European Data Protection Board
Rue Wiertz 60,
B-1047 Brussels
Belgium

ISPA AUSTRIA'S CONTRIBUTION TO THE PUBLIC CONSULTATION ON THE DRAFT RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

ISPA – Internet Service Providers Austria welcomes the opportunity to provide comments to the draft of Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. We are a voluntary business representation and act as the voice of over 220 internet service providers from various fields all along the internet value chain. Moreover, the majority of ISPA members are SMEs, and as such, face novel challenges from any new requirements. In our role as the voice of the Austrian internet industry we would like to address the following aspects of the draft text and provide recommendations where appropriate.

1) The Recommendations further enlarge the burden on small and medium-sized companies

In its recent judgement C-311/18 ("Schrems II"),[1] the Court of Justice of the European Union (CJEU) has severely exacerbated the situation for data exporters that until now have relied on appropriate safeguards in Article 46 GDPR when transferring personal data to a data importer in a third country. The Court has put the burden on these companies to assess whether – despite relying on the tools listed in Article 46 - a data transfers to a third country is still in accordance with the GDPR when taking into account the local laws. The judgement affects thus any company based in the EU and beyond[2] collaborating with business partners in a third country, using the services of such a company or even just transferring personal data to an associate company. Many European companies were therefor hopeful for additional guidance by the EDPB on how to implement the judgement in practice and find workable solutions, in particular considering the threat of a fine up to 4 % of the annual turnover for unlawfully transferring data to a third country.[3]

Unfortunately, the recommendations do not live up to these expectations, leave companies, among them many small and medium-sized enterprises (SMEs) in doubt and even enlarge the burden for companies. According to the recommendation's step by step guide, every data exporter must not only assess the circumstances of a particular data transfer but evaluate the legal system of a whole

[1] Case C-311/18 *Data Protection Commissioner v Maximilian Schrems, Facebook Ireland Ltd* [2020] ECLI:EU:C:2020:559
[2] Insofar as the company falls under the extraterritorial scope of Article 3 (2) GDPR
[3] Art 85 (5)(c) GDPR

third country, a highly complex task that takes even the experts at the EU Commission several years but must now be solved by a simple company in a short time and at their own expenses. Such an evaluation puts an immense burden on all small and medium-sized companies without their own legal department and without the financial resources to conduct external legal advice and put them in a significant disadvantage over large companies.

As the representation of many of such small and medium sized companies, ISPA Austria thus urges the EDPB to take their situation into account when revising the recommendations and to come up with solutions that are workable in practice also for companies with limited resources. At the very least, ISPA Austria asks the EDPB to provide the required assessments for the most common trading partners of the EU.

2) The Recommendations should follow the risk-based approach of the GDPR and the CJEU

The CJEU clearly stipulates that data transfers must be assessed on a case-by-case basis[4] as well as that all circumstances of a data transfer have to be taken into account.[5] Such an assessment is clearly in line with the risk-based approach underlying the entire GDPR. It follows that any assessment of a data transfer must go beyond a strict evaluation of merely the legal system of the relevant third country. In fact, such an evaluation is obligatory for the EU Commission to do only before issuing an adequacy decision subject to Article 45 GDPR – as this would be valid for all data transfers. As regards the use of SCCs it must however only be ensured that for the particular data transfers to which the SCCs apply, the rights guaranteed therein are ensured. Therefor ISPA Austria disagrees with the EDPBs assessment, that only objective and not subjective (i.e. case-by-case) factors must be taken into account in the assessment of a data transfer. Rather, it appears from both the risk-based approach of the GDPR and the elaborations of the CJEU that exactly the opposite applies.

Furthermore, in practice it would be up to the national DPAs to decide whether the specific assessment by a data exporter under their jurisdiction has been appropriate and a data transfer thus is in accordance with the GDPR. This has also been clarified by the CJEU.[6] It is however foreseeable, that without any guidance by an EU institution there will be diverging decisions of national DPAs, leading to a situation where data exporters in some Member States would be permitted to use SCCs when transferring data to a particular third country whereas others would not. This does not only lead to disadvantages for the companies in those Member States but also appears to clearly go against the function of recommendations issued by the EDPB which according to Article 70 (1)(e) GDPR should encourage the consistent application of the GDPR in the Member States.

Moreover, the draft of new SCCs that was presented by the EU Commission only a few days after the release of these draft recommendations provides in Clause 2 (b)(i) explicitly that the circumstances of a data transfer, including the “nature of the personal data transferred” and “the

[4] C-311/18 para. 134
[5] Ibid. para. 121, 146
[6] Ibid. para. 106 ff.

absence of requests for disclosure from public authorities received by the data importer for the type of data transferred" must be taken into account. The latter implies that even if there are local laws in place under which personal data may have to be disclosed under a regime that appears not adequate to the EU data protection and fundamental rights regime, this in itself is not reason enough to preclude the use of SCCs in this context entirely such as suggested for example in para 42 and 44 of the recommendations. Rather, if the data exporter comes to the conclusion, that there is in practice no risk that the personal data transferred will be disclosed to public authorities in the third country it should continue to be allowed to rely on the use of SCCs without any supplementary measures put in place.

This interpretation is further supported by the procedure provided in Clause 3 of the draft SCCs which requires a data importer to inform the data exporter immediately about any government access request that appears not to be in line with the SCCs. If the mere objective possibility of such a request would suffice to render a data transfer ex-ante unlawful this procedure would in practice be irrelevant.

The generalized approach taken by the EDPB and the restrictive interpretation of supplementary measures (see below under Pt. 3) basically would prohibit data transfers to many third countries based on the use of SCCs or other measures under Article 46. This would have the drastic result that routine business relationships with companies in many third countries could not be upheld and lead to a de facto isolation of the EU market which would severely hamper the position of EU companies on the global market, making an already difficult economic situation due to the current crisis even much worse. ISPA Austria is convinced, that this cannot be in the interest of the EU and its institutions and therefor urges the EDPB to revise its recommendations and adapt the risk-based case-by-case approach suggested both by the CJEU and the GDPR.

Lastly, it is also questionable, how the EDPB justifies that companies in the same third country may either process personal data where they fall under the extraterritorial scope of the GDPR under Article 3 (2) or not process it where they would be a data importer, as the legal obligations under the third country law and the ability of EU data protection authorities to intervene are essentially the same.

3) The listed supplementary measures are not workable in practice

The EDPB provides a non-exhaustive list of 'supplementary measures' that may be implemented where the data exporter comes to the conclusion that the guarantees provided in the SCCs cannot be complied with by the data importer due to the local law in the third country. Unfortunately, however, the case studies provided by the EDPB show a very restrictive interpretation of such supplementary measures that again goes against the risk-based approach of the GDPR already highlighted above. In fact, by already requiring the maximum set of safeguards for any data transfer to a third country where the initial assessment suggests that the third country legislation impinges on the effectiveness of the SCCs disregards the requirement in the SCCs itself, that for special categories of data (e.g. health or biometric data) stricter additional safeguards have to be applied. This would not be possible if the maximum level of safeguards is already the standard for any data transfer.

Instead of providing concrete examples for supplementary measures that are workable in practice, the EDPB unfortunately used the list of examples to generally exclude many of the most common constellations for data transfers entirely from the use of SCCs such as any transfer of personal data to an importer where the data is accessible 'in the clear'. This basically precludes the use of SCCs for all forms of electronic communication, transmission of employment data, or generally for cooperation with associate companies as for all of these purposes, the personal data transferred must be accessed in the clear by the receiving entity.

In general, the provided list of use cases lacks a prior evaluation of the available technical measures. The conclusions drawn by the EDPB therefore appear to be incomplete and inaccurate in parts and it seems that the EDPB focuses too much on encryption and pseudonymisation as the only available measures, without considering that even encryption technology can be reverse engineered and therefor does not serve as a guarantee against disclosure of data to law enforcement agencies in the third country. ISPA Austria thus encourages the EDPB to also evaluate other technical control and security approaches and techniques such as data masking or the use of pre-authorization controls that hitherto have been left out of the scope of the list.

Ultimately ISPA Austria requests the EDPB to rework the list and provide concrete examples for supplementary measures that are workable in practice. In this context the EDPB should also consider additional contractual measures as the CJEU has not ruled them out in *Schrems II* and the draft recommendations therefor also in this context go beyond the requirements set out by the Court.

ISPA would like to reiterate that it is very thankful for this opportunity to contribute. For further information or any questions please do not hesitate to contact us.

Sincerely,

ISPA Internet Service Providers Austria

Dr. Maximilian Schubert
Secretary General

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675