大成 DENTONS

Data Transfers – What's Next?

Transferring personal data outside the European Economic Area (EEA) is one of the greatest data protection challenges facing most businesses. The level of protection required for data transfers has risen significantly in recent years. This brochure gives an overview of the current data transfer legal framework and outlines the data transfer solutions that are available.

Personal data transfer regulations

Companies intending to transfer personal data from the EU to countries outside the EEA should ensure that the level of protection of natural persons ensured by the GDPR is not undermined by the transfer and meets the requirements laid down in Chapter V of the GDPR.

In general, transferring personal data outside the EEA is allowed in cases where:

i. the European Commission has decided that the given third country ensures an **adequate level of protection** – in an "adequacy decision" (e.g. as recently issued for the UK), or

ii. the transfer is subject to **appropriate safeguards** (transfer tools set out in Article 46 of the GDPR) – e.g. Standard Contractual Clauses (SCCs) adopted by the European Commission. Although Chapter V of the GDPR provides for alternative data transfer tools (other than SCCs), e.g. binding corporate rules / codes of conduct, they are of limited practical use at present.

Therefore, when dealing with transfers out of the EEA, companies should check whether the country of the data recipient is covered by an adequacy decision. If not, appropriate safeguards should be used such as Standard Contractual Clauses. While the GDPR provides for certain derogations from this obligation, in practice they only apply in exceptional circumstances.

New Standard Contractual Clauses

As of 4 June 2021 the European Commission published a final implementing decision adopting the new Standard Contractual Clauses (new SCCs).

The old SCCs, pre-dating GDPR, do not meet current data protection requirements. They fail to address the complexity of today's international data flows, e.g. by not allowing for onward transfers from a processor to a sub-processor.

The new SCCs are adapted to the GDPR and cover all four types of contractual relationships:

i. controller to controller (C2C),

ii. controller to processor (C2P),

iii. processor to processor (P2P) and

iv. processor to controller (P2C).

For the wording of the new SCCs please go here.

When to switch to the new SCCs?

Companies should start using new SCCs for new transfers after 27 September 2021.

For existing transfers (i.e. based on old SCCs concluded before 27 September 2021), businesses can still rely on the old SCCs until 27 December 2022, but only on condition that processing operations that are the subject matter of the contract remain unchanged and that reliance on the old SCCs ensures that the transfer of personal data is subject to appropriate safeguards.

Although the18-month transition period for replacing the SCCs for existing transfers with the new version looks long, we highly recommend that you start preparing for this process as soon as possible.

A good starting point is to identify all processes in the company (or group) where data is transferred and all existing agreements in place with third country data recipients.

Does using SCCs suffice?

As stressed by the Court of Justice of the European Union (CJEU) in its judgment in the Schrems II case, companies intending to rely on SCCs (even the new SCCs) when transferring data should ensure that the data subject is granted a level of protection essentially equivalent to that guaranteed by the GDPR. In practice, using SCCs *per se* might not be enough to achieve full GDPR compliance.

To some extent the uncertainty regarding data transfer compliance has been reduced by the recommendations of the European Data Protection Board on measures that supplement transfer tools. The EDPB sets out the following types of supplementary measures:

i. **contractual** (additional clauses in the agreement with the data recipient – supplementing SCCs)

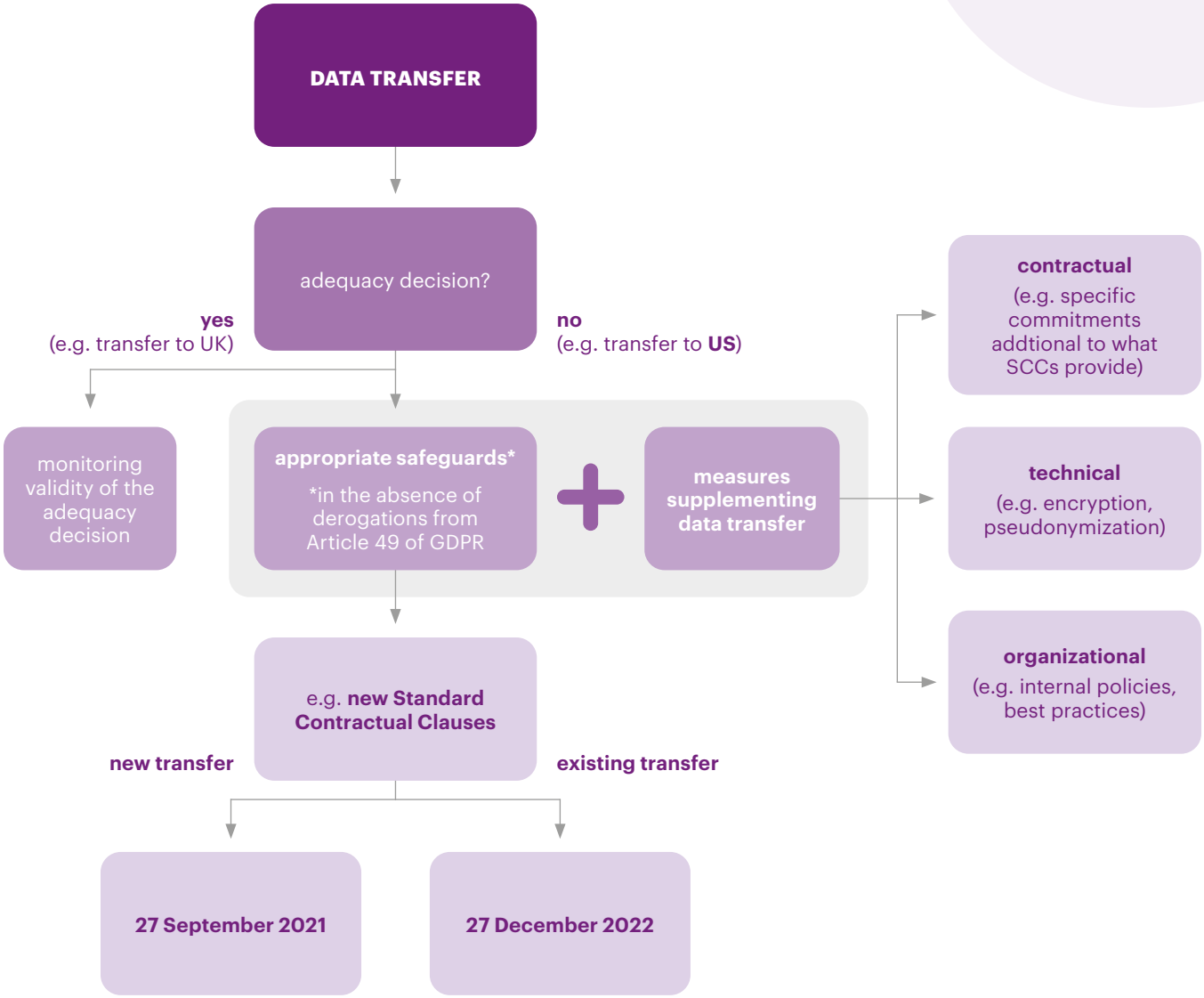
ii. **technical** (e.g. encryption, pseudonimization)

iii. **organizational** (e.g. internal policies, best practices)

To choose appropriate supplementing measures you need to develop a deep understanding of the data flow and adopt a case-by-case approach.

Companies need to be aware that additional measures might be needed even where the data recipient does not access the personal data (i.e. no access does not mean no data transfer). The reason for this is that even if data is transferred in encrypted form, say, it may be exposed to the risk of loss. Thus, even inaccessible data should be properly secured and the risk related to transfer should be mitigated by adequate measures.

Transfer tools in a nutshell



Why is it important to secure transfers?

Personal data is an essential asset in today's technology-driven world. The potential fines for breaching transfer regulations can be severe and the related reputational damage may be immense and irreparable. Failure to secure data transfers may also result in greater risk of loss, theft or unauthorized disclosure, with adverse consequences for data controllers and data subjects alike.

How then to achieve data transfer compliance?

Achieving data transfer compliance requires fitting the transfer tool to the particular data flow. Dentons Warsaw Data Privacy Team is experienced in helping implement tailored data transfer solutions. We provide comprehensive legal support throughout the whole process leading to data transfer compliance. Our methodology is consistent with the recommendations of the EDPB and follows a six-step plan:

i. **Data transfer mapping** – We help clients take stock of their transfers by creating a data inventory of assets and processing activities, and populating the inventory attributes through risk assessments, which enable organizations to identify cross-border data transfers;

ii. **Verification of the transfer tool underpinning the client's transfer** – We help identify cases where transfers should be subject to safeguards laid down in Article 46 of the GDPR;

iii. **Assessment of the law or practice of a third country** – Through close cooperation with Dentons offices around the world our legal support is supplemented with analysis by local counsel. A legal opinion issued by a third-country lawyer might be crucial in evidencing to the data protection authority that the level of protection afforded by the GDPR is not jeopardized by the transfer;

iv. **Identification and adoption of supplementary measures** – Dentons helps clients assess and select the best contractual, technical, and organizational supplementary measures to protect personal data;

v. **Formal procedural steps** – We constantly monitor the EDPB's recommendations and, depending on the transfer, may advise on additional formal steps with respect to the transfer;

vi. **Periodic re-evaluation** – We help organizations re-evaluate personal data transfer mechanisms on a regular basis.

The six-step process outlined above results in a **Transfer Impact Assessment (TIA).** By having a TIA process in place, our clients can demonstrate compliance when they are asked how they are responding to Schrems II. Additionally, if a TIA process is in place and the organization comes under regulatory scrutiny, they can quickly scale the TIA process to all of its processing activities and vendors.

Please reach out to us if you have any questions.

KEY CONTACTS

Karol Laskowski
Partner
+48 22 242 51 27
karol.laskowski@dentons.com

Dariusz Czuchaj
Counsel
+48 22 242 51 54
dariusz.czuchaj@dentons.com

Aleksandra Danielewicz
Senior Associate
+48 22 242 55 23
aleksandra.danielewicz@dentons.com

Anna Szczygieł
Associate
+48 22 242 58 64
anna.szczygiel@dentons.com

Paulina Węgrzynowicz
Associate
+48 22 242 52 52
paulina.wegrzynowicz@dentons.com

CSBrand-66624-A4-Flyer-Data-Transfers_03 — 23/08/2021