Comment

of the German Insurance Association (GDV)
ID-number 6437280268-55

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

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Phone: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Contact:
Datenschutz/Grundsatzfragen

E-Mail: **data-protection@gdv.de**

www.gdv.de

Executive summary

The German Insurance Association welcomes the EDPB's attempts to create more clarity with regard to the conditions for transfers of personal data to third countries. While the draft recommendations 01/2020 succeed in giving data exporters and importers a step by step instruction on how to proceed if they carry out data transfers to third countries, the details of some aspects are in need of reconsideration:

- Requirements for consent under Art. 49 GDPR
- Obligation to assess the level of data protection in third countries
- No additional commitments in BCR's
- Application of the risk-based approach and
- Examples of supplementary measures

1. Introduction

The German Insurance Association welcomes the EDPB's attempts to create more clarity with regard to the conditions for transfers of personal data to third countries. In the wake of the ECJ's Schrems II – decision European companies find themselves in a difficult position. They are in need of practical instruments for ensuring that established processes do not have to be abandoned where no adequate alternative exists. The global interconnection of the European economy requires solutions which ensure the protection personal data without isolating the European Union. The free flow of data remains an important aspect for fostering innovation, prosperity and well-being of the EU. Data localization schemes cannot be an answer. Against this background, the ECJ has imposed on the data protection supervisory authorities a difficult and important task. While the draft recommendations 01/2020 succeed in giving data exporters and importers a step by step instruction on how to proceed if they (plan to) carry out data transfers to third countries, some details should be reconsidered:

2. Consent under Art. 49 GDPR

As the EDPB correctly states the Derogations in Art. 49 GDPR are of exceptional nature. While the derogations should be interpreted in the light of that nature, clear differentiation is necessary between the individual subparagraphs of Art. 49 (1) GDPR. It is important to note that recital 111 of the GDPR only requires that processing activities based on Art. 49 (1) (b), (c) and (e) have to be occasional. Meanwhile recital 113 only states that transfers based on compelling legitimate interests pursued by the controller shall be non-repetitive. Both, the requirements of being occasional and non-repetitive, do not apply to consent under Art. 49 (1) (a) GDPR. The exceptional nature of this provision is instead upheld through the enhanced requirements for valid consent compared to Art. 6 (1) (a), Art. 7 and Art. 9 (2) (a) GDPR. It has to be explicit and the data subject has to be informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards. Thus, the EDPB should take the opportunity to clarify this in para. 24-25 of the recommendations 01/2020. The already strict requirements in Art. 49 GDPR should not be interpreted even more restrictively than what is established by the GDPR text and the recitals.

3. Assessing the level of data protection in third countries

The EDPB tries to provide guidance on how the parties involved in the data transfer can assess the level of data protection in third countries and whether their transfer tool is effective in light of all circumstances. In theory, the explanations and the recommendations 2/2020 do show data exporters

and importers which aspects should be taken into account when trying to conduct the assessment. However, a practical realization will rarely be possible. It is highly questionable if even big groups of undertakings can successfully perform such an assessment with or without external help. The EU-Commission (EC) itself failed twice with respect to Safe Harbor and the Privacy Shield. It is all but impossible for SME's to correctly conduct the assessment on a case by case basis (Step 3 of the recommendations) and perform a re-evaluation at appropriate intervals (Step 6).

With this situation in mind, we would ask the EDPB to provide more concrete guidance by supporting the companies with specific assessments of the level of data protection for particular third countries.

4. No additional commitments in BCRs

According to para. 59 the EDPB is currently discussing the precise impact of the Schrems II judgement on BCRs. We would argue against requiring to include additional commitments in the BCR's themselves. The ECJ did not make any deliberations that would question the validity of past practices concerning BCR's. Working papers 256 and 257 already contain specifications which can make the implementation of BCRs more difficult than what is established by Art. 47 GDPR. Furthermore, both Working papers already account for the national legislation in third countries in criteria 6.3 and 6.4 for the approval of BCR's. The inclusion of additional commitments which apply to all members of the group regardless of the specifics of intragroup procedures, interactions, data transfers and the country of their establishment is neither appropriate nor reasonable. Instead, additional commitments and/or supplementary measures should be arranged and implemented separately and on a case by case basis depending on the particular data transfer.

5. Risk-based approach

When assessing the level of data protection in the third country and choosing to implement supplementary measures, one important aspect to take into account is the risk-based approach. As the EDPB states, effective supplementary measures must be identified on a case by case basis (para. 46). However, the EDPB also states in para. 42 that for the assessment of the level of data protection in third countries only objective factors should be looked into. In contrast, subjective factors such as the likelihood of public authorities' access to the data should supposedly not be relied upon.
The exclusion of subjective factors is not justifiable. The EC has emphasized on several occasions that the risk-based approach also factors into risk assessment when evaluating the level of data protection in third

countries. In its draft for an implementation act on updated standard contractual clauses for the transfer of personal data to third countries the EC explicitly calls for the data exporter and importer to

> *"in particular take into account the specific circumstances of the transfer (such as the content and duration of the contract, the nature of the data transferred, the type of recipient, the purpose of the processing and any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred)"*

when assessing the laws of the third country (rct. 19-20). Furthermore, the draft SCCs add *"the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used;"* as factors to consider (draft SCCs Section II Clause 2 (b) (i)).

These extracts further underline that the regulator intends for the subjective factors to be another element to rely upon for the assessment of the level of data protection.

This is in line with the fact that the risk-based approach is a fundamental pillar of the GDPR and must thus also apply to data transfers to third countries. We would ask the EDPB to better reflect this circumstance in the recommendations 01/2020. The risk-based approach is expressed in particular in the selection of technical and organisational measures under Art. 24 and Art. 32 GDPR. The implementation of the Schrems II legislation is concerned precisely with technical and organisational protective measures to prevent access by authorities in third countries.

When assessing whether an equivalent level of data protection can be ensured, the risk-based approach must necessarily factor into the equation. If it is not applied to data processing in third countries, the EU would in conclusion demand a level of data protection from other countries that goes beyond the one guaranteed by the GDPR.

6. Examples of supplementary measures

a) General remarks

In line with our deliberations under point 4, we would also ask the EDPB to adjust its explanations in Annex 2 on examples of supplementary measures. The use cases do not adequately reflect the risk-based approach but rather try to establish a rigid threshold. This contradicts the flexibility granted to controllers by the GDPR.

The EDPB should accentuate that contractual and organizational supplementary measures alone can suffice under the risk-based approach depending on type of data concerned, its sensitivity and the likeliness of public authorities' access among others. Purely technical supplementary measures especially with the requirements outlined by the EDPB in Use Cases 1-6 will often not correspond with the principle of proportionality. Due to the fact that much data is both, of low sensitivity and no interest to intelligence services, in many cases contractual and organizational supplementary measures can be sufficient to guarantee an adequate level of data protection under the risk-based approach. Therefore, especially Use Cases 6 and 7 should be changed to accommodate this aspect. The statement that no effective measures could be found for these scenarios appears disproportionate. In their current form, the Use Cases will rarely be of use and should be either overhauled or complemented with additional Use Cases.

b) Exemplary illustration of the lack of practicality on the basis of Use Cases 1 and 6

In Use Case 1 the EDPB requires the encryption keys to be retained solely under the control of the data exporter or other entities residing in the EEA (or a third country for which there is an adequacy decision) and the keys have to be reliably managed.
"Reliable key management" may sound realizable in theory. However, without specific guidance by the EDPB on how to fulfil this requirement in practice, sole retainment of encryption keys by the data exporter without access of the hosting service provider would actually create a different, much more likely risk than unauthorized access to the data by public authorities. Despite the implementation of detailed key management policies and other safeguards, human mistakes which lead to the loss of the encryption key and thus the loss of data are likely to occur. Without additional key management by the hosting service provider the loss of data will be final and could create a data breach that is both harmful to the data exporter and the data subject.

An alternative to the requirements described in Use Case 1 would be to allow key management by the hosting service provider and implement other additional measures. Such a measure could be the immutable logging of all accesses to the key management system and enabling direct access to the logfiles for the data exporter. This would allow the data exporter to identify cases of unauthorized access to the data and take countermeasures. It would further serve as deterrence to third parties since access cannot happen secretly. While this alone does not remove all risks, it can minimize them and guarantee an adequate level of data protection even in situations like Use Case 6 wherein processing of data in the clear is necessary,

provided that it is complemented with other (technical, contractual or organizational) measures.

Berlin, 21.12.2020