EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

Comments on the

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

European Federation of Data Protection Officers

December 2020

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

The European Federation of Data Protection Officers (EFDPO) welcomes the recently adopted Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data issued by the EDPB ("Recommendations") and appreciates the opportunity to provide feedback to the ongoing discussion providing comments on them. Although the EFDPO considers the Recommendations being a step towards the right direction, we would like to stress the following points and open questions:

For any DPO the topic of international data transfers remains a challenge, because clear guidance on it is hard to find. The situation has got even more complicated since the Schrems II decision of the CJEU, which invalidated the Privacy Shield as a valid data transfer mechanism in July 2020, and upheld the validity of the standard contractual clauses subject to the implementation of "supplementary measures" (where necessary) in order to ensure compliance with obligations under European privacy law, particularly with respect to access requests from public authorities.

It is worth recalling that the Schrems II decision as well as the draft Recommendation are issued in a reality where numerous data transfers continuously already take place, and to terminate or suspend those is not a matter of singular „management decision", but a complex project. Some EU businesses are relying on such transfers, and to change the suppliers again presents a complex set of steps to be taken. The EU companies rely on the state-of-the-art technology provided by the US enterprises, which is in question since then.

Consistent with our previous position to Schrems II, the situation for the DPO is very difficult, because it is almost impossible to provide controllers and processors with appropriate legal advice which at the same time can be practically viable for the companies. Given this situation, we, as professional association of DPOs, had hoped for some clarification and more precise guidance in the Recommendations. Yet, the Recommendations address the specific questions in a rather general way. They do not focus on specific, practical problems that need to be solved. Furthermore, the addressees are limited to the ones that usually do not have the power to change the state of affairs.

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

Clear and realistic guidance on EU-US data transfers is desperately needed

The requirements deriving from the Recommendations are directed to the controllers (and therefore the DPOs that consult them) are almost impossible to fulfil. The reason for that has to do with the fact that the core business involves many everyday processing activities, whereas the Recommendations have a more theoretical character (their starting point are the legal requirements from Chapter 5 of the GDPR in consistence with the new requirements stated by the CJEU decision). As a result of their broad and generalised perspective, they contribute to a well elaborated theoretical knowledge and serve as a very good basis for the understanding of the issues involved, but they do not give the required specific answers to questions of practical importance for so many European controllers and processors. Inevitably, we all need to know how the EU-US data transfers need to be dealt with. It should be emphasized here that a number of processing operations based on the transfer of data to third countries are similar and could therefore be assessed in greater detail than indicated in the Annex to the Recommendations. From this point of view, relations with the US seem to be the most critical, not only with regard to US legislation, but also with regard to the enormous importance of ongoing trade between the EU and the US.

In fact, the Schrems II decision names clearly and specifically that the relevant US legislation has to be considered. It would be useful to know through the Recommendations which of the mentioned options are appropriate for each kind of standard data transfer in the light of the given legislation. A list is presented in the document, but there is no clear guidance on evaluating and documenting the appropriateness. The practical perspective of the problematic situations companies and their DPOs are facing is clearly missing: we believe that this issue is bound especially to the question of EU-US data transfers by using international IT and cloud services. These services are the most common services used by European companies.

We would welcome even more practical examples on a more specific level. For example, the requirement to analyse the “law and practice” of the third country can be found in the Recommendations. Even knowing that the CJEU explicitly addresses the FISA legislation of the USA, it is not possible to make final decisions regarding the data

transfers, only by following the Recommendations. There are open questions regarding the law and its practical application including the possible access that realistically need to be considered in this case and the computing capabilities that are available to US Intelligence Agencies. No SME or DPO could be possibly asked to do the required research to be able to answer these questions and there are even more inaccessible fields of legislation or information that can be thought of. As a result, the above-mentioned requirement regarding the description of law and practice of the third country can prove to be extremely difficult or even impossible to fulfil.

The EFDPO acknowledges that the EDPB made a good starting point by providing a generalised process of evaluation. However its practical relevance and use would be greatly enhanced though by addressing specific questions regarding important groups of cases that are part of everyday business, especially of the medium or even the small size companies. These could either cover some generalized processing activities, or the particular major partners (importers) for data transfers (we believe that the most used international services need to be considered directly). Almost every company in the EU needs clear answers regarding EU-US data transfers, given the US legislation, named in the CJEU decision, answers that cannot be found in the Recommendations adopted. It should be emphasized that many controllers, especially from small and medium-sized enterprises, are simply not able to support the performance and further review of the detailed foreign law scrutiny (including local „practices“) required by the EDPB as a next step (in practice, such an assessment is very demanding even for larger controllers).

Clearly (also) address the Processors (Importers)

The Recommendations are addressing the controllers in the EU as exporters. However, many relevant provisions of GDPR are not only directed to controllers but also to the processors (the processors are very often at the same time the importers of data). Art. 44 GDPR addresses the processors directly, therefore they should also be addressed by the Recommendations. This would also reflect the intended changed relationships between controllers and processors in the transition from the guideline 95/46 to the GDPR. Processors are no longer meant to form only an assisting entity but a powerful part of the processing procedure, making their own decisions, especially

when it comes to technical and organisational safeguards. In many cases the data transfers to be considered are not necessary as part of the processing itself but a business decision of the company involved as processors. Addressing processors (importers) would also be more appropriate because these companies will need to evaluate the legislation of their country of origin (which of course would be much more easy for them than for the controllers). The current draft for the standard contractual clauses, and some of the contractual measures of the Recommendations also take the same direction. For the DPO the elaboration on the responsibilities and closer regulation of obligations of the processor is of high importance, since this could result in direct obligations imposed on them. It should be made clear that processors (especially the major IT-Companies) are obliged to provide the controllers with relevant information, including the necessary description of legislation and its practical enforcement, so that they can make the final decisions for their companies. It would help the DPOs to properly fulfil the tasks set for them in GDPR.

Relevance of Commissions' decisions

Finally, the GDPR mentions that the EU Commission is supposed to make decisions on behalf of all actors of the whole EU market. These include the decisions about Standard Contractual Clauses (Art. 46 II b GDPR) and Adequacy Decisions (Art. 45 I GDPR). These decisions could and should include and consider political perspectives (within the boundaries of European law). However, such an opportunity to take account of political perspectives is not available for controllers and their DPOs, although this sometimes seems the only possible solution to deadlock situations like the one companies are facing with the issue addressed here. Therefore, the process should also take a viable stance to the relation between EU Commissions' decisions and companies relying with their business practices on the stability of these decisions. Due to the recent CJEU decision, which instantly changed the rules laid out before, it is not clear from the recommendations adopted to which extent companies can rely on the decisions in the future. It should be made clear that companies may not be penalised for inappropriate decisions made by the Commission.

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

EFDPO contacts:

EFDPO Press Office, phone +49 30 20 62 14 41, email: office@efdpo.eu,
President: Thomas Spaeing (Germany)
Vice Presidents: Xavier Leclerc (France), Judith Leschanz (Austria), Inês Oliveira (Portugal), Vladan Rámiš (Czech Republic)

About EFDPO

The European Federation of Data Protection Officers (EFDPO) is the European umbrella association of data protection and privacy officers. Its objectives are to create a European network of national associations to exchange information, experience and methods, to establish a continuous dialogue with the political sphere, business representatives and civil society to ensure a flow of information from the European to the national level and to proactively monitor, evaluate and shape the implementation of the GDPR and other European privacy legal acts. In doing so, the EFDPO aims to strengthen data protection as a competitive and locational advantage for Europe. The new association is based in Brussels.

Founding members:

- Austria: Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter privacyofficers.at
- Czech Republic: Spolek pro ochranu osobních údajů
- France: UDPO, Union des Data Protection Officer - DPO
- Germany: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
- Greece: Hellenic Association for Data Protection and Privacy (HADPP)
- Liechtenstein: dsv.li-Datenschutzverein in Liechtenstein
- Portugal: APDPO PORTUGAL Associação dos Profissionais de Proteção e de Segurança de Dados
- Slovakia: Spolok na ochranu osobných údajov