POST-SCHREMS II: TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

HAS THE EDPB SUCCEEDED IN CREATING MORE CLARITY FOR BUSINESSES?

Date: 14-1-2021
WHITE PAPER
POST-SCHREMS II: TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Has the EDPB succeeded in creating more clarity for businesses?

Citizens of the European Union (EU) have the right to privacy. To protect this fundamental right, the GDPR provides a wide range of rules and regulations with regard to the processing of personal data. Where personal data are being transferred from the EU to the United States (US), the EU-US Privacy Shield program was supposed to ensure that such data traffic would be handled at an ‘appropriate level of security’. On July 16 2020 however, the Court of Justice of the European Union (CJEU) ruled this arrangement to be inadequate and therefore invalid. Which made it extremely unclear for European businesses to know how to manage their data flows to the US. To resolve the situation, on November 11 2020 the European Data Protection Board (EDPB) issued a set of (draft) guidelines or recommendations for transfers of personal data to third countries. Question is, has this provided the transparency so badly needed?

In this whitepaper, we will first outline the legal framework governing the transfer of personal data to third countries. In doing so, we will explore the situations in which controllers are allowed or not allowed to forward personal data to countries outside the EU. Next, as the issue at hand has been specifically impacted by two CJEU rulings, the so-called Schrems Decisions, we will take a look at the logic of these rulings. Finally, we will discuss the (draft) recommendations issued by the EDPB, followed by our conclusion and some practical advice for organisations acting as controllers in the sense of the GDPR on how to proceed under the current conditions.
1. TRANSFER TO THIRD COUNTRIES

Personal data may not be transferred to parties outside the European Economic Area (EEA) as a matter of course. Countries that are not part of the EEA (which, apart from the EU member states, includes Norway, Iceland and Liechtenstein), are referred to as ‘third countries’. Chapter V of the GDPR lists various exemptions based on which personal data may legitimately be transferred to third countries. What these exemptions have in common is that, in the third countries involved, the level of protection required by the GDPR must not be undermined (Article 44).

1.1 ADEQUACY DECISION (ARTICLE 45 GDPR)

The EU-US Privacy Shield was an adequacy decision in the sense of Article 45 of the GDPR, in other words, a decision made by the European Commission implying that (a territory or sector within) a third country ensures an adequate level of protection. The phrase “ensuring an adequate level of protection” means that the country is committed to guarantee a level of protection that is essentially equivalent to that which is guaranteed in the European Union. With the exclusion of the US, there are now 13 ‘white list’ countries. It is the European Commission’s intention to provide a definitive adequacy assessment for the United Kingdom before the end of 2020, but if this deadline will not be met, the UK will, as of 2021, be considered a third country as well.

1.2 APPROPRIATE SAFEGUARDS (ARTICLE 46 GDPR)

In the absence of an adequacy decision, the insufficient level of protection offered by a third country may be remedied by ‘appropriate safeguards’ as specified in Article 46 of the GDPR. One example of such appropriate safeguards are the Standard Contractual Clauses (SCCs) mentioned in Art. 46(2)(c), which are provisions included in standard contracts drawn up by the European Commission to which a party within the EU and a party in a third country may jointly commit.

There are three sets of standard contracts adopted by the European Commission: two for the transfer of data from one controller to another controller and one for the transfer of data from a controller to a processor. All three of these actually originate from the days of the GDPR’s predecessor, Directive 95/46. On November 12 2020, the European Commission opened a consultation on two new standard contracts, which are closer aligned with the GDPR and more fitting for the complex processing operations of the present day. These new contracts, when approved, will replace the existing SCCs.

Another example of appropriate safeguards are Binding Corporate Rules (BCRs), as mentioned in Art. 46(2)(b). These BCRs have to be part of a legally binding privacy policy associated with an international organisation or a multinational business with establishments outside of the EU. BCRs have to be approved in advance by the competent supervisory authority, the procedure for such approval being specified in Article 47 of the GDPR. Also qualifying as appropriate safeguards under condition of approval by the relevant supervisory authority are codes of conduct (Art. 46(2)(e). These codes of conduct, once approved according to the requirements specified in Article 40 of the GDPR, then apply to all affiliated controllers or processors carrying out the same sorts of processing operations or operating in a specific sector of industry, such as, in The Netherlands, the NLDigital trade association, whose Data Pro Code is the first code of conduct to have been approved by the Dutch Data Protection Authority.

1.3 DEROGATIONS (ARTICLE 49 GDPR)

For situations where none of the options mentioned above are available, the GDPR lists a number of specific conditions on which transfers of personal data to third countries are still allowed. This list however, requires strict interpretation. One of the conditions specified, in Art. 49(1)(b), is necessity for the performance of a contract, as in the case of a travel agency having to transfer personal data for the purpose of booking accommodations in a third country.
2. THE SCHREMS DECISIONS

2.1 SCHREMS I

Transferring personal data to third countries has become significantly more complicated as a result of the legal proceedings initiated by Maximillian Schrems, a citizen of Austria who was still in law school when he decided to go to court following revelations by whistleblower Edward Snowden to the effect that American and other intelligence services had gained large-scale access to personal data for the purpose of espionage. Based on this information, he sued for a ban on the transfer of personal to the US by Facebook. In the end, ruling on Schrems’ complaint from 2015, the CJEU decided to invalidate the Safe Harbor program, Privacy Shield’s predecessor, on the grounds that it failed to provide appropriate protection of privacy, i.e. at a level equivalent to that ensured within the EU. This decision is now commonly referred to as the Schrems I Decision or simply Schrems I.

Consequently, in 2016, the European Commission approved the Privacy Shield program, thus making it, once again, legitimate for participating American businesses to process, within the US, personal data related to European citizens. Among other things, it was judged that the demands made on American organisations had significantly been intensified with the introduction of Privacy Shield and that clear safeguards and transparent restrictions were now in place concerning access to such data by US government institutions.

2.2 SCHREMS II

Meanwhile, after a new case filed by Schrems, the CJEU has invalidated the Privacy Shield system as well, ruling in the Schrems II Decision that it too offers insufficient protection of privacy because, based on US legislation, in the context of certain surveillance programs, intelligence and security services retain the right to view data related to EU citizens and use those data as they see fit, without limitations of any kind.

The fact that EU citizens have the option of lodging complaints they may have about US-based processing of their personal data with a so-called ombudsman, is not considered to resolve the issue as there are no assurances as to the impartiality of the office, which, moreover, does not have the authority to make binding decisions.

In contrast, the CJEU did confirm the validity of SCCs, while emphasising that where the related standard contracts are applied, the controller must still ensure an appropriate level of protection, taking into account the agreed upon contractual provisions, possible access to transferred personal data on the part of government institutions and all relevant elements of the legal system adopted by the third country in question (specifically the elements mentioned in Art. 45(2) of the GDPR – of which there are quite a few).

In view of the above, it is fair to say that for the controller to ensure an appropriate level of privacy protection is by no means an easy task. After all, how is a controller to guarantee that there will be no peeking over the processor’s shoulder by government agencies? According to the CJEU, the advisable course of action is to assess the feasibility of supplementary safety measures on a case-by-case basis. Unfortunately, the CJEU ruling fails to specify the nature of such measures.
3. THE EDPB’S (DRAFT) RECOMMENDATIONS

For some time after the Schrems II Decision, a good deal of ambiguity remained as to the practical consequences of the ruling and the possible follow-up action to be taken next. Finally, on November 11 2020, the EDPB issued its Recommendations for the transfer of personal data to third countries, including a roadmap for ‘exporters’ of personal data. Below, in summary, are the steps outlined in this roadmap.

3.1 STEP 1: KNOW YOUR TRANSFERS

The first thing a data exporter obviously needs to know, is to what country the data are being transferred. Recording and mapping all transfers can be a complex exercise, especially where multiple transfers to a variety of processors in different third countries are involved, but it is nevertheless essential to fulfil the obligations under the principle of accountability. Also, the exporter must verify that the data being transferred are adequate, relevant for and limited to what is necessary in relation to the purposes for which they are transferred to and processed in the third country.

3.2 STEP 2: IDENTIFICATION OF TRANSFER TOOLS

As mentioned above in section 1.2, Chapter V of the GDPR lists a number of tools – or mechanisms – justifying the international transfer of personal data. Here, the EDPB advises to identify the tools a particular transfer is relying on. If an adequacy decision is in place or if one of the derogations from Article 49 applies, the transfer is clearly legitimate. If the transfer relies on some other appropriate safeguard in the sense of Article 46 of the GDPR, the exporter is to continue with step 3.

3.3 STEP 3: SAFEGUARD EFFECTIVENESS

The third step is about assessing, on a case-by-case basis, whether there is anything in the legislation or practices of the third country in question which may impinge on the effectiveness of the appropriate safeguard in the sense of Article 46 of the GDPR. Phrased differently, this step implies that the appropriate safeguard the transfer relies on, must be actually effective in practice. A standard contract entered upon with a party in the US can, after all, prove to be less than practically effective if it turns out that US authorities have unrestricted access to the personal data involved.

According to the EDPB, it is up to the ‘importer’ to point the ‘exporter’ to relevant sources of information for making the necessary assessment. Additional sources mentioned by the EDPB include CJEU jurisprudence and case law history in the third country. The EDPB also refers, as did the CJEU in the Schrems II case, to legislation adopted in the third country and the criteria listed in Art. 45(2) of the GDPR. Finally, in this step, the EDPB also refers to the European Essential Guarantees recommendations, which serve as guidelines in assessing whether or not there is the likelihood of interference by the third country’s authorities.

In describing this step, the EDPB emphasises the importance of thoroughly documenting and carefully carrying out the entire process of assessment, as the controller will be held accountable for decisions based on the results.
3.4 STEP 4: SUPPLEMENTARY MEASURES

Step 4 is about adopting supplementary measures if there is the likelihood of impingement on the effectiveness of the appropriate safeguard. The EDPB urges exporters of data to identify, on a case-by-case basis, which supplementary measures, if the effectiveness of the applicable appropriate safeguard is deemed to be in doubt, could be implemented as a remedy. There are various factors to be considered in this deliberation, such as the nature and format of the personal data to be transferred, the length and complexity of the data processing workflow and the parties involved in the processing.

As mentioned above, the CJEU in its Schrems II Decision failed to specify the nature of possible supplementary measures. Meanwhile, this gap has been filled by the EDPB, which, in its Recommendations, has included a non-exhaustive list of technical, contractual and organisational supplementary measures. In various sample scenarios, the EDPB illustrates the effectiveness of different types of supplementary measures under different types of conditions. In one such scenario it is argued that only supplementary measures of a technical nature can prevent government institutions from gaining access to personal data from the EU, examples of such technical measures being solid encryption and pseudonymisation of data to be transferred. Under the proper conditions, according to the EDPB, split or multi-party processing may qualify as well, the idea being that the actual tasks of processing are being assigned to two different processors, neither of whom having knowledge of the data to be processed by the other party nor being able to trace back the data to the data subject(s).

Apart from the regular contractual measures which often have to be taken anyway in case of the applicability of an appropriate safeguard in the sense of Article 46 of the GDPR, the EDPB mentions a number of supplementary contractual measures, such as concluding sound agreements on the use of specific technical measures, transparency requirements and the obligation to dispute requests for access from a third country’s authorities, the latter of which Microsoft, for instance, has already committed to.

Finally, on the subject of organisational measures, the EDPB mentions the example of internal policies with unambiguous allocation of responsibilities.

In describing this step, the EDPB once again emphasises the controller’s responsibility for the selection of (a combination of) measures to be taken and the importance of properly documenting the choices made. Where no supplementary measures are found to provide sufficient assurance, transfer of data must be avoided, suspended or terminated.

3.5 STEP 5: FORMAL OR PROCEDURAL STEPS

Step 5 focusses on the formal / procedural steps that need to be taken to allow for implementation of supplementary measures. In this step, the EDPB explains, for each individual appropriate safeguard in the sense of Article 46 of the GDPR, which preliminary steps have to be taken – or need not to be taken - if the choice is made for implementation of supplementary measures. If, for instance, supplementary measures are being considered in addition to application of a standard contract, there is no need to contact the Data Protection Authority as long as the supplementary measures are not, directly or indirectly, in conflict with the provisions of the standard contract.

3.6 STEP 6: REGULAR RE-EVALUATION

The final step implies regular re-evaluation of data transfers to third countries and monitoring of local developments that could affect the initial assessment of the level of protection offered by the third country in question.
4. CONCLUSION

Have the EDPB’s (draft) recommendations provided the clarity European business so badly needed? The mere fact that the reaction period was extended to December 21 2020 instead of the original November 30 deadline, is in itself an indication of the negative answer to this question.

Specifically, carrying out steps one, three and four of the EDPB roadmap presupposes such in-depth legal familiarity with the complex judicial systems existing throughout the EU and in the relevant third countries as to raise serious doubts about the ability of average European organisations to reliably make the assessments required of them. Presumably, most businesses simply will not have the resources nor the expertise needed to correctly evaluate individual cases of international data transfer and implement the appropriate additional measures where needed.

5. ADVICE

Negotiations are currently being conducted to reach agreement on a new adequacy decision regarding exchange of personal data between the European Union and the United States, but this may still be a long time coming. Meanwhile, in the interest of global economy, it is obviously essential that there is the option of transferring personal data, if only because many businesses, large and small, use American ICT applications like email and videoconferencing on a daily basis.

The most obvious solution for continued transfer of personal data, based on the above, is to use existing SCCs. Research conducted by DigitalEurope shows that this is exactly what 85% of the organisations surveyed is already doing. And with expected new and improved SCCs on the horizon, this is certainly a feasible workaround. Do note however, that where the SCCs are not being literally adhered to or where supplementary measures are being implemented that are, directly or indirectly, in conflict with these SCCs, approval must be obtained from the Data Protection Authority.

We are very interested in learning what the EDPB will come up with by way of final recommendations and what the European Commission’s definitive SCCs will look like. If in the meantime you have any questions, please feel free to contact The Privacy Factory.
ABOUT THE PRIVACY FACTORY

The Privacy Factory is a dedicated data protection software and service provider for compliance with the GDPR and other sectoral laws and regulations. More than 600 customers have called upon The Privacy Factory to assist them in becoming compliant using the Privacy Manager software and services.

The Privacy Manager platform is based on a set of well-researched GDPR libraries. By answering just eight questions Privacy Manager’s record of processings and the privacy activity planning will be automatically pre-filled. The result is a privacy management platform ready for demonstrating GDPR compliance to regulators and auditors at any time.

Our GDPR libraries are enriched with content generated during 20,000 + research and development hours spent by our world-class team of certified privacy and software experts.

The Privacy Factory is headquartered in Maastricht, The Netherlands. To learn more, visit theprivacyfactory.com

DISCLAIMER

No part of this document may be reproduced in any form without the written permission of the copyright owner.

All our publications are provided as general guidance. Users of this document should consult their own legal advisers for legal advice specific to their own circumstances and The Privacy Factory accepts no liability of any sort arising from the use of this document.

Copyright © 2021 The Privacy Factory
All rights reserved.