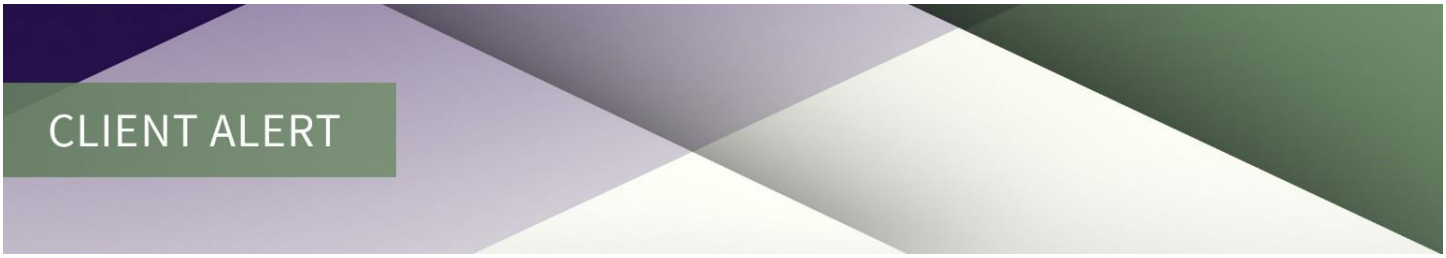
WILLKIE FARR & GALLAGHER LLP



European Data Protection Board Adopts Guidance on Supplemental Transfer Tools

June 29, 2021

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Richard M. Borden | Henrietta de Salis
Marilena Hyeraci[*] | Stefan Ducich

On June 18, 2021, the European Data Protection Board ("the EDPB") adopted its recommendations on measures that supplement transfer tools to ensure compliance with the European Union ("EU") level of protection of personal data ("the Recommendations"). This follows a consultation period regarding the draft Recommendations published in November 2020, and comes on the heels of the release of the updated Standard Contractual Clauses ("SCCs") earlier this month by the European Commission ("the Commission").

The final Recommendations represent a shift from the November 2020 draft, with the EDPB now incorporating risk-based assessments for data transfers based on the likelihood of third-country law enforcement accessing transferred personal data. However, differences remain between the Recommendations and the SCCs. The Recommendations increase the scope of review and level of documentation required to demonstrate compliance, which will require significant ongoing recordkeeping. These requirements will further increase diligence burdens on companies transferring data from the EU to third countries not deemed to have "adequate" data protection regimes.

[*] Marilena Hyeraci is an associate at Studio Legale Delfino e Associati.

Background

In July 2020, the European Union Court of Justice invalidated the EU-U.S. Privacy Shield framework in *Schrems II*. This increased uncertainty around the lawfulness of personal data transfers from the EU to the United States ("U.S."), including through the use of SCCs.

In November 2020, the EDPB and the Commission issued draft versions, respectively, of the Recommendations and the SCCs, which notably diverged over the permissibility of risk-based data transfer assessments. The draft Recommendations suggested that even theoretical access by governmental authorities to transferred personal data (e.g., for criminal law enforcement, regulatory supervision, and national security purposes) might render the transfer unlawful for the purposes of General Data Protection Regulation ("GDPR"). Moreover, the EDPB stressed in its January 2021 comments on the draft SCCs that an assessment of a third country's law and practice must be objective "regardless of the likelihood of access to the personal data."[1]

Earlier this month, on June 14, the Commission adopted the new SCCs, which adopted a subjective, risk-based approach to third-country law and practice rather than the formalistic approach promoted by the EDPB.

The Recommendations

The EDPB and the Commission appear to have reached what has been described as a practical compromise on the question of risk-based data transfer assessments, which attempts to account for the likelihood that governmental authorities will seek or obtain access to transferred personal data. Both the Recommendations and the SCCs require a case-specific analysis of the law and practice of third-country destinations, or third countries through which transferred personal data may transit, with respect to the protections provided for such data. The adoption of this subjective analysis represents the greatest substantive distinction between the November 2020 draft and the Recommendations as adopted. However, the scope of review and level of documentation required to complete this analysis and demonstrate compliance with the Recommendations will be significant.

[1] EDPB-EDPS Joint Opinion 2/2021 on the European Commission's Implementation Decision on standard contractual clauses for the transfer of personal data to third countries (here).

First, the Recommendations set forth a specific legal analysis which is more nuanced than that required by the SCCs. The Recommendations emphasize not only the analysis of the governing legislation, but also address situations where known practice suggests that non-enforcement of, or non-compliance with, such legislation may be expected. These assessments should be made in consultation with legal counsel, must include relevant internal and external operational and technical components related to the transfer, and may be based upon the following publicly available sources of information:

- Relevant case law;
- Adequacy decisions (if the transfer relies on a different legal basis);
- Resolutions and reports from intergovernmental organizations;
- Reports and analyses from competent regulatory networks;
- Reports of independent oversight or parliamentary bodies;
- Reports based on practical experience with prior instances of requests for disclosure (or the absence of the same);
- "Warrant canaries" of other entities processing data in the same field as the importer, or of the importer itself;[2]
- Reports produced or commissioned by Chambers of Commerce, business, professional and trade associations, governmental diplomatic, trade and investment agencies of the exporter or other third countries exporting to the destination country;
- Reports from academic institutions and civil society;
- Reports from private providers of business intelligence on financial, regulatory, and reputational risks for companies;
- Transparency reports; and
- Internal statements or records of the importer expressly indicating that no access requests were received for a sufficiently long period.

[2] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Annex 3.

Generally, where uncertainties arise in light of the application of "problematic legislation,"[3] either the transfer must be suspended or supplemental measures must be implemented. However, where the parties determine they "have no reason to believe that relevant and problematic legislation will be applied, in practice, to [the] transferred data" in such a manner as to prevent the importer from fulfilling its obligations under GDPR,[4] supplemental measures beyond the SCCs may not be necessary.

Required Documentation – A Comprehensive Report

Next, per the Recommendations, the data transfer risk assessment and resulting findings must be documented in a detailed report. This report must demonstrate through "relevant, objective, reliable, verifiable, and publicly available or otherwise accessible information" that problematic legislation, as applied in practice, will not interfere with a data importer fulfilling its obligations under GDPR Article 46.[5] Moreover, the report must identify all actors involved in the assessment (e.g., law firms, consultants, or internal departments), the dates of the relevant checks or assessments made, and it must be kept up to date. The report should also be endorsed by the legal representative of the data exporter. The data exporter and data importer may be held liable for any decisions taken on the basis of the data transfer risk assessment report, which may be requested by competent supervisory authorities and/or judicial bodies.

Practical Outcomes

Companies will have to further build out their GDPR compliance programs to accommodate ongoing assessment of third-country data protection laws and practices, and – as reinforced by yesterday's announcement that the Commission adopted an adequacy decision for EU-UK data flows – companies will need to stay flexible as they make decisions in the context of a fluid legal landscape. The assessment will likely require increased due diligence, deep legal analysis of relevant law and practice, and the maintenance of detailed records. We may expect a more standardized process to develop over the coming months as companies and their counsel perform these detailed analyses, as further guidance is issued by regulatory bodies, and/or as trade associations weigh in, though no timeline on standardization is available. Moreover, questions remain concerning the acceptable methods of verification of the publicly available information used in the analysis described above. One thing is clear: companies relying on SCCs will face significant burdens in the near future for both analysis and documentation.

3 *Id*. at Para. 43.

4 *Id*.

5 *Id*. at Para. 46.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Henrietta de Salis
+44 20 3580 4710
hdesalis@willkie.com

Marilena Hyeraci
+39 02 76363 1
mhyeraci@delfinowillkie.com

Stefan Ducich
+1 202 303 1168
sducich@willkie.com