August 2020

THE FUTURE OF DATA TRANSFERS TO THE US

More than one month after the pivotal *Schrems II* decision of the Court of Justice of the European Union (CJEU), companies may still find themselves without clear guidance for the transfer of personal data to the US. The CJEU only defined key areas which must be reviewed when assessing the legal framework of the third country (see our client alert). In the same decision, the CJEU upheld the general validity of Standard Contractual Clauses (SCCs). However, where SCCs alone cannot provide an adequate level of protection, contractual frameworks must be amended by additional measures.

To date, most national data protection authorities have published statements acknowledging the decision though none of these statements included further clarification on the additional measures demanded by the CJEU. Companies were only reminded of their obligation to assess the legal framework in place when transmitting data to third countries. Similarly, the Austrian Data Protection Authority also issued a general statement referring to the response of the European Data Protection Board and addressing the CJEU's decision without further clarification.

Only on 24 August 2020, the data protection authority of Baden-Württemberg (LfDI-BW), Germany, published the first information on specific measures in their *Guidance regarding Schrems II* (available as PDF in German here).

ADDITIONAL MEASURES FOR SCCS

In order to evaluate which additional measures must be implemented, data exporters must first identify which risks are not yet addressed by the SCCs. The measures must then address these country specific risks. For the US, the CJEU reviewed US Executive Order 12333 allowing the NSA to access data in transit to the US, as well as Section 702 of the FISA Act allowing for surveillance of Non-US citizens without a court order. In both cases data subjects are not informed and have no actionable rights before the courts against US authorities.

The following measures can offer possibilities to mitigate the identified risks:

Data localization: Storing data solely and exclusively within the EU may mitigate potential risks of surveillance in transit. However, where national surveillance laws (e.g., the US CLOUD Act) require companies to provide government authorities access to all data processed by them worldwide, data localization alone does not mitigate all risks.

Encryption of data: Adequate encryption restricts the access to personal data and thus increases the level of protection offered to data subjects. For encryption to be a viable protection measures, the implemented processes must ensure that data is encrypted prior to being transferred (as data in transit can be surveilled), and that the decryption key is not available to the data importer. Otherwise, national authorities may either intercept data being transferred to the third country or may enforce administrative orders against the data importer to decrypt the data or receive the key. The data exporter must therefore be in sole control of the key management. Where services use the imported data on behalf of the data exporter (e.g., a newsletter service), data must be available to the data importer and thus are potentially exposed to access requests. Notably, this approach was also mentioned and acknowledged by the LfDI-BW. In any case, it must be highlighted that encrypted data is still personal data. Neither a Caesar cipher nor AES256 can change this classification.

Pseudonymization: Where the encryption of data is not possible, companies may choose to pseudonymize the transferred data. Just as with encryption, data must be pseudonymized prior to transmission and the data exporter must remain in sole control of the pseudonymization table. Even so, the level of protection will only be improved where the data importer and national authorities will effectively not be able to assign data to individuals.

Anonymization: True anonymization removes any personal reference in an irreversible manner. Data anonymized in such a way is no longer subject to the EU General Data Protection Regulation ("GDPR") and thus can be shared without data protection restrictions. As with encryption and pseudonymization, the anonymization must be conducted by the data exporter prior to transmission. Anonymization, however, will in many cases not be a viable solution where the personalization of data is of the essence.

Additional contract clauses: In addition to the SCCs, additional contract clauses can be implemented to increase the level of protection. For the SCCs regarding transmissions of an *EU controller to non-EU or EEA processor*, such clauses may, according to the LfDI-BW, include:

SCC clause	**Proposal of the LfDI-BW**	**Comment Wolf Theiss**
4f	Extension of the notification obligations to data subjects for all cases where any data, not just special categories of data, are transferred to a third country without an adequate data protection level.	These information requirements are already mandatory according to Art 12 and 13 GDPR. We do not see much added value in this.
5d	Obligation of the data importer to challenge any governmental access request before courts and only disclose data upon a final court judgement.	This provides additional comfort and similar clauses have already been put in place by major service providers.
5d i	Notification not only of the data exporter, but also the data subject in case of a governmental access request, or where this is not possible, notification of the data protection authority of the data subject or data exporter respectively.	This broad instruction to communicate with the data subjects directly interferes with the distinctive roles of controllers and processers and should be used with care.

7 (1) lit a, b	Acceptance of dispute resolution *solely* by the courts of the Member State in which the data exporter is established. This proposal would delete clause *7 (1) lit a* regarding mediation by an independent person.	From a formal perspective, data subjects would be deprived of rights they have under the original wording of the SCC. Also, deleting a clause will most likely result in the obligation to apply for authorization by the supervisory authority (see below).
Annex 2	Liability of the data importer.	The liability clause increases the stakes for the data importer. In any case, such clauses are already common in data processing agreements and therefore do not necessarily have to be repeated.
n/a	Additionally, but not highlighted by the LfDI-BW: Right of the data exporter to terminate the contract where an adequate level of protect cannot be maintained.	Termination on good cause or in case of violation of a contractual or legal obligation by the data importer are already widely used in data processing agreements. Termination clauses may include reimbursements for the data exporter.

While the CJEU and recital 109 GDPR allow for adding clauses to the SCCs, contradicting or deleting clauses would require their users to obtain the prior approval of the amended clauses of the competent supervisory authority. Also, it is uncertain whether a supervisory authority would approve of SCCs as amended in accordance with the suggestions of the LfDI-BW.

TAKE-AWAYS

In order to maintain transmissions to the US, companies must assess how the exposure to US surveillance laws can be mitigated. The CJEU requires companies to assess the level of protection on a case-by-case basis. While this may retrieve memories from extensive compliance audits prior to the GDPR coming into effect, it also opens opportunities for companies to choose both technical and legal safeguards suitable to the individual matter.

Interceptions in transit (EO 12333) may be mitigated by a combination of encrypting transmitted data and a contractual obligation to refrain from voluntarily assisting governmental operations.

Section 702 of the FISA Act is primarily applicable for all electronic communication service providers. However, where companies are not directly subject to such Section 702 orders or have not received any orders in the past, arguments can be made that a combination of transit encryption and notification obligations can increase the level of protection provided for data subjects.

However, these theoretical possibilities may not be feasible for all applicable cases or other surveillance laws (especially the CLOUD Act, or upcoming variations of the LAED Act or the EARN IT Act).

While the decision of the CJEU is solely covering the transfer of data to the US, the same criteria and principles will apply to data transmission to any other third country where SCCs should be employed.

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