To: **The European Data Protection Board (EDPB)**

Dear Sir or Madam,

Feedback on '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 provide feedback on the draft recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ('the draft Recommendations'). As a company with more than 435 million users around the world whose online freedom we are striving to protect, we take data protection compliance very seriously and want to participate in the public debate about the most pressing privacy issues.

We, along with a great many European and international businesses, welcome the further guidance contained within the recommendations. Notwithstanding this, there are several specific points concerning the draft Recommendations that we would like to raise for your consideration, in particular where we believe the recommendations go too far beyond the requirements of the GDPR and the *Schrems II* ruling,[1] and could result in a disproportionate limitation on international transfers of personal data:

Assessment of Third Countries, 'Objective' and 'Subjective' Factors

With the scope of the draft Recommendations being wide-ranging, yet obviously focused heavily on the particular risks as highlighted in the Schrems II case, there appears to be some risk of the suggested measures being appropriate for international transfers involving a particularly high level of risk to privacy or data protection rights, however without sufficiently dealing with transfers in potentially more low-risk situations. In fact, some of the working (particularly the reference to 'subjective' factors in paragraph 42) seems to oust the possibility of taking the level of risk into account. This will potentially place an unreasonably high burden on data exporters and importers in situations not subject to the level of risk which was under discussion in the *Schrems II* case.

For example, Section 702 of the US Foreign Intelligence Surveillance Act (FISA) was one of the particular points at issue in the *Schrems II* case, presenting a particularly high level of risk (despite a comparatively low likelihood for any particular transfer, but strongly weighting the invasive nature the potential access to personal data). It was also the only piece of surveillance legislation in the US that was explicitly considered inadequate in the draft Recommendations. However, the suggestion in the draft Recommendations that the focus should only be on whether the data importer or any recipient falls in any way under the general scope of FISA, fails to take into account the specifics of a particular transfer, particularly whether only a subset of that data falls within the scope of the risk identified in *Schrems II*.

[1] C-311/18

This runs the risk of applying more onerous, disproportionate burden on all potential data processing by the importer, beyond the scope of the higher risk.

More generally, it does not appear clear where the line between 'objective' and 'subjective' factors as referred to in the draft Recommendations should or even could be drawn - running the risk of applying the highest standards to all transfers, irrespective of actual risk, and of leading to increasingly inconsistent and disparate approaches to transfers. If the aim is that data exporters assess not just formal legal risk, but the actual 'law or practice' in third countries,[2] an important factor is whether certain transfers of personal data are at a 'practical risk' of being subject to surveillance, not merely that the relevant government has a theoretical/formal right to access it.

Proportionality and Efficiency, Risk-Based Approach

The draft Recommendations outline a very robust procedure that should be followed by each data exporter in connection with transferring of personal data outside the EEA. Before the *Schrems II* judgement, the data exporters, which were diligent about their GDPR obligations would have already routinely followed the steps 1, 2, 5 and 6 outlined in EDPB recommendations with respect to all their international transfers. They have, however, in our experience, undertaken additional actions similar to those described in steps 3 and 4 only in specific circumstances of high-risk transfers of personal data.

The draft Recommendations now seem to require all data exporters to take all six steps independently for each international data transfer regardless of its risk profile. This would have a big impact on EU businesses, particularly small-to-medium enterprises (SMEs). It is important to note that EU businesses today routinely cooperate with a large number of third parties providing them with services or software solutions that they rely on in their everyday operations. Many of these third parties are located outside the EEA. The current draft Recommendations, if applied strictly and enforced across the board, could result in a compliance burden disproportionate to the risk and which may prove virtually impossible for some SMEs.

The risk of such an approach is that it could result in many EU businesses simply decide to take their chances or ignore the recommendations, such as by taking a very simplistic or formalistic approach to meeting the obligations, as they realize that they are unable to comply with them in a strict sense. The alternative outcome, that strict recommendations or rules are in place, but only enforced lightly or inconsistently, is not a desirable outcome for the reputation or effectiveness of the GDPR, nor for the general interest for both the public and businesses in legal certainty.

Further, in the context of paragraphs 88-91 of the draft Recommendations, describing the types of transfers for which no effective measures can be found, this also appears to take a disproportionate, 'all or nothing' approach to mitigating risks in international data transfers. We suggest that the approach to such situations should rather be one that allows for a more risk-based assessment of whether the type of the

[2] As suggested in paragraphs 20, 30, 60, 66, and 107 of the draft Recommendations

data in the context of the particular transfer is actually at risk of being subject to surveillance and not that it may be subject to such surveillance under applicable law regardless of how unlikely it is in practice. The alternative approach runs the risk of disrupting a large number of transfers and processing operations, which data subjects rely on and expect, where the residual risk is low or non-existent, whilst diverting resources and focus from identifying solutions to higher-risk scenarios.

Given the above, we ask the EDPB to consider introducing a more risk-based approach in general to the process of assessment of international data transfers to allow EU businesses to focus their compliance efforts on truly risky transfers. For example, the EDPB can develop criteria for assessment of the risk-profile of data transfers and require data exporters to follow a full-fledged procedure only with respect to transfers identified as high-risk. We believe that this risk-based approach allowing EU businesses to strive for compliance would in practice deliver more protection to the EU data subjects than the currently proposed solution.

Burdens to Assessment of Third Countries

Step 3 of the assessment process outlined in the draft Recommendations requires data exporters to assess whether the Article 46 GDPR transfer tool that the data exporter is relying on is effective in light of all circumstances of the transfer. In particular, this means that the data exporter must assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards.

Paragraphs 28 to 44 of the draft Recommendations provide a general description of factors that must be taken into account by the data exporter as part of this assessment. The draft Recommendations explicitly state that it is not enough for the data exporter to assess the laws of the third country, but that it also needs to take into account the actual practice and other objective factors.

The examples of invalidation of the Safe Harbour and Privacy Shield decisions have demonstrated how difficult it is to correctly assess adequacy of third countries in connection with transfers of personal data. According to the CJEU, the European Commission repeatedly failed to correctly assess the adequacy of the US legal framework despite the considerable amount of time and resources devoted to this assessment. In such a case, can it reasonably be expected of businesses, particularly SMEs, in Europe to be able to carry out these assessments as part of their ordinary course of business, with more success than the European Commission?

It is clear that conducting a proper assessment of a legal framework of a third country is a very complex legal task, which will require enormous resources on the part of the EU businesses. In addition, this approach would also lead to massive inefficiencies as each data exporter would be doing the same (or a very similar) legal exercise independently on each other. Finally, even after completion of the assessment,

the relevant data exporter will have no guarantee that its assessment would withstand a challenge by a supervisory authority or court.

Given the above, we consider the requirements for assessment of legal frameworks of third countries laid down by the draft Recommendations as difficult and potentially ineffective to implement in practice. We see two possible solutions to this problem. The EDPB or the European Commission could conduct general assessments of legal frameworks of third countries and make them available to the public. The data exporters would then only need to assess the particular circumstances of their transfer in the light of the assessments made by the EDPB or the European Commission to determine whether the relevant transfer is possible or not. The second option is for the EDPB to simplify the requirements for assessment of legal frameworks of third countries. For example, the EDPB can specify that the assessment is not needed for certain low-risk types of transfer. Furthermore, the EDPB could also determine an exhaustive list of aspects of the third country's legal framework that must be assessed by data exporters to narrow down the scope of legal analysis required in connection with the assessment.

We would be happy to discuss any of the above suggestions with you in more detail. You can contact us at privacy@avast.com

Kind regards,

Shane McNamee (Chief Privacy Officer)

Ondřej Kramoliš (Senior Legal Counsel)

Avast Software s.r.o.