ALLEN & OVERY

EDPB recommendations on third country law assessment and data transfer practices post-Schrems II

New measures offer useful guidance but also leave open questions

On 10 November 2020, the EDPB issued two key documents that describe how organisations can transfer personal data outside the EEA following Schrems II. These are:

1. **The Supplementary Measures Recommendations**: Practical guidance for data exporters (both controllers and processors) on how to comply with the Schrems II decision of the CJEU in assessing the level of protection in third countries combined with supplementary measures where such levels of protection appear to fall short. These recommendations are subject to public consultation, which closed on 21 December 2020.
2. **The EEG recommendations**: an update on the guidance that was issued by the Article 29 Working Party after the CJEU decision in Schrems II to help exporters make the third country law assessment.

The recommendations provide important insight on how organisations should amend their data transfer practices in compliance with the GDPR and Schrems II. The EDPB offers **a six-step procedure** to assess data transfers and provides a number of use case scenarios on how to apply this procedure.

In this report we address all important aspects of these recommendations and give our view on the most significant aspects of the six-step procedure.

Our key takeaways are:

– The EDPB stated in the press release about the Supplementary Measures Recommendations that, despite being subject to consultation, they apply immediately. Although the EDPB appears to take a restrictive approach to interpreting the Schrems II judgment and many practical questions about compliant data transfers remain, we do not expect a complete rewrite of the draft Recommendations following the consultation period.

– The EDPB also announced on 20 November 2020 that it will look into the modernised set of the SCCs and provide a joint opinion with the EDPS. However, the EDPB Chair Andrea Jelinek stated that the SCCs are “not a catch-all solution” for data transfers post-Schrems II but rather “an important piece of the puzzle”, and data exporters must complete the puzzle with the help of the draft Supplementary Measures Recommendations.

– Data transfer assessments that would include the assessment of third country law and practice set out in both the Supplementary Measures Recommendations andthe EEG Recommendations, along with putting in place supplementary measures, will form part of an organisation's accountability obligation. Document your data transfer impact assessments and the supplementary measures identified, ensure ongoing monitoring of third country laws and practice and re-evaluate your transfers on regular basis.

– If effective supplementary measures can be identified and implemented, the international data transfer may go ahead; if not, the data transfer should not start or the existing transfer should be halted. If the data has already been transferred, it must be returned or destroyed by the data importer.

– When transfer is based on the SCCs and supplementary measures do not contradict or undermine the level of data protection provided by the SCCs, no authorisation by the supervisory authority is required.

– The EDPB will issue further guidance on the supplementary measures relating to BCRs and ad hoc contractual clauses.

A number of open questions

While the recommendations provide an insight, it is still unclear how organisations will have to apply these steps in reality. Some typical modern business data transfer methods are currently left without practical solutions. For example when exporters transfers data to cloud service providers or other processors that require access to encrypted data (use case 6) or when EU-based exporter transfer personal data to a group company located in a third country for HR purposes or customer support services (use case 7).
In addition, the Supplementary Measures Recommendations are not aligned with the draft modernised set of European Commission’s standard contractual clauses (SCCs) for transferring personal data to non-EU countries that were issued on 12 November 2020. The EDPB already commented that the Recommendations are still in draft form, the use cases are not exhaustive and offer only some possible examples, and that any inconsistencies will be resolved in the final version.

A six-step roadmap to applying accountability principle to data transfers

The EDPB reiterates that the principle of accountability in the GDPR requires data exporters and importers to actively, effectively and continuously seek to comply with the right to data protection of individuals when transferring their data to third countries, and be able to demonstrate their efforts to do so.

To this end, the EDPB recommends data exporters to follow six steps with respect to each intended transfer of personal data outside the EEA.

Step 1:
map international personal data transfers

Step 2:
identify transfer tools currently relied on

Step 3:
assess the effectiveness of the transfer tools relative to the third country's laws and practice, if effective, personal data may be transferred

Step 4:
if not effective, identify and adopt supplementary measures in relation to the selected transfer tool

Step 5:
take necessary procedural steps for effective supplementary measures depending on the selected transfer tool

Step 6:
re-evaluate the steps regularly

Step 1:
Map in detail all international personal data transfers.

The EDPB highlights that knowing, recoding and mapping all international data transfers of organisations is an essential step to fulfill accountability obligations under the GDPR.

This step should cover data destinations, sub-processor situations and verification that transferred data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to the third country. In relation to cloud services, organisations should assess whether data is transferred to third countries and where.

Step 2:
Identify transfer tools currently relied on with respect to each specific transfer of personal data, which may be:

1. An adequacy decision of the European Commission (**EC**);
2. Standard Contractual Clauses (**SCCs**) adopted by the EC or adopted by a supervisory authority and approved by the EC;
3. Binding Corporate Rules (**BCRs**) approved by competent supervisory authorities;
4. Codes of conduct or certifications mechanisms;
5. Ad-hoc clauses authorised by competent supervisory authorities; and
6. Derogations for specific situations under Art. 49 GDPR.

The EDPB notes that no further steps are required in case of a data transfer to the country covered by an **adequacy decision**. Nevertheless, a data exporter must continuously monitor that the decision is not revoked or invalidated.

Under specific circumstances, occasional and non-repetitive data transfers can also be based on a **derogation** listed in Article 49 GDPR. Similar to the situation with adequacy decisions, transfers based on Article 49 derogations do not require further steps.

The EDPB further importantly notes that the precise impact of Schrems II on transfers under **ad hoc clauses** and **BCRs** is still under discussion of the EDPB.

If transfers cannot be based on an adequacy decision or a derogation, organisations should proceed with Step 3.

Step 3:

Assess the effectiveness of the selected transfer tools in light of all circumstances of transfer relative to the third country's laws and practice.

The Supplementary Measures Recommendations point out that data exporters must assess whether there is anything in the law or practice of the third country that may impact the effectiveness of the selected transfer tool in the context of the specific transfer. The EDPB emphasizes that data exporter must look into the characteristics of each transfer and determine how the domestic legal order of the importer's country (or country of onward transfer) applies to these transfers. In addition, data exporter must verify whether commitments enabling data subjects to exercise their rights, such as rights to access, correct or delete data, can be effectively applied in practice and are not frustrated by the third country law.

The Supplementary Measures Recommendations set out elements that data exporters should include in their assessment, such as all the actors participating in the transfer, including controllers, processors and sub-processors. To that effect, the EDPB highlights the importance of laws that require disclosure of personal data to public authorities or granting such public authorities powers of access to personal data. The EDPB also notices the importance of the right to effective redress of individuals in case of such access to their data.

According to the EDPB, the complexity of the data transfer increases the complexity of the country assessment. The EDPB clarifies that the applicable legal context will depend on the specifics of the transfer, including:

– purpose for which data are transferred and processed, eg HR, marketing, storage, IT support etc.;

– types of entities involved in the processing (public/private; controller/processor);

– sector in which the transfer occurs (eg financial, ad tech or telecom);

– categories of personal data transferred (naming example of children's data that might fall within a scope of special legislation);

– whether the data are stored in the third country or the data are stored in the EEA and merely accessed from abroad;

– data format (eg whether the data are encrypted or pseudonymised), noting that some third countries prohibit import of encrypted data; and

– the possibility of onward transfers from the third country to another third country.

The EDPB recommends basing the assessments primarily on the publicly available legislation. However, if this is not possible (for instance, if such legislation does not exist in a destination country) but the parties intend to proceed with the transfer, other relevant and objective factors can be looked into. Some examples of possible objective sources of information to assess third country and its laws are listed in Annex 3 to the Supplementary Measures Recommendations and include, among others, case law of the CJEU, the European Court of Human Rights or national courts, resolutions of UN bodies or other intergovernmental organisations and reports of civil society organisations.

The EDPB specifically states that exporters should not rely on subjective factors such as the likelihood of public authorities' access to the transferred data in a manner not in line with EU standards. This point of the Supplementary Measures Recommendations seems to contradict the position of the European Commission in the draft modernised SCCs, where the clauses require to take into account any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred.

The assessment should be conducted with due diligence and should be documented. The EDPB states that exporters will be held accountable to decisions taken on this basis.

In addition to the Supplementary Measures Recommendations, the EEG Recommendations help exporters assess whether third countries' surveillance laws meet the European human rights standards. The EEG Recommendations are an important guidance document for organisations making assessments under Step 3 of the Supplementary Measures Recommendations. In addition, the EEG Recommendations are directed at the EC when it intends adopting an adequacy decision in relation to a third country.

In the EEG Recommendations, the EDPB updates earlier guidance on the EEGs to reflect the GDPR and the CJEU case law (including the Schrems II judgment). The EDPB summarised these essential guarantees as follows:

– Processing should be based on clear, precise and accessible rules.

– Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.

– **An independent oversight mechanism should exist**, such as an independent administrative authority or a court.

– Effective remedies need to be available to the individual.

Step 4:
Identify and adopt supplementary measures.

According to the Supplementary Measures Recommendations, data exporters should identify, on a case-by-case basis, which supplementary measures could be effective for a set of transfers to a specific third country when using a specific transfer tool. That means that there are no one-size-fits-all effective supplementary measures.

In principle, supplementary measures may have a contractual, technical or organisational nature. The EDPB states that contractual or organisational measures alone would generally not suffice in situations where only technical measures might halt or render ineffective access to personal data by third country public authorities. In such situations, contractual or organisational measures may supplement technical measures and support the general protection of data.

To help data exporters identifying which supplementary measures would be most effective, the EDPB provides a list of four factors to analyse the personal data:

– Format (ie in plain text/pseudonymised or encrypted);

– Nature (eg sensitive data);

– Complexity (ie number of actors and the relationship between them);

– Possibility of onward transfers within the same third country or to other third countries (eg sub-processor in the data chain).

In Annex 2 to the Supplementary Measures Recommendations, the EDPB provides a non-exhaustive list of possible supplementary measures applied to specific transfer situations. Below are some key examples discussed by the EDPB.

Technical measures:

– **Encryption**, for instance, encryption of **data in-rest** (eg for back-up purposes) applied before transfer and not requiring access in third country (regardless of adequacy status) constitute an effective supplementary measure if it is (1) based on a state-of-the-art encryption algorithm, (2) robust against cryptanalysis, (3) properly implemented and maintained, and (4) if the keys are reliably managed and retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or an adequate third country.

– If data is merely geographically routed through a third country without an adequacy status, **transport encryption providing effective state-of-the-art security**, might qualify as an effective measure if, in addition to the conditions mentioned above, (1) decryption is only possible outside the relevant third country, (2) the parties involved in the communication agree on a trustworthy public-key certification authority (3) specific protective and state-of-the-art measures are used against active and passive attacks on transport-encrypted., or (ii) transport encryption does not provide appropriate security by itself, but is end-tot-end encrypted on the application layer, might qualify as an effective measure if, in addition to the conditions mentioned above: (1 the encryption algorithm is robust against cryptanalysis (2) takes into account when confidentiality of the personal data must be preserved, (3) the existence of backdoors (in hardware or software) has been ruled out, (4) the keys are reliably managed by the exporter or by an entity trusted by the exporter under a jurisdiction offering an essentially equivalent level of protection.

– If data is imported by a **protected data importer** under the relevant third country's laws (eg a duty of professional secrecy, such as doctors or lawyers), **encryption** will constitute as an effective technical measure if (1) the personal data is encrypted before it is transmitted by state-of-the-art encryption, (2) the key is in the sole custody of the data importer and is appropriately secured and (3) the data exporter has reliably established that the encryption key corresponds to the recipients' decryption key, and (4) exemption from government access extends to all information possessed by the protected importer that may be used to circumvent the protection of privileged information.

– **Pseudonymisation** may be an effective measure if (1) the data are first pseudonymised by the exporter before being transferred; (2) the specific data subject cannot be identified, without the use of additional information, (3) that additional information is held exclusively by the data exporter and kept separately in a Member State or in an adequate third country (4) disclosure or unauthorised use of that additional information is prevented by technical and organisational safeguards, and data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and (5) the data exporter has established that pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with information that public authorities in third countries might possess.

– **Split or multi-party processing** by several independent processors may be an effective measure if data exporters (1) prior to transmission, split personal data to be processed by multiple processors in different jurisdictions, (2) after which the personal data can no longer be interpreted or attributed to a specific data subject without the use of additional information; and (3) there is no evidence of collaboration between the public authorities located in the respective jurisdictions where each of the processors are located.

Contractual measures:

– Providing for the contractual obligation to **put specific technical measures in place**.

– **Transparency obligations** imposed on data importer on the access to data by public authorities including (1) which measures are taken to prevent the access to transferred data and information on all requests of access to personal data by public authorities which the data importer has received over a specified period of time, (2) importer certifying that (a) it has not purposefully created back doors, (b) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data and (c) national law or government policy do not require importer to create back doors, facilitate government access to data or systems or hand over encryption key, (3) apply the "Warrant Canary" method, whereby the data importer commits to regularly publish a cryptographically signed message informing the data exporter that as of a certain date and time it has received no order to disclose personal data, or (4) the data exporter could enforce its power to **conduct audits** of the data processing facilities of the data importer to verify if personal data was disclosed to public authorities and under which conditions.

– The data exporter could enforce the data importer to **challenge access orders**, by seeking interim measures to suspend the effects of the order until the court has decided on the merits. The data importer would have the obligation not to disclose the personal data requested until required to do so under the applicable procedural rules or to commit to providing the minimum amount of information permissible.

Organisational measures:

– Adoption of **adequate internal policies with clear allocation of responsibilities** for data transfers. Especially in case of transfers among multinationals, these policies may include the appointment of a specific team, which should be based within the EEA, composed by experts on IT, data protection and privacy laws, to handle requests involving personal data transfers from the EU.

– **Document and record the requests for access received from public authorities** and the response provided, alongside the legal reasoning and the actors involved.

– **Data minimisation** should be considered, such as adoption of strict and granular data access and confidentiality policies based on a strict need-to-know principle. These policies must be regularly audited and enforced through disciplinary measures. In some cases restricted remote access to data can be granted instead of full access or transferring only a limited set of data rather than entire database.

– **Development of best practices** to timely involve and provide access to information about international data transfers to the data protection officer, or legal team.

– **Adoption of strict data security and data privacy policies** based on EU or international certifications, codes of conduct or best practices.

– **Adoption and regular review of internal policies** to assess the suitability of the implemented measures.

We would recommend reviewing Annex 2 to the Supplementary Measures Recommendations in detail to analyse the conditions of the effective supplementary measures mentioned by the EDPB, including cases where the EDPB cannot envision effective technical measures. In such a case, EDPB also recognises that contractual and organisational measures will generally not be sufficient to enable the transfer. In particular, the EDPB stated that it could not envision an effective technical measures in the use-cases 6 and 7 that relate to typical processing scenarios by cloud service providers of unencrypted data or remote access by the data importer for business purposes, such as for HR purposes or outsourced call centers. These use-cases are typical modern business situations that are left unfortunately with no practical solution.

If the transfer tool in combination with the supplementary measure reaches a level of protection that is essentially equivalent to the level of protections guaranteed within the EEA: the transfer may go ahead. If not, the data transfer should be halted. If the data has already been transferred, the data must be returned or destroyed by the importer.

Step 5:

Take procedural steps necessary for the effective supplementary measures you have identified aligned with the selected transfer tool.

The EDPB discusses in detail the procedural steps to implement the supplementary measures in relation to the SCCs, and only briefly touches upon such steps in relation to BCRs and ad hoc contractual clauses.

The EDPB clarifies that when data exporter put in place supplementary measures **in addition to SCCs**, it is not necessary to request an authorisation from the competent supervisory authority as long as the supplementary measures do not contradict the SCCs and do not undermine the level of protection guaranteed by the GDPR.

The data exporter and data importer should ensure that additional contractual clauses do not restrict the rights and obligations stated in the SCCs or lower the level of data protection. The EDPB states that data exporters should be able to demonstrate the unambiguity of all clauses, ie that there is no contradiction with SCCs and that there is sufficient level of data protection. The competent supervisory authorities have the power to review these supplementary clauses where required.

Step 6:

Re-evaluate the steps at appropriate intervals.

The EDPB reiterates that, under the accountability principle of the GDPR, organisations must continuously monitor developments in the third country that could affect organisation's initial assessment of the level of data protection and the decisions taken on data transfers. Where relevant, this continuous evaluation should be done in collaboration with data importers.