DORDA

European Data Protection Board
Rue Wiertz 60
1047 Brussels
BELGIUM

Public consultation reference:
R01/2020

Vienna, 30 November 2020

Via: Online form

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

Dear Madam or Sir,

We, DORDA Rechtsanwälte GmbH, are gladly taking the opportunity to comment in the public consultation phase on the draft of the Recommendations 01/2020 on measures that shall supplement transfer tools to ensure compliance with the EU level of protection of personal data ("Recommendations").

A. PRELIMINARY REMARKS

First of all, we welcome the approach taken by the EDPB to issue Recommendations on the data transfer to third countries. The concerns of the CJEU in the "*Schrems II*" decision in July 2020 lead to a high level of uncertainty in practice as to how to deal with existing as well as envisaged EU-US data transfers. Due to the stellar position of US providers and technology there is an extreme need and urgency for a secure and safe data transfer to the US. In particular, many services from US providers cannot be equally replaced by services offered within the EU and are therefore indispensable. Furthermore, already existing data transfers as part of outsourcing and cloud computing projects have initially been based on (i) EU Standard Contractual Clauses ("SCC") and/or (ii) EU Commission's adequacy decision on Safe Harbor / Privacy Shield. Due to the recent CJEU ruling all those data transfers are at risk of being illegal. There is in addition high pressure from data protection associations to efficiently enforce the CJEU rulings. This leads to business, but also governmental associations located in EU being in a deadlock: They cannot replace US provider and respective data transfers but are not offered realistic and reliable measures to overcome the legal restraints resulting from the CJEU ruling. Thus, a reliable legal procedure enabling EU data controllers to further use established and reliable international IT providers by ensuring reasonably high level of data protection is required.

Further, we appreciate the step-by-step structure of the Recommendations: This allows users to rely on practical instructions and to systematically implement the Recommendations into its own environment. However, some aspects of the Recommendations do not cover already established market standard in the EU and are, at least in parts, exaggerated: The intended shifting of the obligation to evaluate the legal situation in the respective third country to the data exporters although (i) an adequacy decision is in place and/or (ii) approved SCC have been concluded, does not create legal security. Moreover, it weakens the effect of the transfer tools provided by the GDPR – in particular the SCC – and thus undermines its purpose. Since supervisory authorities, courts, inhouse councils and lawyers frequently use EDPB's guidelines as a valid source for interpretation of the GDPR, it is of upmost importance that the Recommendations do not only provide legal guidance, but also reflect the established market standard, international practice and business needs of both, European data controllers and the leading IT providers from abroad.

B. COMMENTS

1. Transfer mapping and tools

We endorse the approach of the Recommendations that data controllers shall create an overview of its data transfers as a first step. Apart from the fact that the data transfers must be displayed in the records of processing activities, a transfer mapping helps to provide additional transparency for both, the responsible data controller and the data subject. Thus, it is a reasonable starting point to identify if and what next steps are required.

Although the suggested mapping may help to determine the required transfer tool, the most relevant tool in absence of an adequacy decision is the conclusion of SCC: Using already approved clauses (i) gives the data controller security that the privacy standards required by the GDPR are met and (ii) limits lengthy and cumbersome contract negotiations with IT providers on individual level. Any other tools (i) have to pass a time-intensive examination process before they can be validly applied, (ii) usually cover specific data processing activities, only, and (iii) create legal uncertainty as regards to the sufficiency of the guarantee used. This does not match with the fast-moving and continuously progressing IT-field. Decisions on implementing relevant tools, software or other services are frequently time-critical, which is not only a result of business needs, but even more deriving directly out of the GDPR: Adequate technical and organisational measures need to be in line with the established state of the art according to Art 32 GDPR – thus, time efficient decisions are required.

Since the CJEU has also not declared the SCC as insufficient per se, the focus shall be on strengthening the safeguards implemented by the SCC in order to allow European entities to solely rely on this tool for international transfer of personal data, providing for the required legal certainty of being compliant with Art 46 GDPR: In practice particularly big

US providers are not willing to adjust its data protection safeguards on a case by case basis, but are following the approach to establish a general set of standard documents applicable to all customers. Usually, the single EU customer does not have the market power to enforce changes to the documentation. Thus, it is of crucial importance to provide US providers with (i) a final set of provisions and (ii) reasonable and clear guidelines what is needed with regard to GDPR compliance. It is simply no realistic approach to shift this on individual level. Thus, a realistic and reliable draft of SCC as valid basis for data transfers is needed.

2. The importance of the SCC

We consider it as a great asset that the drafts for the Recommendations and for the new SCC were published at the same time. This allows a holistic view on both documents and understanding of its interaction and dependencies. It is of greatest importance that these two documents remain consistent in their final versions.

In order to meet the outlined market standard and practical requirements, SCC shall in particular – as they did in the past – provide a solid basis for data transfer to recipients situated in third countries. The most common issues in third countries, like the potential access of foreign authorities or lack of efficiency of data subjects' freedom and rights as addressed in "*Schrems II*", must be taken into account in such a way that the implementation of any other supplementary measures shall only be necessary in exceptional cases (see Pt 3 below). Otherwise, the European data controllers and processors, in particular SMEs, would have to bear the political issue of the consequences of lacking bilateral agreements on EU level. Mandating European companies to carry out critical examinations of each and every transfer of personal data to any foreign recipient although relying on already approved SCC is unrealistic and would lead to an increase of already existing legal uncertainty and connected liability issues. At the same time, this would also undermine the initial intent of the SCC, which always has been to (i) ensuring compliance with EU data protection standards, (ii) preventing case-by-case contract negotiations and (iii) avoiding lengthy approval proceedings. This should be uphold for the future. Thus, it shall still be possible in practice to rely to a large extent on the obligations provided for in the SCCs in order to maintain the required level of data protection rather than shifting the political issues and risks on data controllers. It is absolutely understood that there might be some specific scenarios that require additional supplementary measures, but this should rather be an exception than the basic rule.

3. Supplementary measures and approval requirements

Following the outlined approach above, it is, of course, understood that every data processing including data transfer must be assessed on a case-by-case risk decision. However, obligating all European data exporters to implement supplementary (technical) measures on top of the conclusion of approved SCC would undermine its established function as foreseen in the GDPR:

We agree to the approach that the audit provisions and required measures to be implemented depend on the specific type of data processing concerned and other factors of the case. However, it is important to note that additional measures should be necessary for specific constellations, only. However, especially when implementing simple marketing or web analysis tools or using other ordinary standard cloud solutions, data exporters must be able to rely on the agreement of strong SCC. This is even more true since the Commission has already addressed the concerns of the CJEU in its draft and has thus ensured a much higher level of data protection for the data importer when using the SCC as a transfer tool. Thus, if the new SCC will already provide a high contractual level of protection, this must at least be sufficient for the majority of processing activities in practice:

The latest draft of the SCC (i) updates the clauses – after more than 10 years – to be in line with the requirements of the GDPR (rather than the outdated EU Data protection Directive) and (ii) already covers the concerns raised in the "*Schrems II*" decision by the CJEU. Thus, the new set-up increases the level of data protection, privacy as well as data subjects' freedom and rights to a great extent. At the same time, the older version still in place – which has not even mentioned despite reflected the GDPR (!) – has been validly used without any need of supplementary measures or even official approval due to Art 46 Para 5 GDPR. The reason for enabling European companies to still rely on (already outdated) SCC was, of course, the practical need of legal certainty, in particular with a view on international transfer of personal data in the IT field. The new approach is somehow the extreme opposite of the approach during the last few years. Furthermore, it shall not be assumed that the parties agree on contractual measures that they cannot comply with. Since SCC itself constitute a contractual measure, this would undermine its purpose and make it impossible in practice to rely on SCC in the most cases.

Thus, if the EU Commission does now elaborate and decide on new SCC in order to strengthen the rights of European data exporters as well as the duties of international data importers, the overall obligation to (i) provide for supplementary measures and (ii) seek for prior approval would fully undermine the function of SCC. First of all, it is often not possible to implement technical measures – such as encryption or pseudonymization – prior to any kind of data transfer, since migration, maintenance and support services do factually need access to clear data. Thus, if any international data transfer does always required encryption, pseudonymisation or comparable technical measures, most of the already established and required IT services would have to be stopped. This would,

however, lead to the underlying, needed main service by the US provider not being employable for European companies.

The fact that the EDPB does currently not seem rather confident that strong contractual safeguards are sufficient is also evident from the examples at the end of the Recommendations: The implementation of such measures is tied to many different "*conditions for effectiveness*", which in the end leads to the conclusion that contractual measures shall never suffice so that again a practical implementation seems almost impossible. In addition, this does not sufficiently reflect that contractual measures can also increase the level of data protection: Simplified contract termination, data retransmission mechanisms, data minimization and the implementation of strict and short retention and termination periods are already established market standard – also in line with the rather stringent EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) for credit institutions or EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002) for insurances. In fact, strong contractual obligations are of most relevance in practice. Thus, an agreement on SCC shall usually suffice, while additional technical measures should be considered only in case the data importer actually believes that he cannot comply with the measures laid down in the SCC.

As to the approval requirement, the current draft of the Recommendations states that (i) no request for approval shall be required in case of "*supplementary measures in addition to SCCs*" are in place, while (ii) an approval shall be mandatory for any intend to "*modify the SCCs themselves*". This would, in fact, lead to a general approval requirement: In case supplementary measures are required – irrespective if on a technical or contractual side – these need, of course, to be reflected in an agreement with the data importer (eg duty of the data importer to provide for sufficient encryption). Such wording would – irrespective if included directly in the SCC or in another document – always "*modify the SCCs themselves*", which would then lead to an approval requirement. As we assume that this was not intended, we strongly recommend to merely state that an approval shall be mandatory in case "*the supplementary measures added 'contradict' directly or indirectly the SCCs*", only (as already stated in Recital 109). Otherwise we would fall back to the regime of previous approval of SCC that applied in Austria prior to the GDPR which did lead to waiting times of some months, even years. This would either hinder GDPR compliance or proper service provision.

C. CONCLUSION

In summary, we see significant added value by the Recommendations. Nevertheless, we encourage a more practical approach and consideration of already established market standard, eg in line with EBA and EIOPA Guidelines. In particular, we recommend to reconsidering the rather reluctant statement that contractual measures shall not be sufficient in most cases as this would fully undermine the function of SCC in the EU.

* * * * *

Please do not hesitate to contact us if you have any further request.

Best regards,

DORDA Rechtsanwälte GmbH

(Axel Anderl / Nino Tlapak)