Position Paper

# Response to EDPB consultation on recommendations 01/2020 on measures that supplement transfers tools to ensure compliance with the EU level of protection of personal data

| | | | |
|---|---|---|---|
| Our reference: | COB-DAT-20-105 | Date: | 21 December 2020 |
| Referring to: | EDPB consultation on Recommendations 01/2020 on measures that supplement transfers tools to ensure compliance with the EU level of protection of personal data | | |
| Contact person: | Áine Clarke, Policy Advisor, General Insurance | E-mail: | Clarke@insuranceeurope.eu |
| Pages: | 7 | Transparency Register ID no.: | 33213703459-54 |

## General comments

Insurance Europe welcomes the opportunity to provide input to the European Data Protection Board's (EDPB) consultation on draft recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. The 16 July 2020 Schrems II judgement cast uncertainty over the future of personal data transfers outside of the EU, which many insurers rely on to conduct their day-to-day business activities.

The draft EDPB recommendations present a roadmap of six steps that data exporters can take to assess whether there is a need to implement supplementary measures to ensure that data transferred to third countries are afforded a level of protection equivalent to the General Data Protection Regulation (GDPR). The EDPB recommends following the steps in the order in which they are presented, as arriving to certain conclusions under some of the steps waives the need to proceed with the others. The recommendations also provide a non-exhaustive list (Annex 2) of examples of the supplementary measures that can be put in place if deemed necessary by the data exporter, including technical measures (use cases 1-7), additional contractual measures, and organisational measures. While the draft recommendations offer clear steps and examples of use cases, they do not give due acknowledgement to the considerable effort involved with many aspects of the assessment of the data transfer and possible implementation of supplementary measures (including the requirement for case-by-case analysis of data transfers), and the burden this places on individual companies. Insurance Europe therefore believes that the recommendations should be radically revised, and the following points considered:

- Uneven application of the GDPR

The draft recommendations place a very large responsibility on individual data controllers within the EU. They must carry out assessments regarding the law or practice of the third country (step 3), identify and adopt supplementary measures (step 4), take formal procedural steps (step 5) and re-evaluate the level of protection afforded (step 6). However, while it is reasonable to assume that most controllers will possess the will to follow this procedure, it is very unlikely that they will be in a position to carry out the steps in the correct way, as they will not possess the means to do so. This issue relates primarily to steps 3 and 4 where, even with these recommendations in place, there will be a great degree of ambiguity around what is actually required to meet the requirements in Chapter V GDPR.

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

Paragraph 69 of the recommendations accurately captures this ambiguity: selecting supplementary measures from the non-exhaustive list in Annex 2 will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. As a consequence, the legal vacuum mentioned (but perhaps wrongfully rejected) by the European Court of Justice in C-311/18 p. 202 is becoming quite apparent and there is reason to believe that the application of the drafted recommendations will be neither uniform nor correct. For similar transfers, it is reasonable to expect that controllers will draw different conclusions on how to ensure compliance with the GDPR. For example, controller A might assess that the legislation in the third country may not impinge on the effectiveness of the appropriate safeguards, while controller B might assess that it may and adopt supplementary measures, and controller C might assess that there are no supplementary measures that can bring the level of protection up to the EU standard of essential equivalence. From a regulatory perspective, and given the objectives of the GDPR, this would not be a satisfactory outcome and considering the draft recommendations in full, it is questionable if these would fulfil the main purpose – which is to give guidance.

If the data controller is not able to assess the legislation of a third country as regards the existence of provisions granting access by public authorities to data for supervision purposes, then, under the draft recommendation, the data controller will be obliged to suspend or terminate the transfer of personal data to a given third country or bear the cost of commissioning such an analysis: eg prepared by a specialized entity (law firm). At the same time, the supervisory body may evaluate the actions taken by the controller and, regardless of the risk-based assessment documented by the controller, the supervisory body may suspend or prohibit the transfer of data in cases where, as a result of an investigation or complaint, it finds that it is impossible to provide a substantially equivalent degree of protection. A situation in which the provisions of the law of a third country will be interpreted differently, be it by an entrepreneur or a supervisory authority, does not result in the consistent application of the GDPR.

- A task equivalent to an adequacy assessment

Fulfilling the requirements laid out under step 3, particularly if a risk-based approach is not adopted, would effectively amount to carrying out an assessment similar to that which the European Commission conducts when preparing for the adoption of an adequacy decision with a third country – the main mechanism for transfers of personal data to third countries, according to Article 45 of the GDPR. When assessing the adequacy of the level of protection of the third country, the Commission shall consider elements from Article 45(2), some of which are: the rule of law; the respect for human rights and fundamental freedoms; relevant legislation; the access of public authorities to personal data; data protection rules; case-law; effective and enforceable data subjects rights; and effective administrative and judicial redress for the data subjects. According to the draft EDPB recommendations, controllers within the EEA will, when fulfilling their obligation to provide appropriate safeguards in line with Article 46, in practise be obligated to carry out similar assessments as the ones the Commission carries out in line with Article 45, considering more or less the same elements. However, most of these elements are not mentioned in Article 46, which could be seen as an expression of the European Parliament's and the Council of the EU's (the co-legislators) view that assessments regarding such elements should be an activity exclusively carried out by the Commission, and not by controllers. This point must be considered by the EDPB, and revised accordingly, or else it will amount to placing a new obligation on entities (obligation to locate and process data in the EU), which is not provided for under the GDPR.

- Alignment of initiatives

Currently, two different bodies of the European Union are drafting texts that aim to ensure compliance when personal data is transferred to third countries (the Commission's implementing decision on standard contractual clauses (SCCs) for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council *and* the European Data Protection Board recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data). Looking at the draft versions of these texts, it is unclear how they relate to each other. For example, Article 1(1) of the implementing decision suggests that with the SCCs set out in the Annex in place, appropriate safeguards within the meaning of Article 46(1) GDPR is provided. However, according to the recommendations, emphasis is put on assessing on a case-by-case basis, without

acknowledging the need for a risk-based approach (which contrasts with the approach taken in the draft SCCs), if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tool (referred to as step 3 in the recommendations) and to identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence (step 4 in the recommendations). Currently, the wording of Article 1(1) suggests that the SCCs in the Annex is sufficient to ensure compliance with Article 46 GDPR. The wording of the recommendations needs therefore to be adapted to the implementing decision.

- Risk-based approach

A risk-based approach must be permitted when assessing the level of data protection in the third country and choosing to implement supplementary measures. As the EDPB states, effective supplementary measures must be identified on a case by case basis (paragraph 46). However, the EDPB also states in paragraph 42 that, for the assessment of the level of data protection in third countries, only objective factors should be considered, while subjective factors, such as the likelihood of public authorities accessing the data, should not be relied on. This exclusion of subjective factors is not justifiable. The EC has emphasised on several occasions that the risk-based approach also factors into the risk assessment when evaluating the level of data protection in third countries. In its draft implementing act on updated SCCs 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 pro-cessing 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 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, it would amount to the EU demanding a level of data protection from other countries that goes beyond the one guaranteed by the GDPR.

- Data transfers in the insurance sector

The recommendations list a number of "scenarios in which no effective measures could be found" (p. 26). The list of scenarios includes a situation where a data exporter uses a cloud service provider or other processor to have personal data processed according to its instructions in a third country (paragraph 88-89). It is precisely this kind of data transfer – to a cloud service provider in a third country, for example, the US (ie, the use of Microsoft, Google or Amazon services, as well as other, less popular, solutions used in the industry) – which is one of the most widespread data transfer situations used by insurers (See the European Insurance and Occupational Pensions Authority (EIOPA) guidelines on outsourcing to cloud service providers here). However, the recommendations do not solve the issue with such transfers, since cloud services which allow data encryption or complete anonymization or pseudonymization on the customer's side are almost never used in the industry. Rather, almost all cloud services which are used are cloud services where the service provider processes data by accessing them. The recommendations therefore do not provide any guidance as to how insurers can use the most popular cloud services while ensuring that data transfers are in line with the requirements of the GDPR and the findings of the Schrems II judgment.

Furthermore, a ban on data transfers to the US would, if taken to its logical conclusion, amount to a blanket ban on all transfers outside the EU (as there are many cases of sub-contracting by secondary sub-processors). In order to avoid such a general ban, all data would have to be systematically encrypted or anonymized, which could then prevent the provision of the service sought. The EDPB should also take into consideration that, to date, very few European providers are able to provide the same services as those located outside the EU (in particular the USA). However, the tools and solutions offered by providers outside the EU are truly indispensable to the business of their clients, who have widely deployed these tools in their IT systems. Therefore, in order to ensure the continuity of insurance services (among many other industry services), it is crucial that the EDPB provides concrete recommendations on ways in which insurers can continue using the most popular and widely used cloud services, which are necessary for their day-to-day business activities.

- Binding Corporate Rules (BCRs)

According to paragraph 59 of the recommendations, the precise impact of the Schrems II judgement on BCRs is still under discussion. In this context, we argue against requiring additional commitments in the BCR's themselves, given that the ECJ did not make any deliberations that would question the validity of existing practices concerning BCRs. 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. Establishing additional requirements which would apply to all members of the group regardless of the specifics of intragroup procedures, interactions, data transfers and the country of their establishment is therefore neither an appropriate nor reasonable approach. Instead, additional requirements and/or supplementary measures should be arranged and implemented separately and on a case by case basis depending on the particular data transfer.

## Comments on specific paragraphs

### 1. Accountability in data transfers

*Paragraph 3:*
It is questionable if the principle of accountability according to Article 5(2) GDPR applies in relation to the data subjects or the general public. A controller who fails to (for example by choosing not to) demonstrate compliance with Article 5(1) in relation to a data subject or the general public (but complies with the provisions on data subjects' rights in Chapter III) would probably not infringe the principle of accountability. Instead, the principle of accountability should be interpreted in the light of the general obligation to cooperate with the supervisory authority according to Article 31. Therefore, this principle would only be applicable in relation to the supervisory authority (ie the "burden of proof" only exists in relation to the supervisory authority).

**Recommendation**: If the current wording in paragraph 3 regarding Article 5(2) is an expression of the EDPB's view on how far-reaching the scope of the principle of accountability is, this view should either be developed further in these recommendations or be subject to a clear reference (to other EDPB guidelines, decisions from the authorities, court rulings or any other legal source).

### 2. Roadmap: Applying the principle of accountability to data transfers in practice

#### 2.2. Step 2: Identify the transfer tools you are relying on

*Paragraph 25*
Under step 2, the recommendations provide for the use of derogations according to Article 49 GDPR, however only in the case of *"occasional and non-repetitive"* transfers. This is expanding the prerequisite from what the EDPB have previously held in its guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 and goes beyond the wording of Article 49 but also goes further than recital 111 of the GDPR that set a pre-requisite only regarding 49.1 b, c and e.

**Recommendation**: Ensure that recommendations 1/2000 do not go beyond existing guidelines and the GDPR.

#### 2.3. Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer

*Paragraph 37 (and 138):*
The current wording of this paragraph suggests that controllers within the EU must, in practice, interpret the EU Charter of Fundamental Rights when conducting their normal business activities. The charter is primarily a legal act that applies to, and should be interpreted by, the institutions of the European Union and its member states. In addition to using the charter as a reference, controllers will also be recommended to refer to the non-exhaustively sources mentioned in p. 138 (for example, resolutions and reports from intergovernmental organisations, other regional bodies, UN bodies and agencies and reports from academic institutions). Generally, controllers would lack the prerequisites of "using" the charter, and many of the sources mentioned in p. 138, as a reference to their assessments.

**Recommendation:** The recommendations in paragraphs 37 and 138 should be reconsidered**.**

*Paragraph 42:*
The recommendation that exporters assess legislation other than what is publicly available is unfeasible in practice. Furthermore, this paragraph would apply in situations where the legislation in a third country "may be lacking", a term which is very unclear.

**Recommendation: Further develop when this would be the case. For example, is the legislation lacking in situations where the legal requirements that govern public authorities' access to data or on enforceable rights and effective legal remedies, are vague? Or is the legislation only lacking when it is partly or in full covered by secrecy?**

### 2.4. Step 4: Adopt supplementary measures

*Paragraph 48:*
The parenthesis in this paragraph mentions the data importer's obligation. SCCs could indeed impose obligations on the data importer, but the obligation according to GDPR to ensure that transfers are subject to appropriate safeguards (in practice, to ensure essential equivalence) would primarily be an obligation of the data exporter.

**Recommendation: Clarify paragraph 48.**

### 2.5. Step 5: Procedural steps if you have identified effective supplementary measures

The obligation to systematically notify the national data protection authority of the stop of export of data outside the EU is very cumbersome. Under these requirements, national data protection authorities would have a mapping of the providers with which data exporters conduct business, which goes far beyond the control of the implementation of a compliance approach, which is the guiding principle of the GDPR.

**Recommendation: Review these obligations in line with the approach to compliance under the GDPR.**

## Annex 1: Definitions

The definitions in Annex 1 on the crucial concepts of *data exporter* and *data importer* should be reviewed. Regarding the concept of a data exporter, it is questionable if a processer in the EEA who transfers personal data to a third country on behalf of a controller in the EEA should carry out assessments and, if need be, put in place supplementary measures. Instead, this would be an obligation of the controller. Regarding the concept of a data importer, all data importers will not assume the role as a controller or processor according to Article 4(7) or 4(8) with obligations under the GDPR.

**Recommendation: The following alternative definitions should be considered:**

- "Data exporter" means the controller within the EEA responsible for the transfer of personal data to a data importer in a third country (with or without the engagement of a processor or sub-processor within the EEA involved in the transfer).
- "Data importer" means the controller, processor, recipient or third party in a third country who receives or gets access to personal data transferred from the data exporter.

## Annex 2: Examples of supplementary measures

- *Use case 2: Transfer of pseudonymised Data*

When data is pseudonymised in the way described in use case 2, and the information to revert the pseudonymisation is held exclusively by a data exporter, it is questionable if the provisions in the GDPR will be applicable to *the transfer*. Example 13 in the Opinion 4/2007 on the concept of personal data (01248/07/EN, WP 136, p. 15 and 16), suggests that *personal data* will not be transferred in such a situation (the importer will receive data but not personal data).

**Recommendation: Use case 2 should be reviewed by the EDPB in light of opinion 4/2007.**

- *Transparency and accountability measures*

*Paragraph 127:*
GDPR contains a series of provisions on communication to data subjects (for example in Chapter III on data subjects' rights and in Article 34 regarding personal data breaches). However, there are no provisions in the GDPR that relate to the obligation to provide the mentioned records. When public authorities within the EEA request access to personal data processed by controllers in the EEA, the controllers could be prohibited by national legislation (see Article 23) to communicate the disclosure to the concerned data subjects. The same could be true for disclosures of personal data to an authority in a third country (for example when a crime fighting authority within the EEA requests an authority in the third country to collect the data from the data importer).

**Recommendation**: This paragraph should be reviewed.

*Paragraph 131:*
This paragraph contains the concept of *unauthorised access*. This concept is also used in some of the more central provisions in the GDPR (Articles 4(12), 5(1)(f) and 32(2)). One of these provisions holds the definition on *personal data breaches*. Simplified, if someone would gain unauthorised access to personal data, a personal data breach has occurred.

If a public authority in a third country would gain access to personal data transferred by a data exporter in the EEA, it is questionable if the access should be seen as *unauthorised* even if the access goes beyond what is necessary and proportionate in a democratic society *according to EU-standards*. When the access, by all accounts, is considered to be acceptable to the standards in the third country, for example when a public authority is entitled to the data according to national legislation, perhaps the access should not be seen an unauthorised (that would be the case when a public authority within the EEA gets access to data when it is entitled to it according to national legislation in a member state).

**Recommendation:** If the concept of unauthorised access will be used in the final version of these guidelines, the EDPB should express its view on why, or to what extent, an access to personal data that a public authority is granted according to national legislation in a third country should be seen as unauthorised and if it could give rise to personal data breaches that a controller in the EEA must assess according to Articles 33 and 34 GDPR.