RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

CONTRIBUTIONS OF SPANISH STARTUP ASSOCIATION

On November 10th 2020, the European Data Protection Board adopted two sets of recommendations on the transfer of personal data from the European Union to third countries further to the Court of Justice of the European Union ruling in the Schrems II.

These recommendations about the CJEU's invalidation of the EU-US Privacy Shield were highly anticipated by all kind of businesses and organisations, and specially by startups. Although many were hopeful that the EDPB would provide data exporters with practical measures that would help to comply with the Court's decision, we think that this Recommendations, by proposing a non-risk approach that goes far beyond the requirements of *Schrems II,* they are missing that chance. Rather than following the Court's instruction to take the context of a transfer into account, the Recommendations are even more restrictive than the GDRP and may make impossible for most startups to transfer personal data outside the EU, which is crucial to provide global services, to compete and to survive.

Furthermore, if these *Recommendations* are adopted in their current form, any organisation that uses an online service to process and transfer personal data, including email, mobile apps, hosted applications, or any other online service as ubicuous as search engines, cloud hostings, chat applications, online banking, GPS and so on, could face fines up to 4% of its annual turnover.

As a result, they will make it impossible for most EU startups to provide their services.

In its Recommendations on Supplementary Measures, the EDPB suggests following a methodology oriented around the six following steps.

- ***Step 1****: Know your transfers. Data exporters should record and map all international personal data transfers and verify whether they are adequate, relevant and limited to what is necessary in relation to the purposes for which they are operated. Organisations should aim to be fully aware of their data transfers (including onward transfers) despite the existence of numerous processors and sub-processors.*

In *Schrems II*, the Court indicated that data exporters should consider the full context of a transfer when evaluating its legality—specifically, that transfers should be evaluated "in the light of all the circumstances of that transfer" and "on a case-by-case basis". However, several passages in the *Recommendations* appear to foreclose this contextual approach. For instance, they state that, if the data importer falls within the scope of certain national security laws, the data exporter must use additional technical measures—

even, presumably, if the data importer has never faced an order under those laws and the data is of no conceivable relevance to national security (e.g., an employee's menu preferences for a holiday party). Other passages similarly suggest that the likelihood that a public authority will ever access the data is irrelevant, contravening the proactive responsibility principle of GDPR.

Restricting transfers of data even where the risk assessment and Privacy Impact Evaluations show there is virtually no risk to data subjects will not be proportional and it may endanger the EU economy and society. Rather than discourage EU organisations from considering contextual factors, the *Recommendations* should encourage organisations to take into account the real-worlds risks of a transfer, including the relevance of the data to law enforcement agencies and the likelihood that such agencies would request access to the data. If these real-world risks are low, which they are for most categories of data, the *Recommendations* should not require organisations to adopt any supplemental measures than the ones recommended by their Data Protection Officers.

By denying a risk-based approach, the *Recommendations* not only do not respect this essential principle of the General Data Protection Regulation, contained in the Schrems II, but it also contradict the Standard Contractual Clauses published by the Commission, putting organizations in an impossible situation.

- ***Step 2**: Identify the transfer tools relied upon. Organisations should identify the appropriate mechanism for the data transfer (e.g. adequacy decision, SCCs, derogation for specific situations of Article 49(1) GDPR, etc.). The EDPB notes that no further steps are required for transfers relying on an adequacy decision, provided that the data importer has implemented measures to comply with the obligations of the GDPR as appropriate.*

The *Recommendations* propose a list of technical measures that data exporters can use to supplement the safeguards in the SCCs. Unfortunately, the *Recommendations'* case studies on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice. For instance, the *Recommendations* suggest that organisations can rely on encryption as a safeguard in most cases only if the data never appears in an unencrypted form in the third country and if the decryption keys are held only within the EU (or an adequate jurisdiction. They also suggest that encryption almost never provides sufficient protection where data is accessible "in the clear" in the third country, including where an EU organisation uses an online service that may process the data in the third country, or where employees or others in the third country can access the data on a shared IT system (e.g., human resources data). Moreover, because the *Recommendations* state that even remote access by an entity in a third country to data stored in the EU constitutes a "transfer", organisations in many cases would need to apply these technical safeguards to EU-stored data as well.

More pragmatically, the *Recommendations'* positions on technical measures would render the SCCs virtually worthless as a transfer mechanism. In the vast majority of cases, the reason companies transfer data to third countries is to communicate and share information with people in those countries. If those people cannot access the information —as the *Recommendations* would require—there is no point to the transfer. Similarly, many online services that EU businesses rely on today must be able to process the information in unencrypted form in order to work properly; given the nature of the Internet and the global economy, this might entail some processing that occurs outside the EU, irrespective of where the data controller or data processor is based.

Finally, although the ruling, apart from the EU-US Privacy Shield, held that organizations may need to adopt additional safeguards to protect personal data from access by public authorities in third countries, we understand that the principles set out by the ruling should equally apply to other transfer basis, such as the binding corporate rules.

- ***Step 3**: Assess whether the transfer tool you relied upon is effective in light of all the circumstances of the transfer. Organisations are responsible for assessing and analysing whether the laws and practices of the third countries concerned are effective enough to meet the appropriate safeguards set by the GDPR. This assessment shall include the circumstances as well as all the players participating in the transfer previously mapped in Step 1.*

Although the *Recommendations* propose a list of contractual measures that can offer additional safeguards, they also include language suggesting that contractual or organisational measures on their own (i.e., without additional technical measures) cannot provide the level of data protection that EU law requires. This position appears to be based on the assumption that the mere theoretical possibility of access by third-country authorities—even if the practical risk of such access is vanishingly small—renders a transfer unlawful.
This position adopts an overly restrictive reading of the *Schrems II* judgement. The Court in *Schrems II* held that transfers of data to third countries should be prohibited only "in the event of the breach of [the SCCs] or it being impossible to honour them. This language, and similar passages elsewhere in the judgement, suggest that, so long as the data importer does not in fact disclose data to third-country authorities (or, if it does make such a disclosure, that it notifies the data exporter accordingly), then the parties may rely on the SCCs. Under this reading, it is clear that contractual measures alone can provide the additional safeguards needed to safely transfer data to a non-adequate jurisdiction.

To align with the *Schrems II* judgement, the *Recommendations* should remove all language suggesting that contractual measures alone are insufficient safeguards. The *Recommendations* should instead articulate several possible contractual measures that EU organisations may consider when transferring data to a non-adequate jurisdiction, then leave it to data exporters and importers to evaluate which measures are appropriate in context and "in the light of all the circumstances of that transfer".

They also will require EU organisations to undertake their own costly analyses of the laws and practices of dozens of non-EU countries (i.e., those not subject to an EU adequacy decision), which will be unrealistic for most startups.

- ***Step 4**: Adopt supplementary measures. If the appropriate safeguard adopted for the data transfer is not effective according to the assessment in Step 3, organisations (in cooperation with data importers) will have to adopt supplementary measures along with that appropriate safeguard to attain an equivalent level of data protection, as is required by the GDPR.*

The Court's holding in *Schrems II* was a major and unexpected development, one that is requiring organisations across the EU to prepare new data transfer impact assessments and, in certain cases, to overhaul aspects of their data transfers. In many cases, these efforts require changes not only to contracts, but also to underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organisation.

Notwithstanding these facts, the *Recommendations* imply that supervisory authorities should move directly to "corrective measure[s] (e.g. a fine)" if they determine that a data transfer does not comply with the *Recommendations*. This focus on sanctions will lead EU organisations to rush through changes to their data transfer practices—making it far less likely that organisations address these issues carefully and precisely.

To avoid this outcome, the *Recommendations* should expressly advise supervisory authorities, when they determine that a specific data transfer does not comply with EU law, to work with data exporters to find acceptable safeguards, and give them sufficient time to implement such solutions. This approach will provide incentives for EU organisations to address these issues thoughtfully, while also encouraging good-faith, collaborative solutions to these quite difficult legal and technical issues.

- ***Step 5**: Adopt procedural steps if you have identified supplementary measures. Organisations which have identified adequate supplementary measures will have to implement supplementary procedural steps or additional requirements before use.*

Startups are always looking for more efficient ways to satisfy human needs and they focus on make their customers lifes easier. If we want our startups to be able to help people and to compete with startups from other regions, we need to reduce administrative burdens and facilitate their work.

- ***Step 6**: Re-evaluate at appropriate intervals. Data exporters must continuously monitor significant developments that may affect the level of data protection in the third countries concerned. If a country has passed a new national security law, organisations might, for example, have to repeat Step*

It is impossible for almost any company to know the different laws of every country in the world and specially for SMEs and startups. Even European lawyers struggle to understand the different EU countries' Law so if we want to have a strong EU economy, we need to guarantee legal certainty for EU companies.

In conclusion, to avoid these consequences we need a more pragmatic approach that provides practical and workable guidance. That will allow for businesses and organisations to take steps to ensure that they can continue to transfer data in a responsible way. The EDPB should revise the *Recommendations* to ensure that the proposed technical measures are workable in practice, and should leave it to data exporters to determine whether any particular measure adequately protects the transferred data. The *Recommendations* should not prohibit all access to data in the third country; doing so will discourage organisations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorised access.