas Fillmann
E andreas.fillmann@squirepb.com

Annette Demmel
E annette.demmel@squirepb.com

UK

Caroline H. Egan
E caroline.egan@squirepb.com

US

Paul C. Besozzi
E paul.besozzi@squirepb.com

Gretchen A. Ramos
E gretchen.ramos@squirepb.com