Spolek pro ochranu osobních údajů

Comments on the EDPB's draft "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"

We welcome the opportunity to present our comments to the recently published EDPB draft Recommendations on measures that supplement transfer tools.

General comments

As a general comment we understand that the Recommendations 01/2020 can´t but reflect the argumentation contained in the Schrems II decision of the CJEU. In this the draft Recommendation comments in more detail on how to comply with the conclusions of the decision whilst transferring data outside EEA.

To this end we believe the freedom of the EDPB in drawing conclusions and recommendations is rather limited (even if in some cases we might perceive the EDPB recommendations overly strict).

Also, we would like to emphasize the fact that the Schrems II decision does not provide any transition period for the implementation of its conclusions has unfairly put data controllers and processors into a non-compliant situation without actually causing such a situation. All these had been acting in a good faith in compliance with existing rules and regulations and suddenly they all became non-compliant with those. In this connection we would like to emphasise that from our point of view it is always important to consider whether it is appropriate to issue judgments setting out "with immediate effect" obligations which, in principle, cannot in the short term effectively be complied with by the addressees. We believe that considering the deferred effectiveness of the judgment would have been an appropriate solution to make ensuring compliance realistic.

We find it is also important to point out that the Schrems II decision requirements seem to be so strict that their full implementation in practice will be extremely demanding in terms of time and resources not only for implementation but also for the required regular reviews required under the "active compliance" concept presented in point 3. of the draft Recommendation.

As follows from above, DPOs will find themselves in a very difficult situation when providing the right advice to controllers and processors. The requirements will bring a number of difficult dilemmas for both the DPO and the controller and processors themselves. If controllers are to fully comply with the requirements of the Recommendation, this will entail very high costs both for documenting compliance and for assessing the legal situation in third countries. A similar cost would apply to the requirement to assess "practice and precedents in the third country" (points 30 and 43 of the draft Recommendation) in a country of import. Here the question is what effort will be considered proportionate, in reaching full compliance with the Recommendation. This question will become very relevant for all players as in the event of a

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat at the address Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

wrong/insufficient assessment, the exporter may be subject to a fine of up to EUR 20 million and private enforcement actions by the affected data subjects.

It is worth recalling that the Schrems II decision as well as the draft Recommendation are issued in reality where numerous data transfers have already take place, and to terminate or suspend those is not a matter of a simple „management decision", but a complex project. Many EU businesses are relying on such transfers, and to change the suppliers again presents a complex set of steps to be taken.

We acknowledge the idea of the "digital sovereignty of the EU" supported by the EU authorities, however so far, no real alternative to replace big global players with EU ones has been created. For this reason, many EU businesses still use services hosting data outside the EU. In many cases the negotiating power of the small and medium EU businesses (often even the big ones) is not strong enough to negotiate specific conditions with their suppliers. In this context we would strongly support the regulation to focus more on the obligations of importers in the field of compliance with the Schrems II decision. Moreover, this is also supported by the increased extraterritoriality of the GDPR within the meaning of Article 3. Although, of course, there would be a partial overlap with competition law, we believe that there is in fact nothing to prevent EDPB from imposing such requirements on importers.

Unfortunately, if the above is not taken into account, we must state that in our opinion, in practice, it is very challenging in normal business practice to ensure 100% compliance with the requirements set by the EDPB and the CJEU when exporting personal data. From this point of view, it would probably be simpler and fairer for the competent EU authorities to declare that in many cases data cannot be realistically transferred to selected third countries (eg the US) except for the use of Article 49 GDPR instruments. The solution could then be for example to order by legally binding instrument for foreign companies providing services to EU entities to domicile data in the EU/EEA (being aware, of course, of all the implications that such a declaration would have for Euro-Atlantic relations and trade, not mentioning other already discussed implications in specific areas, such as medical research).

From the view of the practical application of the rules set by the EDPB, it would help controllers and processors, and especially individual DPOs, to assess the measures chosen by the controller or processor, if the evaluation of legislation and practice in a third country was undertaken by the EDPB or another EU body. 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 (in practice, such an assessment is very demanding even on the side of larger controllers).

An alternative solution could be that the EDPB in its Recommendations would impose such an obligation directly on importers who offer their services in the EU for several controllers (again for basic type processing). Such an instruction issued by EDPB could be based on the co-operation obligation of the processor under Article 28 (3) (f) GDPR and Article 32 GDPR. A breach of this obligation or the provision of incorrect data could then be primarily to the detriment of the processors directly concerned. For the time being the primary responsibility still lies with the data exporter.

At the same time, we consider it appropriate for the EDPB to indicate by when individual importers/exporters should meet the requirements of the Recommendations. Fulfilling such complex requirements and possibly changing the systems used requires sufficient time. From the point of view of individual DPOs operating at exporters, such a time perspective would allow them to provide specific recommendations regarding the individual steps that will need to be taken to the relevant controller or processor. This is all the more important as the different supervisory authorities differ significantly in their approach to enforcing the Schrems II judgment.

In general we would recommend to amend the draft Recommendation in the following way:

1. **To emphasize the role and responsibilities of importers who offer systems based on the transfer of data to third countries, especially where processors offer standardised tools for multiple controllers.**
2. **To declare a clear obligation of data importers within the framework of cooperation pursuant to Article 28 (3) (f) GDPR to provide controllers with an assessment of the legal situation in the country to which the data are transferred and to declare the responsibility of such importers for its correctness.**
3. **To recommend to the relevant EU institutions to issue model assessments according to point 2 for countries that are significant trading partners of the EU so that individual controllers or processors in the EU can follow such a recommendation and do not have to perform other costly assessments of their own in standard model cases.**
4. **To define a timeframe within which the obligations under the Recommendations should be fully met.**

Specific comments

Section 2.1: The idea of knowing your transfers is in general difficult to oppose. However, it is a concept requiring a detailed map of all data transfers performed. All privacy experts would confirm how challenging such an exercise would be. Especially considering the requirement to also cover onward transfers (point 10 of the draft Recommendation). To set out such a complex obligation without providing a proportionate time limit is clearly unrealistic.

Point 30: We have serious doubts regarding how an accurate assessment of the law and practice in the country of import the data exporter is capable of performing, even if supported by the importing entity (here the point only mentions the support as regards the „laws“, not „practice“).

Point 33: We believe that there are a number of other similarly important aspects that can be taken into account, such as the data subject's own active use of the service offered by a non-EU controller, the retention period of the non-EU data, the credibility of a non-EU processor, level of democracy exerted in the country, etc.

Point 42: The draft recommendation requires assessment to be performed with regards to the legislation publicly available. However, in countries where the public legislation is lacking, the assessment should be based on „other relevant and objective factors...“. The question here is, how realisticly can the exporter efficiently perform such an assessment.

Furthermore we believe that when assessing the compatibility of the level of data protection, it is also possible to take into account subjective factors, such as "likelihood of public authorities' access to ... data in a way not in line with EU standards", especially in countries that have democratic nature and are based on the principle of the rule of law.

Point 84: We would welcome an explanation of the extent to which the controller should verify compliance with the requirement: "a data exporter transfers personal data to a data importer in a jurisdiction ensuring adequate protection, the data is transported over the internet, and the data may be geographically routed through a third country not providing an essentially equivalent level of protection“. In practice, controllers usually do not have information on where data is "flowing" within the internet. At the same time, we point out that the requirement that "the existence of backdoors (in hardware or software) has been ruled out" may be in direct

conflict with recent efforts by Member States to incorporate such backdoors into communication systems.

Point 88: Use case 6 doesn't take into consideration any additional measures, such as usage of HSM on controller's premise (and having data in clear format in memory for processing only, but encrypted in general), processes like Customer's Lockbox or similar tools.

We are grateful for the opportunity to provide our comments on the draft Recommendation.

Prague, 20 December 2020

JUDr. Vladan Rámiš, Ph.D.
Chairman of the Committee
Spolek pro ochranu osobních údajů

Mgr. Alice Selby, LLM
Member of the Committee
Spolek pro ochranu osobních údajů