crowell moring

CLIENT ALERT

EU Data Protection Authorities Partially Extend Grace Period After Announcement of 'EU-U.S. Privacy Shield'

Feb.03.2016

The Article 29 Working Party (WP29), consisting of the data protection authorities (DPAs) of all 28 European Union (EU) Member States, today confirmed that due to the announcement of the "EU-U.S. Privacy Shield" (Privacy Shield), the deadline for widespread enforcement actions involving EU-U.S. data transfers will partially be extended.

Isabelle Falque-Pierrotin, Chair of WP29, confirmed in a press conference on February 3, 2016 that all EU Member States' DPAs have uniformly agreed to continue to allow the use of EU-approved model contract clauses and Binding Corporate Rules (for intra-company transfers only) for data transfers to the U.S. until the new Privacy Shield has been analyzed and assessed by WP29. The decision to adopt the Privacy Shield formally lies with the European Commission (EC), but the DPAs' opinion is important in practical terms with regard to implementation, enforcement, and potential legal challenges to the framework.

The WP29 has set an end-of-February deadline for the EC to provide the Privacy Shield documents for WP29 review. A WP29 plenary meeting is expected in March 2016 to discuss the Privacy Shield in detail, and a WP29 opinion is expected at the end of March 2016 or beginning of April 2016.

What Companies Should Do Until the Privacy Shield is Implemented

Individual EU Member State DPAs remain free to carry out investigations and enforcement actions against companies that have not put in place transfer mechanisms apart from the invalidated U.S.-EU Safe Harbor Framework (Safe Harbor), particularly when the DPAs receive individual complaints from EU citizens. Relying solely on Safe Harbor certification for EU-U.S. data transfers would "clearly be illegal" as a result of the judgment of the European Court of Justice (ECJ) on Safe Harbor, according to Falque-Pierrotin.

As a result, U.S. companies that were previously relying solely on Safe Harbor for their EU-U.S. data transfers are expected to implement non-Safe Harbor transfer mechanisms unless and until the Privacy Shield is implemented and the company has certified to it. This is a critical interim requirement, particularly with regard to transfers from those EU Member States whose DPAs have been critical of EU-U.S. data flows generally.

As we mentioned in yesterday's client alert, the remaining legitimate transfer mechanisms are:

- EU-approved model contract clauses.
- Binding Corporate Rules (for intra-company transfers only).

Certain other specific derogations that companies could rely on include:

- informed consent of the data subject (though this may not be possible for human resources or other data relating to employees);
- performance of a contract (*e.g.*, limited to circumstances such as booking a hotel in the U.S. where personal information must be provided to the U.S. entity to fulfill the contract).
- important public interest grounds (*e.g.*, cooperation between authorities regarding fraud or cartel investigations).
- the vital interest of the data subject (*e.g.*, urgent life or death situations).

Assessment of Other EU-U.S. Transfer Mechanisms

While WP29 confirmed that companies should use the alternative transfer mechanisms (besides Safe Harbor and the yet-to-be-implemented Privacy Shield) until the Privacy Shield is implemented, they reiterated their intent to continue to review the alternative mechanisms, along with the Privacy Shield, with regard to compliance with the ECJ decision. Over the past few weeks, WP29 came to the preliminary conclusion – while reviewing the alternative transfer mechanisms (e.g., model contract clauses and Binding Corporate Rules) against the ECJ Safe Harbor decision – that there are four essential guarantees that any transfer mechanism from the EU to any third country must provide, which are as follows:

1. Processing should be based on clear, precise, and accessible rules.
2. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated (with regard to national security data access).
3. An independent oversight mechanism must be present.
4. Effective remedies must be available to individuals.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Jeane A. Thomas, CIPP/E
Partner – Washington, D.C., Brussels
Phone: +1 202.624.2877, +32.2.282.4082
Email: jthomas@crowell.com

Frederik Van Remoortel
Partner – Brussels
Phone: +32.2.282.1844
Email: fvanremoortel@crowell.com