Raiffeisen Bank International AG (RBI) comments on

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

We welcome the publication of these Recommendations by the EDPB and gladly take the opportunity to provide feedback on the proposed measures.

General remarks

In principle, the Recommendations are highly appreciated with regard to the CJEU's invalidation of the EU-US Privacy Shield. They are presented in an understandable way, contain suggested steps and use cases and provide for a roadmap of good practices for data exporters. However, for some of the proposed measures we have questions or concerns regarding the practical implementation (please refer to the Specific remarks below).

The recommended "contractual measures" are useful and from our point of view applicable for use cases where the data are stored and processed in Europe, but the mother company is in U.S./third countries.

Also Annex 3 – *Possible sources of information to assess a third country* is helpful and we understand it in a way that **exporters don't have to evaluate the same level of data transfer of the import country by themselves case by case,** but can rely on assessments of the possible sources mentioned in Annex 3. Please confirm in the Recommendations (e.g. in an example or use case) that our understanding is also the view of the EDPB. Because **if it was left to the exporter to case-by-case assess whether the legislation of a third country in its entirety allows for personal data to be transferred to it**, this would lead for each and every single data exporter (e.g. companies operating in an economic perimeter) to completely assess each and every legislation in third country on a use-case basis. This would not only constitute a **massive and unacceptable burden** for a single data exporter, it would also lead to severe economic disadvantages countries within the EEA perimeter as personal data transfers by exporters operating in these countries would be severely damaged by the need to bear the burden of establishing huge own legal systems to be able to comply with the need to assess all third country legislations by themselves. And last but not least, it would lead to legal uncertainty due to possible different legal opinions in a country and in Europe.

Further assessments must be done centrally on EU-level, e.g. by speeding-up the process of taking adequacy decisions on the one hand and addressing all legal issues of any third country that prevent data exporters from transferring personal data.

According to the underlying Recommendations (e.g. 2.6.), this assessment should be done on an ongoing basis. This would lead to an even bigger burden for the data exporter and **has to be firmly rejected**. From our point of view, the **Whitepaper "Information on US Privacy Safeguards relevant to SCCs and other legal bases for EU-US Data Transfers after Schrems II** " (see here: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF) should be explicitly considered regarding remedies provided by the specific US surveillance laws mentioned in Schrems II (also in the light of similar surveillance laws within the EU) and could be applicable for an evaluation which measures would provide an adequate mitigation for which types of transmission or data categories.

- ⇨ In general, an **overview of recommendations regarding the necessary measures for data transfer to third countries would be helpful**. Such an overview should particularly state, which countries don't require additional measures to Art 46 GDPR as well as which do, including the required measures. This would provide a clear guidance for data transfers to third countries and ensure a unified approach by all EU companies. In the absence of respective Adequacy decisions by the European Commission, guidance by the EDPB – at least for the most important third countries in terms of international data transfers – would be appreciated.

Specific remarks and questions for clarification

- **Article 46 GDPR Transfer Tools (Nr. 21, page 11):**
  We do not share the opinion that there really is a series of transfer tools at the (immediate) disposal of data exporters, as most of the available transfer tools are not very practical.
  Binding Contractual Rules especially for big multinational market players as financial institutions very often are, do take years to come into effect as they need to be adopted by each and every Data Protection Authority in the countries of presence of these.
  Codes of conduct and certification mechanisms are still very rarely adopted by the national authorities and other relevant bodies.
  - ⇨ In fact, the very vast majority of data exporters has to rely on Standard Contractual Clauses for personal data transfers to third countries, which is why the current status and the underlying Recommendations do not provide sufficient support. Further, the **process of adequacy decisions legislation must be speeded up** in order to remove the heavy burden from data exporters as stated above.

- **Article 49 GDPR derogation (Nr. 26, page 11)**
  EDPB confirms that Art. 49 derogations do not require an assessment of the level of protection in the third country. However, it reiterates its standpoint that all derogations mentioned in Art. 49 have an exceptional nature as mentioned in its prior guidelines. More clarification would be useful either in this document or in the recommendations concerning Art. 49 GDPR. (Guidelines on derogations applicable to international transfers (art 49)

- **BCRs (Nr. 58.ff, page 18):**
  Art 46 GDPR lists **Binding Contractual Rules as an appropriate safeguard for personal data transfers to third countries**.
  BCRs are an instrument that the Data Exporter needs to get approved by the relevant Data Protection Authorities. This is why it should be assumed that the relevant Data Protection Authorities do approve BCRs considering relevant legislation for the involved third countries.
  - ⇨ Therefore, **Data Exporters should not be requested to ensure by themselves that the third countries involved provide an essentially equal level of data protection when BCRs are in place approved by the relevant Data Protection Authorities.**

- **Examples of supplementary measures (Nr. 69.ff, page 21):**
  Unfortunately, the listed use cases are not fully reflecting the business reality and thus only to a limited extent supportive. Use case 1 (encryption) and 2 (pseudonymization), deemed to be an effective measure by EDPB, do not provide for a feasible solution.
  Option Encryption of data requires, that the key stays only with the controller within the EU. This is not an option, as providers need the key in order to provide processing services, analytics, calculations, …

Option Pseudonymization means that absolutely no re-identification is possible. This is also not an option, as EDPB states, that interactions with internet-based services may allow for identifications, even if plain identifiers as names are omitted.
Most common transfer of data to third countries is use case 6 (Transfer to cloud services providers or processors which require access to data in the clear). Unfortunately, not even deemed to be an effective measure by EDPB.

- ⇨ **Consequently, it should be granted more feasible guidance from EDPB** or national authorities, also in terms of specific countries. **The most common use cases along with guidelines how to provide for remedy should be listed**.
- ⇨ Further, in this whole context, **efforts on EU-level to induce and foster EU- infrastructure providers need to be amplified and strengthened**. Current developments around GAIA-X will take presumably years until a cloud infrastructure of a relevant scale is provided within the EU.

- **Additional Contractual measures (Nr. 92 ff., page 28):**
  Please confirm or point out in the Recommendations (e.g.as a use case or example), that the measure of data localization in Europe (i.e. data in Europe - mother company in third country) is sufficient and that in case contractual measures (as provided in the Recommendations, especially the "warning clause") are concluded between the exporter and importer this is sufficient to be compliant.

- **Annex 3 (Nr. 138, page 38):**
  A confirmation would be appreciated in the Recommendations that exporters don't have to evaluate the same level of data transfer of the import country by themselves cases by case but can rely on assessments of the possible sources mentioned in Annex 3. These "possible sources" should be called upon the EDPB to issue binding legal opinions concerning the most important third exporter countries. (See also our comment in the *"General remarks"*).

Further observation

Concerning a new pact between Europe and the US following the Privacy Shield – without a change of especially the FISA law and also taking into consideration the arguments raised by Deputy assistant Secretary James Sullivan concerning the limited scope of application of US surveillance practices and the US published White Paper – a similar level of data protection is difficult to ensure only on a contractual level (learning from Schrems I and Schrems II).
Currently we can observe due to the Schrems II judgment, that US companies as Microsoft and AWS are aware of the situation and try, as far as their local law allows, to comply with European law. On the one hand, because they do not want to be penalized under GDPR, on the other hand, because they do not want to lose customers in the EU. However, in the current situation this is very much dependent on the respective companies. **A commitment from EDPB that European companies, which largely depend on the US providers, will not be punished for further using them after trying to comply with the recommendations and taking into consideration economically justifiable expenses, would be very helpful and would relax the situation for European companies.**

Raiffeisen Bank International AG | Member of RBI Group
Am Stadtpark 9, 1030 Vienna, Austria | www.rbinternational.com

Contact: Anja Moser, Group Regulatory Affairs Manager
T: +43 1 71707- 2358 | M: +43 664 8888 2358 | anja.moser@rbinternational.com