STEPHENSON HARWOOD

Is it really as simple as six steps to success?

Summarising the EDPB's approach to supplementary measures

On 11 November 2020, the European Data Protection Board ("**EDPB**") issued two long-awaited sets of guidance:

- The first makes recommendations about potential supplementary measures for international transfers (the "**Recommendations**").
- The second is guidance on the European Essential Guarantees for surveillance measures (the "**Guarantees**").

The Recommendations follow the Court of Justice of the European Union's ("**CJEU**") decision in *Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems (Case C-311/18)* ("***Schrems II***"), which found that organizations exporting personal data to importers based outside of the European Economic Area (the "**EEA**") are responsible for verifying that the importer can comply with European law data transfer requirements, taking its domestic law into account.

The CJEU also found that under certain circumstances organisations could still rely on Standard Contractual Clauses ("**SCCs**") to transfer data from the EEA. Fortunately, the European Commission released updated SCCs almost simultaneously with the Recommendations and Guidance. Read our summary of the key changes in the new SCCs and things to watch out for here.

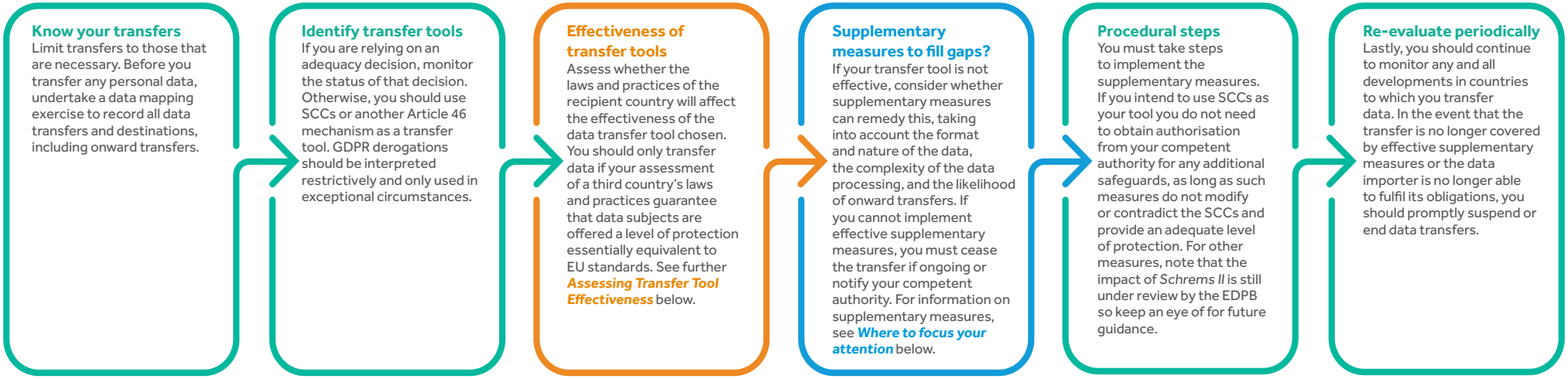
While the guidance is not directly binding, it represents the views of supervisory authorities responsible for enforcing the General Data Protection Regulation ("**GDPR**"). It will therefore be critical for all companies exporting or importing personal data relating to European data subjects to update their procedures and documentation accordingly. This document summarises the key requirements and issues.

The recommended roadmap

The Recommendations set out six steps organisations are expected to take when they transfer personal data outside of the EEA to a third country. These steps are intended to ensure that data subjects are provided with protection that is essentially equivalent to that under the GDPR. Any transfer of personal data to countries that do not benefit from an EU adequacy decision will be subject to immediate change following the publication of these Recommendations and the impact of *Schrems II*.

It follows that companies should consider assessing their current data transfers as soon as possible, by mapping their international personal data transfers and by undertaking transfer impact assessments, following the steps set out in the Recommendations

We set out below the six simple steps proposed by the EDPB in the recommendations and highlight the main action points.



Help or hindrance?

The EDPB expects organisations to undertake the six steps for every transfer. This will require extensive resources and be extremely time consuming. The Recommendations indicate that companies need to understand data flows on a granular level, including not only initial transfers, but also onward transfers (for example, to sub-processors, sub-sub-processors, and so on). With GDPR re-papering exercises only recently completed and the end of the Brexit transition period looming, it seems unlikely that these additional, and somewhat burdensome, expectations will be welcomed by exporters.

Assessing transfer tool effectivess

Survey those surveillance measures

The Guarantees consider how to assess whether third country security and law enforcement surveillance measures can be regarded as a proportionate interference with rights, in accordance with European law.

Under the Guarantees, the assumption is that data subjects are not afforded the same protection as under the GDPR and so an assessment must be carried out in all cases. According to the Guarantees, the four key things that need to be demonstrated for interference to be justifiable are:

- any processing is based on clear, precise and accessible rules
- there is necessity and proportionality with regard to the legitimate objectives of the interference
- an independent oversight mechanism should exist
- effective remedies must be available to the individual.

Two troubling use cases

The Recommendations flag two specific scenarios where the EDPB state that there is **no appropriate supplementary measure** that can sufficiently protect personal data when that data is transferred to third countries. The first of these relates to transfers to cloud service providers or other processors who require access to data in the clear, whilst the second relates to access in the clear (even on a remote basis) to data shared for business purposes. Both of these scenarios refer to data "in the clear", which effectively means unencrypted or in plain text. The first means that using cloud services based in certain third countries (notably the US) could effectively become impossible, whilst the second would severely impede intra-group transfers. It is clear that both of these scenarios will prove frustrating for companies with established transfer procedures.

Subjective vs objective risk

In making an assessment of the third country's legal system, the EDPB recommends that companies should first assess publicly available legislation. If such information is lacking, companies should then assess other relevant factors, such as case law and academic reports. The Recommendations assert that **companies should not rely on subjective factors**, such as the actual likelihood of public authorities' access to data in a manner not in line with EU standards (paragraph 42). However, elsewhere the Recommendations indicate that **subjective factors may be relevant**: for example, organisations may take into account the resources at public authorities' disposal when assessing the third country's legal system, which would appear to involve a risk-based approach. Secondly, the EDPB does not distinguish between subjective and objective factors when considering supplementary measures. For example, the "possibility" of onward transfers may be considered when selecting appropriate supplementary measures *(paragraph 49)* and the suggested organisational safeguards include the adoption of security standards and best practices that take into account the likelihood of a public authority attempting to access data *(paragraph 135)*.

Supplementary measures: where to focus your attention

The Recommendations provide suggestions for certain supplementary measures which are to be used in conjunction with the selected transfer tool to ensure a level of protection '*essentially equivalent*' to that guaranteed under the GDPR. There are three safeguards recommended by the EDPB: technical, contractual and organisational measures. We have summarised some key themes arising out of **all three of these safeguards** to help you streamline your implementation of supplementary measures:

- **Restrict custody of decryption key:** Encryption is a key focus in the potential technical measures recommended by the EDPB. An obvious theme throughout the Recommendations is limiting the custody and control of the decryption key. In fact, the Recommendations go as far as assuming that encryption would only be an effective supplementary measure if the cryptographic keys are retained solely by the data exporter, or other entities entrusted with this task that reside in the EEA. Failing that, the custodian should be an organisation that benefits from an adequacy decision.
- **Understand active and passive attacks:** The Recommendations draw a clear distinction between active and passive attacks by a third country's public authorities and require companies to understand the difference between the two types of attack to ensure technical measures protect against both. An active attack is where a third country public authority accesses the data and manipulates or suppresses it. A passive attach on the other hand would only require a third country public authority to access the data and copy it, such that the data remains unchanged. If your data is susceptible to a passive attack, you could be in breach of the law so it is worth making sure your technical measures are adequate for the type of data being transferred and the mode of processing being undertaken.
- **Consider if you can split data:** The EDPB highlights the option for a data exporter to split data and make use of two or more independent data importers located in different jurisdictions. The only way split data in this way is to make sure that neither importer can identify a data subject from their part of the data received, meaning this work around is restricted to processing that uses multi-party computation and encryption.
- **Ensure clear unobstructed communication channels:** All of the supplementary measures require transparent communication lines that provide for legal notification from importer to exporter. It is key, therefore, to consider how effectively an importer can report data access requests and whether there is any means of secret access by a public authority.
- **Prevent metadata from interpreting personal data:** Exporters also need to consider if any data can be extracted from the encrypted, selective or pseudonymised data which has been transferred outside the EEA. Exporters have to consider, therefore, what can be understood from the data that they choose to transfer.
- **Act quickly:** Lastly, the Recommendations place emphasis on the speed at which notification needs to happen. Think "the sooner the better"!

It is not surprising that these themes are largely related to technical measures. The Recommendations appear to take a view that contractual and organisational measures alone will not be sufficient but does set out that contractual and organisational measures will help in implementing technical measures. The conclusion? It will be important to augment the technical by **layering the safeguards** you use and making sure there is an appropriate mix of technical, contractual and organisation protections.

GET IN TOUCH

Naomi Leach

Partner, data protection

T: +44 20 7809 2960
E: naomi.leach@shlegal.com

Katie Hewson

Associate, data protection

T: +44 20 7809 2374
E: katie.hewson@shlegal.com

Olivia Fraser

Trainee solicitor, data protection

T: +44 20 7809 2844
E: olivia.fraser@shlegal.com

www.shlegal.com

STEPHENSON HARWOOD

© Stephenson Harwood LLP 2020. Any reference to Stephenson Harwood in this document means Stephenson Harwood LLP and/or its affiliated undertakings.
Any reference to a partner is used to refer to a member of Stephenson Harwood LLP.
The fibre used to produce this paper is sourced from sustainable plantation wood and is elemental chlorine free.

BD1118-Is it really as simple-1120