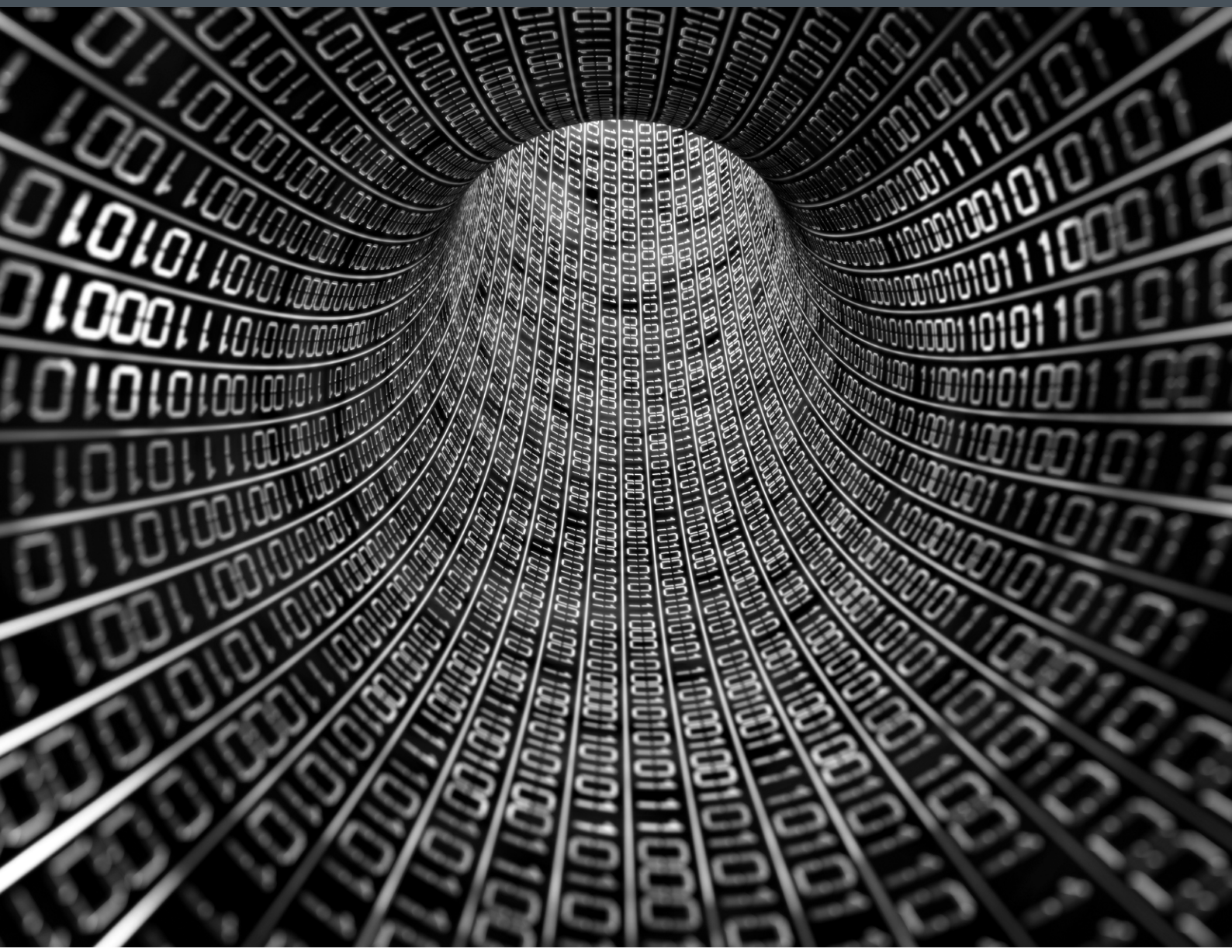

EUROPEAN DATA PROTECTION BOARD PUBLISHES DRAFT GUIDANCE ON TRANSFERS OF PERSONAL DATA OUTSIDE THE EEA

NO ONE SIZE FITS ALL SOLUTION

On 10 November 2020, the European Data Protection Board (EDPB) published its highly anticipated draft Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[1] (the Guidance).

1 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

> **"The Guidance provides organisations transferring personal data with a roadmap of necessary steps they should take to ascertain if they must put in place supplementary measures to transfer data outside the EEA lawfully."**

The Guidance follows the European Court of Justice's (ECJ's) decision in Schrems II, which invalidated the EU-US Privacy Shield, and found that organisations relying on Standard Contractual Clauses (SCCs) could also be required to implement additional safeguards when transferring data outside the EEA. Shortly after publishing the Guidance, the European Commission also released draft updated SCCs which are specifically designed to address Schrems II requirements, and should be read alongside the Guidance by organisations intending to rely on SCCs to transfer data outside the EEA. For more information, please see our briefing on Schrems II[2].

The Guidance

The Guidance provides organisations transferring personal data with a roadmap of necessary steps they should take to ascertain if they must put in place supplementary measures to transfer data outside the EEA lawfully. This is aimed at ensuring that an equivalent level of protection to that guaranteed within the EEA accompanies personal data when it travels to third countries. The step-by-step approach suggested by the EDPB is as follows:

STEP 1: know your transfers

The Guidance requires organisations to ensure that they have full oversight over their transfers to non-EEA countries to fulfil their obligations under the GDPR principle of accountability. It recommends building on records of processing activities to carry out this exercise.

STEP 2: identify applicable data transfer tools

Organisations transferring data outside the EEA must identify applicable data transfer tools in accordance with those the GDPR lists. These tools may include:

Reliance on an adequacy decision

The effect of an adequacy decision is that personal data can generally flow from the EEA to the third country to which the adequacy decision relates without any other GDPR transfer tool (such as an SCC) being necessary. Adequacy decisions may cover all data transfers to a country or be limited to some types of data transfers.

Article 46 GDPR transfer tools

Article 46 GDPR lists a series of transfer tools containing safeguards that organisations may use to transfer personal data outside the EEA in the absence of an adequacy decision. These include SCCs, binding corporate rules, codes of conduct, certification mechanisms and ad hoc contractual clauses. Whichever Article 46 GDPR transfer tool is chosen, it must be ensured that the transferred personal data will have the benefit of essentially the same level of protection as it would have under the GDPR. Therefore, organisations transferring personal data outside of the EEA should not assume that use of one of these tools will, by itself, be sufficient to ensure that the data transfer will comply with the GDPR.

Derogations

Derogations listed in Article 49 GDPR allow for the transfer of personal data outside the EEA in certain exceptional situations. These derogations are interpreted restrictively, and mainly relate to processing activities that are occasional and non-repetitive.

STEP 3: assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer

Where organisations rely on Article 46 GDPR transfer tools, they must ensure that the tool is effective in practice. Therefore, they must assess whether there is anything in the law or practice of the third country that may prevent the Article 46 safeguard being effective. The EDPB recommends that organisations seeking to transfer data outside the EEA ask the data importer to provide information on the laws which apply to it. Other sources should also

2 https://www.hfw.com/International-data-transfers-from-the-EEA-and-UK-Take-care-July-2020

be considered including ECJ case law, resolutions and reports from intergovernmental organisations, national case law and reports from academic institutions. In practice this is likely to mean that organisations will have to seek legal advice to assess the different aspects of the legal system of the third country.

STEP 4: adopt supplementary measures

Where an assessment under step 3 has revealed that the Article 46 transfer tool being used is not effective, organisations must consider implementing supplementary measures in order to bring the level of protection of the transferred data in line with that provided under the GDPR. This assessment should be undertaken on a case-by-case basis depending on the nature of the transfer, how the laws of the destination country operate and the feasibility of the supplementary measures.

A non-exhaustive list of technical, contractual and organisational supplementary measures is provided in the Guidance. Technical safeguards listed include encryption, pseudonymised data and multi-party processing. Contractual safeguards can consist of data importer commitments to transparency, commitments to enable data subject rights and enhanced audits. Finally, organisational safeguards include internal policies for the governance of transfers and putting in place transparency and accountability measures. The Guidance emphasises that it may be necessary for one or more of these measures to be combined in order to be effective, and that supplementary measures which may be effective in some third countries will not be effective in others.

STEP 5: adopt necessary procedural steps

Organisations may have to take additional procedural steps to ensure necessary protections, depending on which transfer mechanism is being used. For example, where an organisation intends to modify the SCCs themselves, or where the supplementary measures added contradict the SCCs, it must seek authorisation from the competent supervisory authority.

STEP 6: re-evaluate at appropriate intervals

The Guidance requires that organisations monitor on an ongoing basis, and where appropriate in collaboration with data importers, developments in the third country that could affect their initial assessment of the level of protection, and the effectiveness of supplementary measures.

Implications

The Guidance offers welcome clarification for organisations seeking to export data from the EEA to third countries. However, it makes it clear that there is no one size fits all solution, that data exporters must carry out their own assessments of the lawfulness and effectiveness of a particular transfer tool in line with the GDPR principle of accountability, and that supplementary measures to those set out in Article 46 GDPR may be necessary.

An important message conveyed by the Guidance is that data transfers from the EEA to the USA are still possible post Schrems II in principle. However, given the potential requirement for supplementary measures such as encrypting and pseudonymising personal data, there will be challenges involved in exporting data from the EEA to the USA. It is likely that both US data importers and EEA data exporters will face heavy burdens in terms of the due diligence, administration and costs involved in assessing the legality of their data transfers.

The Guidance does not at present restrict transfers of personal data from the EEA to the UK. This is because the EU/UK Trade and Co-operation Agreement dated December 2020 provided that the free flow of personal data from the EEA to the UK could continue until adequacy decisions are adopted and for no longer than six months. The UK had previously announced as a transitional measure that transfers of personal data from the UK to the EEA would continue to be permitted following the end of the Brexit transition period. The UK's Information Commissioner's Office is reviewing the Guidance and draft SCCs.

Organisations may also wish to familiarise themselves with the new SCCs as, once approved, subject to a transition period for existing SCCs currently envisaged to be one year, they will need to use these in place of the current SCCs with existing recipients of personal data outside of the EEA, potentially together with supplementary measures.[3]

For further information, please contact:

ANTHONY WOOLICH
Partner
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

JEMIMA MCDONALD
Senior Associate
T +971 2235 4911
E jemima.mcdonald@hfw.com

3 The draft new SCCs are available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our data protection capabilities, please visit hfw.com/Data-Protection.

hfw.com

Americas | Europe | Middle East | Asia Pacific