DBS
DATA BUSINESS SERVICES
EUROPEAN DATA PRIVACY+ PROTECTION

International Data Transfer – Next Steps

&

Standard contractual clauses (SCC)

Scope

The uncertain legal situation regarding an appropriateness decision for the UK forces companies to take early precautions in order not to violate general data protection regulations after the transition period on January 31, 2020. Like other third countries without an adequacy decision by the European Commission, companies involved in data transfer from the UK to the EU and vice versa must implement other appropiate safeguards such as standart contractual clauses. When using SCC for international data transfer, especially to the USA, it is very important to analyze the Shrems II case and take the ruling into account.

Companies should now urgently - and immediately, without waiting - make an inventory of their data exports to third countries and initiate improvement processes with their service providers or other data importers from third countries.

Data Mapping

Companies must identify the international data transfers and implemented transfer mechanisms in their area of responsibility. This includes both data transfers between individual Group companies, including the transfer of employee data within the Group, and transfers to service providers, business partners or other third parties. The complete life cycle of the data is documented. From data collection to the scheduled deletion of data. Mapping also makes it possible to exclude the possibility that, for example, a legal basis that no longer exists, such as the "Privacy Shield", may be used to process personal data.

Type of data collected

A description of the categories of data subjects and the categories of personal data

Purpose of data collection

Storage period of data

Where the data is storaged

Conditions of data storage

Legal basis for data processing

If Shared with third parties

Location of third party (especially international)

The protocols followed during the data transfer

DBS

Having a solid data map implemented can help to minimise the risk of data breaches and privacy threats by ensuring that no data enters or leaves the company without being fully accounted for.

Without a detailed insight into data lifecycle, it is difficult to implement any security. Data mapping becomes an essential step to achieve GDPR compliance. The following GDPR articles and their requirements will help you understand the importance of data mapping further:

Article 6 : Data mapping helps you show the basis of processing.

Article 25 : Data mapping helps you display your commitment to data privacy.

Article 28: Data mapping allows GDPR auditors to comprehend the extent of 3rd party access to personal data.

Article 30: GDPR article on Data mapping provides a written record, which you can easily retrieve, complement and present at the time of the GDPR audit.

Article 35: Data mapping enables business enterprises to satisfy Data Protection Impact Assessment (DPIA) effectively.

Additional diligence

Furthermore, affected companies must initiate organizational improvement processes with their service providers or other data importers from third countries.

- Understand the power of law enforcement in the affected country

- For EU companies this means that they must specifically ask their importer in the USA whether he is subject to FISA702 and/or E.O. 12.333 and whether he has already had to release data on this basis. A similar procedure can be carried out for other countries.

If this is the case, it must be determined which data was transferred in this case.

- Develop standard questionnaire for foreign companies concerned

- Obtain information on the legal situation in the third country (public bodies such as the data protection supervisory authorities, the European Data Protection Committee (EDSA), the EU Commission or the Federal Foreign Office should be able to provide assistance in this regard)

- If possible, companies should move the processing location of their data to Europe or a EEA area. This means that the data processor is located in the European Union instead, which avoids overlap with foreign supervision laws and the GDPR. This is particularly important if no additional guarantees for the data subjects can be created or agreed.

Technical measures

Furthermore, technical measures must be communicated and implemented with the data importer in the third country in order to minimize the existing security problems, which are discussed in connection with international data transfer.

These could be additions to Appendix 2 in the Standard Contractual Clauses, which documents mandatory technical measures of the data importer and exporter to ensure a sufficient level of data protection according to GDPR:

Appendix 2

2a. Data security measures Sphere of the Data Importer

Where personal data are processed, security measures must be taken to,

1. ..prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used **(access control)**
2. ..prevent data processing systems from being used without authorization **(access control)**
3. ..ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage **(access control)**
4. ..ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged **(transmission control)**
5. ..ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed **(input control)**
6. ..ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal **(job control)**
7. ..ensure that personal data are protected from accidental destruction or loss **(availability control)**
8. ..ensure that data collected for different purposes can be processed separately.

2b. Data security measures implemented in Sphere of the Data Importer accessing the it-infrastructure of the data exporter

- Encryption

The data controller should in particular check whether the protection can be realized on a technical level by means of (end-to-end) state-of-the-art encryption using a strong crypto-algorithm.
It should also be examined to what extent the key management can be controlled by the person responsible and whether data is encrypted only during transport (Data in Transit) or also on data processing servers (Data at Rest). Only end-to-end encryption (E2EE) offers maximum security here.

- Anonymization and Pseudonymization

Alternative technical-organizational measures can also be considered, such as the anonymization of personal data or pseudonymization (e.g.: use of a pseudonymization gateway).

- Decentralized data storage
- Perimeter Security
- Zero Trust Network Access (ZTNA)
- Secure Access Service Edge (SASE)-Platforms
- Cloud Access Security Broker (CASBs)
- Secure Web Gateways (SWG)
- Endpoint Detection and Response (EDR)

2c. Data security measures implemented in Sphere of the Data exporter when opening the the it-infrastructure to the data exporter

- Separate delivery portal
- Digital acknowledgements of receipt
- Advanced Virtual Private Network (VPN)
- Permanent monitoring of the regular operation
- Security Information and Event Management (SIEM)

2d. other additional measures

- Only use specially trained personnel for data export/import
- The criticized US monitoring programs focus primarily on large telecommunications companies. Companies that send their data via or to such companies (e.g. via cloud services or external e-mail servers) thus expose them to a greater risk, whereas group-owned servers are likely to be less exposed.
- Separation controls: Personal Data collected for different purposes shall be capable of being processed separately.

Contractual protection

According to the ECJ judges, the Standard Contractual Clauses can still be used for the transfer of personal data to a third country under certain conditions. However, there is an obligation on the part of the data exporter as well as the data importer to review the data transfer. This obligation to review relates to whether the Standard Contractual Clauses already provide sufficient guarantees for the transfer or whether additional guarantees need to be created or agreed upon.

In the absence of effective additional guarantees, in order to at least demonstrate and document your willingness to act in accordance with the law, you should contact the respective recipient of the data and agree in particular on the following additions to the provisions of the standard contractual clauses, which are best set out in a separate agreement or in the main contract.

- For already existing contracts: Obtaining an updated confirmation from the data importer that to his knowledge there are no laws in the recipient country that prevent the processing of personal data in accordance with the contract. Depending on the possibility of influencing the design of the data protection contract with the data importer in general, the permissibility of data access by authorities can be specified in more detail by a business-related clause.

- Inclusion of a contractual clause that makes data access by public authorities to the data at the data importer dependent on prior transparent information and subsequent approval by the data exporter.

- In order to enable the data exporter to assess the data transfer to authorities on a case-by-case basis, a contractual clause can be used which stipulates that the data importer must obtain permission for data access by authorities. In this way, the data exporter is informed of the individual request and can check it for admissibility.

- Supplement Annex Clause 4f: Informing the data subject not only when special categories of data are transferred, but also in any data transfer (before or as soon as possible after the transfer) that their data will be transferred to a third country that does not provide an adequate level of protection within the meaning of Regulation (EU) 2016/679.

- Supplement Annex Clause 5d i: Obligation of the data importer to inform not only the data exporter, but also, to the extent known, the data subject without delay of any legally binding requests by an enforcement authority to transfer the personal data.

- Addition to Annex Clause 5d : The obligation of the data importer to take legal action against the disclosure of personal data and to refrain from disclosing the personal data to the relevant authorities until a competent court of last instance has issued a final judgment ordering the disclosure.

- Addition to Annex Clause 5 h : the obligation of the data importer, if known to him, to also notify the data subject of the award of a processing contract to a sub-processor.

- Addition of Clause 6 : The addition that the data subject who has suffered damage as a result of a breach by a party or the sub-processor of the obligations referred to in clause 3 or 11 is entitled to obtain compensation for the damage suffered not only from the data exporter but also from the data importer.

- Inclusion of an obligation on the data importer to Affected persons independent of fault from all damages which are caused by the access of authorities of his state to the data of the persons concerned.

The European Commission has reported that it will develop and publish guidelines before the end of the year to make it easier for companies to reformulate their SSC's in accordance with the Schrems II ruling and to provide them with necessary additional guarantees.

I HAVE SOME UNANSWERED QUESTIONS. WHOM DO I CONTACT?

For more information, kindly send an email to

niedermeier@data-business-services.com

RA Robert Niedermeier CIPP/E CIPT CIPM FIP