Track Changes

November 2020

EDPB ON SCHREMS II: THE END OF U.S. CLOUD SERVICES?

The decision of the Court of Justice of the European Union (CJEU) in *Schrems II* (C-311/18) left companies without a clear framework for transfers to the US (see our first client alert). Authorities highlighted that the invalidation of the Privacy Shield is enforceable without any grace period and that the use of Standard Contractual Clauses (SCCs) required, yet left undefined, *additional safeguards* (see our second client alert).

Now, after almost four months, the European Data Protection Board (EDPB) published its guidance on additional safeguards (available here). These recommendations feature more than a dozen technical, contractual and organizational measures. However, the EDPB itself concludes that the latter two categories may only be feasible where local laws of the third country are in line with EU data protection principles in the first place. Aside from stopping data transfers altogether, companies are left with a variety of "nice-to-have" but insufficient measures, and merely two concrete options for effective technical measures remain:

- **OPTION A – ENCRYPTION (USE CASE 1)**

  Using US-services only for data storage of fully encrypted data back-ups with autonomous key management by the EU exporter (which is not a subsidiary of the US-entity). This option, however, does not encompass and, thus, excludes any use of remote processing services, data analytics or communication services.

- **OPTION B – PSEUDONYMIZATION (USE CASE 2)**

  Only transmitting truly pseudonymized data. Companies must ensure that neither the data importer nor the authorities would be able to re-identify the data subjects, even considering other information available to the data importer or the authorities e.g. by cross-reference. The EDPB specifically states that interactions with internet-based services may allow for identification even if names, addresses or other plain identifiers are omitted. Practical use cases will therefore also be limited.

- **ALTERNATIVE: A CHALLENGE OF THE EDPB GUIDELINES**

  Implementing (other) proportional measures to ensure an appropriate level of data protection for the data processed and the risk associated thereto. With respect to Use Case 6 (page 26 of the recommendations), the EDPB states that it cannot envision an effective technical measure for using cloud service providers.

WHAT'S MISSING

Data localization: Data localization is one of the most commonly implemented measures since the invalidation of the Safe Harbor Framework by the decision *Schrems I* (CJEU, C-362/14). However, given the global territorial scope of US surveillance laws (e.g. FISA or CLOUD Act), data localization *alone* may only provide limited mitigation (e.g. against surveillance in transit). The EDPB does not mention data localization, which may further reduce the legal value such technical measures could provide.

Proportionality: The EDPB acknowledges that privacy is not an absolute right. With respect to the Charter of Fundamental Rights of the European Union, limitations must be proportionate, necessary and in pursuit of general interests recognized by the Union. The now published guidelines do not reflect arguments raised by Deputy Assistant Secretary James Sullivan (available here) concerning the limited scope of application of US surveillance practices, as well as the general interest of the EU in cooperation and data sharing with US surveillance agencies. Additionally, the EDPB does not evaluate which measures would provide an adequate mitigation for which types of transmissions or data categories.

Art 49 GDPR: The EDPB confirms that Art 49 derogations do not require an assessment of the level of protection in the third country. However, it reiterates its standpoint that *all* derogations mentioned in Art 49 have an exceptional nature as mentioned in its prior guidelines (available here).

TAKE-AWAYS

While the decision of the CJEU left companies with uncertainty regarding transfers to the US, the guidelines of the EDPB mean that everyone using US cloud services will be in an uphill battle from now on. Companies must thoroughly review and document any measures that, in their assessment, provide an essentially equivalent level of data protection. Additionally, such measures must be assessed, knowing that the EDPB, in almost 40 pages, stated that it is "incapable of envisioning any effective *technical* measures".

When using US service providers, companies may therefore primarily rely on the suggested contractual and organizational measures in order to provide utmost transparency and ensure data subjects remain in control of their data.

***

About WOLF THEISS

Wolf Theiss is one of the leading law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We have built our reputation on a combination of unrivalled local knowledge and strong international capability. We opened our first office in Vienna over 60 years ago. Our team now brings together over 340 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region.

For more information about our services, please contact:

Roland Marko
Partner
roland.marko@wolftheiss.com
T: +43 1 51510 5880

Paulina Pomorski
Senior Associate
paulina.pomorski@wolftheiss.com
T: +43 1 51510 5091

Johannes Sekanina
Associate
johannes.sekanina@wolftheiss.com
T: +43 1 51510 5881

Wolf Theiss
Schubertring 6
AT – 1010 Vienna

www.wolftheiss.com