Position Paper on the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – Adopted on 10 November 2020

Berlin, 18 December 2020

Following on from the lawsuit in the jurisdiction of the Court of Justice of the European Union (ECJ) in the case of the Irish Data Protection Commissioner versus Facebook Ireland and Max Schrems (C-311/18), commonly known as Schrems II, the European Data Protection Board (EDPB) has published a set of recommendations which, from the Board's perspective, are to be observed when conducting data transfers with third countries.

These recommendations are intended to provide companies and organisations (in general, data exporters) transferring data to third countries with a manual to follow in order to legally transfer their data to such nations. The manual sets out a six-step schema for data exporters to follow.

The six steps are:

- Know your data transfers
- Identify the Transfer Tools you are relying on
- Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer
- Adopt supplementary measures
- Procedural steps if you have identified effective supplementary measures
- Re-evaluate at appropriate intervals

While, in general, the guidance offered by the EDPB may be regarded as helpful and the manual may give orientation to actors conducting data transfers, there are still critical questions which arise from the detailed elaboration of the EDPB recommendations. The requirements in general impose a great burden on companies and organisations transferring data to third countries, are almost impossible to meet, and can be regarded as obtrusive.

Given the practical impact of such guidance on EU businesses and on their ability to grow their business within and outside of Europe, eco respectfully requests the EDPB to review its guidelines in this respect. Businesses need to have better clarity on how to address the issues raised in the Schrems II ruling. In eco's view, this would also benefit data protection authorities who want to ensure that their enforcement actions will remain effective and proportionate in accordance with Article 83 GDPR.

eco – Association of the Internet Industry's comments on the proposal for the recommendations of the EDPB are as follows:

On “Know your Data Transfers”
While it is clear that companies are required to provide persons whose data they are processing with information on how their data is processed, and to create and maintain overviews of data processing carried out by them or on their behalf, the EDPB guidelines do not give additional technical advice on how such an evaluation is to be conducted, nor do they provide tools that actually may be helpful for companies in doing so. This issue has already been observed in a more general constellation within the context of the GDPR discussion. The EDPB is urged to provide additional information and give examples based upon which data exporters can better identify whether they are transferring critical information.

On “Identify Transfer Tools you are relying on”
The transfer tools organisations and companies are provided with for transferring data to third countries may in general appear broad; however the level of legal certainty they provide is far too insufficient, and would often confront companies with a conundrum. While adequacy decisions provide the highest level of safeguards for data transfers, only a few are in place, some of which have been repeatedly revoked. The new draft standard contractual clauses, which are generally regarded as a very reliable legal tool upon which data transfer can be based, are currently in discussion, meaning that no final statement can be made about them. However, the current draft guidelines suggest that there may well be an extension of the legal uncertainty with which companies are confronted when transferring data to third countries, where legislation may impinge on the privacy of stored or processed data. In this case the guidelines foresee supplementary measures tailored to the specific context of the intended data transfer and target country.

Binding corporate rules have proven burdensome even for large companies. As such, it is not to be expected that they will play a larger role for the majority of planned data transfers to third countries, and smaller organisations will not be able to comply with these rules.

The further options the EDPB has proposed will in turn not provide the necessary legal certainty for companies for several years to come, given that case law around the GDPR is still evolving.

The transfer of data under reference to Article 49 GDPR appears to offer an understandable legitimate basis for data transfers. However, with its narrow scope, the effectiveness of the derogation can be called into question, especially for digital technologies and mass markets.

On "Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer"

Aside from the challenges arising from the appropriate choice of legal justification for a data transfer, the EDPB further argues that the transfer of data may not undermine either the principles of data protection as set out in the GDPR, or fundamental rights. While this can be regarded as a general requirement set up by the GDPR, the EDPB requires that the assessment shall not only take into account legal requirements in the third countries referred to, but also "other relevant and objective factors". It also states that the general rule-of-law situation in a country is of relevance. This may extend the level of assessments required, given that not only the legal situation in a third country may now be regarded as insufficient, but also the fact that there have been incidents that have thwarted such laws. The comprehensiveness and the dynamic of the IT security environment, including practice, could easily pose an an insurmountable challenge for data exporters undertaking assessments according to the recommendations of the EDPB.

On "Adopt supplementary measures"

While the recommendation to adopt supplementary measures is generally understandable, it nonetheless calls into question the existing practice of data exchange with third countries, especially those under the auspices of standard contractual clauses (SCC). Regulations including SCCs should be general and reliable for organisations and companies employing them in their original form, along with general rules for cybersecurity and information security. The amendment of supplementary measures implies specifically tailored approaches which go beyond assessments and measures deployed in line with the catalogue above for certain countries. The benefits of general decisions, especially data protection adequacy decisions of the European Commission, are foiled if they are to be supplemented with additional specific measures, meaning that these decisions – along with additional sector-specific regulation and requirements for IT security and information security – can be regarded as insufficient. The EDPB is called upon to clarify under which circumstances supplementary measures are actually required and to refrain from demanding them in cases where data protection adequacy decisions exist, if general regulation and requirements are observed.

More generally, in its recommendations, the EDPB should more intensively consider the central role of the risk approach when the exporter needs to assess the "adequacy" of third country laws and adopt, where necessary, supplementary measures. Such measures should depend on the likelihood of the risks and therefore result in contractual, operational or technical measures or a combination of these. A general approach, as it is currently being pursued, will not take into account the variety of business situations and related specific technical capabilities.

Taking into account the prohibitive nature of the failure of one or more supplementary measures, to what extent alternatives for the respective

supplementary measures are to be created is open to further question.

On “Procedural steps if you have identified effective supplementary measures”
See above

On “Re-evaluate at appropriate intervals”
See above

Conclusion
eco acknowledges that the recommendations had to reflect the complex ECJ “Schrems II” ruling. And yet, by deviating from the GDPR’s risk-based approach, the recommendations add to the complexity, as they elaborate on a set of requirements and measures that require significant investment from data exporters. As a matter of fact, it is to be expected that a great number of actors, especially SMEs but also larger companies, will not be able to meet the requirements set by the EDPB.

If jurisdiction and case law will follow these recommendations, data transfers into third countries will be seriously impeded – notwithstanding, in turn, the question of what data is transferred and how critical or problematic this is, given the very broad nature of personal data. Beyond that, companies with headquarters within the EEA and subsidiaries in third countries who may be required to export data in order to comply with local jurisdiction may suffer a de facto interdiction of conducting business.

Additionally, it has to be taken into account that not only companies are required to actively follow and orient themselves on up-to-date information concerning legislation and case law in third countries, but also data protection authorities and courts should be required to do so. With new SCCs soon to be adopted, the guidelines of the EDPB may have to be revised, irrespective of further developments in third countries.

In conclusion, eco regards the measures required to “export data” as disproportionate and unsuitable. eco acknowledges that requirements for “data export” are to be met according to the GDPR and that political solutions, namely adequacy decisions, are to be found on a political level. These solutions, however, should not be corrupted through excessive implementation, which may lead to a turn against regulation and, in the end, undermine the aim of protecting people’s personal data.

About eco: With over 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. eco's key topics are the reliability and strengthening of digital infrastructure, IT security, and trust, ethics, and self-regulation. That is why eco advocates for a free, technologically-neutral, and high-performance Internet.