21 December 2020

EBF_043812

# EBF response to the European Data Protection Board's consultation on the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

## KEY POINTS

- The European Banking Federation (EBF) welcomes the opportunity to respond to the European Data Protection Board's (EDPB) consultation on its Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
- While we welcome the EDPB's work to help resolve the uncertainty which has followed the CJEU Schrems II judgement and particularly the use of standard contractual clauses by data exporters, we are concerned on **the substantial burden placed on the data controller** to **assess the adequacy of the level of protection afforded to personal data from the EU of the jurisdiction to which it is being transferred**. This creates an immediate risk of fragmentation from differing assessments by companies and subsequently, to different actions from DPAs. **Practical tools, which provide a uniform starting base for data exporters and help them conduct these assessments, are needed.**
- The **lack of a proportionate and risk based approach in the Recommendations**, which seem to be based on the assumption that the level of risk to data subjects **depends *solely* on the law in the recipient country**, and *not at all* on other factors. The proposed technical measures and Use cases 6 and 7 are particularly concerning.
- The Recommendations should incorporate **proportionate and risk based approach to transfers,** which takes into account, for example, **the type of data (normal/sensitive data), the risk for the data subject, the, level of security of data transferred and the likelihood of inappropriate interception by local authorities**.
- A **meaningful grace period is vital** to allow **for a sufficient period of time to elapse to enable businesses to implement the relevant procedures and measures.** A case by case assessment of transfers, determining the relevant

**European Banking Federation aisbl**

**Brussels /** Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
**Frankfurt /** Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
**EU Transparency Register /** ID number: 4722660838-23

**www.ebf.eu**

supplementary measures (if step 4 is required) and making the necessary changes requires a lot of time, human and financial resources and involves many parties.

The European Banking Federation (EBF) welcomes the opportunity to respond to the European Data Protection Board's (EDPB) Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection and personal data. Below are both general and detailed comments on the document, and an Annex which includes detailed comments on the Use Cases in the Recommendations.

As a preliminary comment, the EDPB draft Recommendations **add new, very detailed provisions to the text of the General Data Protection Regulation (GDPR)[1],** which already **frames international data transfers** with clear and well-defined provisions.

The proposed Recommendations **create new obligations towards data exporters and importers,** using very prescriptive wording ("must"), which will mislead the parties involved into considering them mandatory. The non-legally binding nature of the EDPB's recommendations should be stressed in the document instead.

According to the GDPR, the EDPB is entrusted with the task to issue guidelines, recommendations, and best practices for the purpose of further specifying the criteria and requirements for the personal data transfers under Article 49**. It is not entrusted to design a new framework with a set of detailed and binding obligations.**

By doing so, the **EDPB goes far beyond its competencies since it has no authority under the GDPR to create legal obligations upon data exporters or importers.** Creating legal obligations falls in the sole remit of the European co-legislators i.e., the European Parliament and the Council, according to the Treaty of the Functioning of the European Union.

## 1. INTRODUCTION

Overall, while EBF members **welcome the EDPB's work to help resolve the substantial legal uncertainty** that has followed the Court of Justice of the European Union (CJEU) Schrems II judgement, especially regarding the conditions under which standard contractual clauses (SCCs) can be used for data transfers, **EBF members have significant concerns with regards to the published guidance, notably on:**

- **The substantial burden placed on the data controller** to assess of the adequacy of the level of protection afforded to personal data from the EU of the jurisdiction to which it is being transferred. This represents a shift in responsibility for assessing adequacy which is a public task, to private companies. The Recommendations and the considerations also **seem to equate this assessment with that of the adequacy assessment under the GDPR, which is conducted by a public body (the EC).** We would also like to remind that the CJEU ruling noted that the DPA also has a task in the assessments[2]. Recognizing however that the requirement for data exporters to conduct an assessment draws from the CJEU Schrems II judgement, we would strongly recommend the EDPB and European Commission to provide practical tools to help do so.
- **The immediate risk of** legal **uncertainty and fragmentation** due to potentially diverging assessments by different data exporters and importers **of the same third country jurisdiction.** This would also go against the **purpose to protect**

[1] For example, the requirement to notify the supervisory authority if importer is unable to comply with the commitments taken in the Article 46 GDPR transfer tool (Paragraph 53) is not introduced in the GDPR.
[2] 3 C-311/18 (Schrems II), paragraph 134.

**the data subject's rights and could result in different levels of protection to data subjects which goes against the GDPR.**

- The **lack of a proportionate and risk based approach in the Recommendations** with measures that are flexible enough to be adaptable in a business setting. This is **apparent in the proposed technical and to a certain degree contractual measures in Annex 2** where there is disparity between real world practices and operations' of banks and could impact the provision of services to clients. The Recommendations also **do not seem to take into account the proportionality principle envisaged by the GDPR**. In fact, the Recommendations seem to be based on the assumption that the level of risk to data subjects depends *solely* on the law in the recipient country, and *not at all* on other factors, such as the categories of data subjects involved (e.g., minors, employees, more vulnerable subjects; etc.) and the nature of the personal data transferred (e.g., contact data, sensitive data, bank data, etc.). This is evident in particular in Use Cases 6 and 7.
- The significant impact of such guidance on the business, organisation, and the **day-to-day process of companies** - especially international ones – taking into account the existing situation of such companies and the technical impossibility on implementing such guidance in the short to medium term. Section 4 includes some examples of how the technical measures proposed would make day to day processes and operations challenging.

To address these concerns, we recommend:

- To incorporate **a proportionate and risk based approach to transfers,** which takes into account, for example, the type of data (normal/sensitive data), the risk for the data subject, the level of security of data transferred and the likelihood of inappropriate interception by local authorities.
- To **build more flexibility** into the supplementary measures proposed in the Recommendations.
- For the EDPB and European Commission **to provide data exporters with practical tools** to be in a position to complete the assessments mandated by the CJEU **in a consistent way that limits the fragmentation between EU countries as much as possible**. In Section 3 below, we include several recommendations for practical tools such as providing a country by country legal risk analysis (starting with priority third countries).

**We encourage DPAs to play a more active role in helping exporters/controllers to make the assessment of third country legislation.** An example of such a more active role would be that they furnish basic essential and uniform information on the relevant matters that should be looked at when verifying the risks of a data transfer, while also keeping in mind the need for collaboration with other DPAs in Europe for a coherent approach.

## 2. KEY CONCERNS

### a) The burden on data exporters to conduct the adequacy assessment and the risk of fragmentation

i. The **administrative burden and the economic impact** on EU data exporters/controllers having to conduct the case by case assessments for each

transfer with the considerations laid down by the EDPB (e.g., paragraphs 42 and 43), the legal and operational expertise this would entail, and then continually having to review the transfer would be significant. If a large multinational bank would struggle with this task, smaller banks or SMEs more generally **would face difficulties in terms of resources and expertise to monitor, on an ongoing basis, whether developments in the third country that could impact the initial assessment made by the controller (Paragraph 62).**

ii. EBF members also express concern on the recommendations regarding the assessment of **legislation on public authorities' access to data, notably whether it can be justifiable or not in light of national security reasons.** Paragraphs 36, 38, 42 and 43 of the Recommendations are **very vague**, and lack sources to look to assess if the requirements of public authorities in the third country "are limited to what is necessary and proportionate in a democratic society."

How is a private company supposed to assess if a regulation **is necessary and proportionate in a democratic society?** Furthermore, the EDPB encourages companies to rely on Article 47 and 52 of the EU Charter of Fundamental Rights. **Are data exporters/controllers supposed to assess the fairness of a third country's justice system and to conduct legal and political assessment as well as taking a view on the public authorities' powers in third countries and their level of interference with the rights to privacy/data protection?** This does not seem appropriate.

Ultimately, a geopolitical problem of the different levels of data protection in the world will be placed solely in the hands of individual companies, and global networking in data processing will be ignored.

Placing the obligation on data exporters/controllers to review **and reach a decision on the essential equivalence of a third country legal regime** with that of the EU, in the context of data protection, and the availability of legal remedies to data subjects in such third countries **will inevitably result in a lack of uniformity and legal uncertainty for controllers.**

Every group/entity, from **multi-nationals to SMEs are tasked with undertaking a legal review of the surveillance laws of third countries which may not be readily known, drafted in a different language, opaque, and subject to laws of which the data exporter has no knowledge.** The review of the legal regimes of, for example, the United States, India, Russia, South Africa, and Turkey **will be replicated thousands of times with potentially wildly differing conclusions.**

The result is a responsibility on the part of the data **exporter that is disproportionate and that goes beyond the accountability principle** and an inevitable information asymmetry between data exporters, with consequent damage to legal certainty.

We therefore warn of the consequences of putting the responsibility for conducting the assessment of third country legislation, which the Recommendations appear to formulate as that equal to the same level of the adequacy assessment under the GDPR and taking a view on the powers of public authorities in third countries and their level of interference with the rights to privacy and data protection on the shoulders of exporters/controllers, effectively making it a support function to analyse legal and political systems. This points to a shift of responsibility from the public to the private sector which, crucially, does **not foster economic and legal**

**certainty for companies when it comes to international data transfers and, as a result, for the digital economy as a whole.**

It would be preferable if the European Commission were **to undertake to determine whether a third country regime is essentially equivalent to the EU regime in the context of personal data or not.** This is the best way in which the European Commission can safeguard the personal data of EU citizens. However, recognizing that the requirement for data exporters to perform the assessment stems from the CJEU judgement, **practical tools** are needed from the European Commission and the EDPB to help them do so. Without tools or common information that provides a uniform starting base for companies, the risk of fragmentation is high, as well as that to the data subject.

iii. Under the GDPR, it is the responsibility of the European Commission to assess the adequacy of the level of data protection for a jurisdiction and it is crucial to keep **the hierarchical structure of data transfer mechanisms on which Chapter V GDPR is based**. We understand that the GDPR traditionally required the data exporter to first consider whether the third country provides an adequate level of protection under Article 45 GDPR (adequacy decision provided by the EC is based on a deeper and broader investigation of a third country's entire legal system of the country of the third party).

Where there is no adequacy decision, which implies that i) either the assessment of the entire legal system of the third country is not performed yet by the EC or ii) the assessment provided by the EC is negative, the data exporter can use adequate safeguards under Article 46. **If companies shall use adequate safeguards of Article 46 only with countries considered as "adequate" then, the hierarchy between mechanisms introduced by Article 45 and Article 46 will not be clear anymore for companies.**

Further to this, under the Recommendations EU data controllers or processors are required to implement the supplementary measures described in Annex 2, **even if the third country is covered by an adequacy decision pursuant to Article 45 of GDPR** (see paragraph 71 and 78). This is another instance of how the established framework under the GDPR for international data transfers is called into question, together with the egal certainty for controllers and processors, if relying on this transfer mechanism. Therefore, we would recommend to delete this provision. **Maintaining it would mean a continuing lack of clarity on what is expected from the data exporter**.

Finally, with this shift of responsibility, **comes the huge risk of deadlock and fragmentation** (and a risk of ongoing litigation and legal uncertainty). Data exporters/controllers might come to different interpretations creating potential risks or distortion of competition **and, notably, differing protections for the data subject.** Furthermore, what will be expected from exporters/controllers when the EDPB/DPA, having reviewed specific transfers within a company for a specific situation, finds a jurisdiction inadequate and no risk mitigating measures can be put in place. Are DPA's to notify all other controllers and they would then be expected to stop their own data transfers to that jurisdiction?

### b) The need for a more proportionate and risk based approach

The GDPR proposes at various occasions **the implementation of a risk-based approach, especially with respect to Article 32 GDPR.** Tied to Step 4 in the Recommendations, the idea that an entity cannot send the name or email address to another entity or a third party in a third country under the SCCs unless it is first encrypted

in transit and at rest (because the third country is not essentially equivalent) in order that encryption takes it outside of the reach of the relevant public authorities in these countries **does not acknowledge either the commercial context in which companies operate and personal data is transferred or reflect the risk based approach which runs through the GDPR**.

Similarly, the Recommendations **do not seem to allow firms to consider the *nature of the data and the corresponding risk*.** Although disclosure of any personal data to authorities poses some degree of risk to individuals, **these risks are clearly greater for some types of data than others.** For example, simple contact details of employees or other data subjects do not pose the same level of risk to individuals as special category data. Differences should be reflected in the Recommendations.

The Recommendations also conflict with Section 1 of the Guidance on Accountability which recognises that "*…. the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*". The EDPB states correctly that "*Controllers and processors must seek to comply with the right to data protection in an active and continuous manner by implementing legal, technical and organisational measures that ensure its effectiveness*". However, this does not fully align with the GDPR text, **which includes the word "appropriate**". **The "appropriateness" of such measures requires an assessment of risks and the consideration of several factors, including the likelihood of something occurring**. This "likelihood test" is inherent GDPR Articles 24, 25 and 32, as well as in concepts in the GPDR such as:

- "High risk processing" – processing that is likely to cause harm to data subjects;
- "Pseudonymisation" - where the likelihood of the combination of data with other data sets is key to determining of the suitability of pseudonymisation technics; and
- Triggers for breach notification - the likelihood of harm.

This adequately reflects the reality of the individuals and controllers in an increasingly digital, fast developing, and international business environment and provides the necessary flexibility.

This risk-based approach should also take into consideration the enforcement risk of surveillance laws in third countries, **in the light of the context of the transfer** (such as nature, amount and duration access to the data). More specifically, **it should be possible to assess the probability that specific personal data are really accessed by "unauthorized" state officials in the course of enforcing surveillance laws** (such as FISA Act Section 702) that would only theoretically allow the access to these data. In many cases the application of such approach would result in a low risk (see U.S. Gov. White Paper "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II", issued September 2020) and therefore would give the industries a realistic chance to keep their businesses up and running.

### c) The significant impact of such guidance on the business, organisation, and the day -to -day activities of organisations

The current Recommendations and the limitations that they might create will have a huge impact on the existing operations and business of private companies, especially international corporations. As shown in the practical examples in Section 4 below, it will have immediate effect on some core activities, **namely transverse processing such as HR or compliance processing or global business activities – such as large corporate activities - supported by global platforms.**

In this context, the use cases described in the guidance **are too broad and do not cover the reality and complexity of the different activities**, posing difficulties in terms of implementation in the short to medium term. There is also no consideration of situations where the data controller/exporter may have limited control **as most products have pre-built settings and off the shelf terms and conditions.**

### d) Proposed examples of technical, contractual, and organisational measures in Annex 2

#### i. Technical measures

Members note that several of the **technical measures** proposed do not factor in the necessary flexibility or reflect how banks conduct day to day operations **in a risk managed way** – both internally and with clients – including the relationship with ICT service providers.

For example, the use of pseudonymisation, and encryption does not consider that, in many cases, **this may not be possible due to the requirements of the counterparty receiving the data or due to the products/services that banks are using from external suppliers.** The counterparty might not be able to technically provide the requested service for the bank if the data is pseudonymised or encrypted, for example.

Encryption is essentially (leaving aside pseudonymisation) the only supplementary measure which could elevate a transfer from the EU to the US under the SCCs to essential equivalence status **but there is no recognition as to how the transfers or processing takes place in practice.** The suggestion appears to be that: (i) the personal data is encrypted in transit; (ii) remains encrypted at all times whilst in the US; and (iii) the encryption keys remain within the EU based exporter. **The reality is that, in most cases, the personal data is transferred to enable the data importer to *actively* process the personal data which means that for the vast majority of cases encryption will not be a panacea.**

As a result, where data exporters conclude that there are no third countries (other than those who have been deemed adequate by the EC) which are essentially equivalent and personal data is to be transferred to a data importer in the third country to enable that data processor to actively process (and not just store) that personal data, **the data exporter is effectively prohibited from transferring that personal data outside of the EEA other than to a country deemed adequate by the EC.** If this is the result/intention of the EDPB it brings **companies back to Step 3 and necessitates that the EC provide more meaningful direction as to whether or not countries A, B, and C are essentially equivalent (and/or rule them as adequate) or not.**

Therefore, Use Cases 6 and 7 in the Recommendations are worrying as they do not include elements of flexibility, **seeming to shut down the possibility of any transfers** in the cases, even when it would be technically necessary for the provision of a service. Flexibility is also required with regards to *when* transfers (especially existing ones) must be suspended – **as ceasing operations overnight, without adequate time to examine the specifics is unrealistic from a technical feasibility perspective and the aspect of continuing to provide critical financial services, which would be against the interests of EU individuals.**

***Please see Annex 1 for detailed comments on the different use cases presented in the Recommendations.***

### ii. Contractual measures

Members also have reservations on the proposed additional **contractual measures.** For example, paragraph 105 and the **question of audit rights** whereby *"a data exporter could reinforce its power to conduct audits or inspections of the data processing facilities of the importers, on-site and /or remotely, to verify if data was disclosed to public authorities and under which conditions".* The suggested measures and the conditions for effectiveness, **do not take into account the imbalance in the negotiating power between banks on one hand and large technology providers (for example, large cloud service providers) on the other**. In practice providers are reluctant to negotiate such a broad audit rights.

In another example, regarding Paragraph 112, it is uncertain, or even impossible that an importer can oppose a refusal to provide information to a public authority if it receives a subpoena/requisition. **It would be difficult for the controller to include the provisions outlined in the data processing agreement**. Banking institutions and a data importer in a data transfer agreement are not likely to question a government's binding request for access to data.

### iii. Organisational measures

The proposed organizational measures include internal policies for data transfer governance especially within "groups of enterprises" (see Paragraph 124 p. 35). Such policies should provide clear allocation of responsibilities, reporting challenges and procedures for responding to government access requests. According to the EDPB, these could include the appointment of EU-based teams to assess and respond to government access requests, procedural steps to challenge unlawful or disproportionate requests, as well as transparency to the data subject.

We have three main concerns on these recommendations:

- This aspect is **too prescriptive.**
- Companies should **be free to decide their own organization and procedure** regarding the **management of data transfers.**
- Especially in the financial sector, which is already subject to heavy regulation **there are governance and policies in place for all activities, including personal data protection**.

## e) The Recommendations and their effect on the draft Standard Contractual Clauses for international data transfers

The Recommendations also raise questions **with regards to the status of the draft SCCs for international data transfers** published by the European Commission in November. **The SCCs already oblige to show the measures to be adopted by the data exporter and importer**. **Do the Recommendations consider the measures mentioned in the SCCs insufficient?** Are the SCCs to be considered only as the starting point and that on top of them "the additional measures" of the EDPB need to be implemented? The lack of alignment is a concern for members. There are several points from the approach in the SCCs which could be incorporated into the Recommendations, notably that the **controller should do *a holistic* assessment of risk and then put in place safeguards that correspond**. As mentioned above, the Recommendations seems to suggest that if a third country's surveillance laws do not meet European standards, **no**

**personal data of EU individuals should be stored there in the clear, irrespective of the real, practical risk involved.**

### f) Additional considerations

In addition to the points above, we would like to flag the following with regard to the Recommendations:

- We **welcome and are encouraged** by the **definition of a "data exporter" in Annex 1, which includes the controller or processor** within the EEA who transfer personal data to a controller or processor in a third country. We would however welcome a clarification whether the data exporter is responsible for compliance with the provisions set out in the Recommendations, or if, on the contrary, the responsible is the data controller that has appointed the data exporter.
- We are concerned about **the interpretation on the use of Article 49**, specifically that the derogations contained therein must be interpreted restrictively. There is **no legal basis** for this extended interpretation.
- We would like to remind that the CJEU Schrems II judgement **did not include anything on data localisation**. The implementation of the Recommendations should not result in a de facto obligation to keep data within Europe.
- As regards **BCRs**, we understand from Paragraph 59 that "*The precise impact of the Schrems II judgment on BCRs is still under discussion. The EDPB will provide more details as soon as possible as to whether any additional commitments may need to be included in the BCRs in the WP256/257 referential*". Should any additional commitments be requested to be included in existing BCRs **it should be clarified that these amendments will not require any validation process by the lead DPA other than sending an updated version of the BCRs to such DPA for information.**
- Regarding **the notification (promptly) to "*the data subject of the request or order received from the public authorities of the third country***, *or of the importer's inability to comply with the contractual commitments, to enable the data subject to seek information and an effective redress…*". **It would be extremely difficult to provide such a notification to clients**. Certain requests from foreign authorities are linked with the local activities of a company whose headquarter is in another territory. The third country authority would like to ensure that the company is compliant with obligations resulting from local laws and regulations. In that case, **the notification of the foreign authority's request is not useful, and it is not possible for the company to refuse providing information if the objective is to be able to continue its activity there.**
- In paragraph 100, a range of considerations are listed. We suggest that these are **more relevant at the stage of conducting due diligence**, rather than the **contractual stage.**
- The example of paragraph 110 suggests requiring the importer to regularly publish a cryptographically signed message, informing the exporter that no order to disclose personal data from public authority has been received (so called "Warrant Canary" method). We believe that this form of passive notification is unlikely to be applied in practice by data importer, even if the conditions for effectiveness will be met. See section 3 for a recommendation to help render the Warrant Canary method meaningful.

- The EDPB points out that there is a transfer under the GDPR even in the event that personal data is accessed from a non-EEA country (Paragraph 13). On this basis, it would be helpful to clarify **whether even the mere possibility of accessing personal data from countries outside the EEA in specific circumstances** (e.g., in an emergency with consequent impossibility of access from countries within the EEA) constitutes a transfer of personal data pursuant to the GDPR.
- We are concerned by the fact that Paragraph 118 is **not in line with Articles 13 and 14 GDPR,** stating when and if the data subject shall be informed of his/her data processing. This paragraph also **contradicts national laws in certain cases**[3].
- Paragraph 75 states that public authorities in third countries may endeavour to access transferred data: (a) in transit by accessing the lines of communication used to convey the data to the recipient country. This scenario is also described in Use Case 3 (paragraph 84). This means that potentially, the controller should always know the route travelled by the network flows. Considering that the network flows do not run across fixed "routes", **but the routes made are dynamically adapted**, from time to time, to the network load and through several network "nodes", we believe that knowing the routes made by TLC companies is quite unlikely, other than difficult. Therefore, we would welcome the EDPB to provide further criteria on how to verify the paths made by the data in transit and the route crosses third country.

## 3. RECOMMENDATIONS

To address the concerns raised above, EBF members propose the following recommendations:

1. First, we recommend the EDPB **to incorporate into the Recommendations a risk based approach to data transfers,** we also encourage the EDPB to build flexibility into this approach and to all the example measures, subject of course to diligent record keeping by controllers to record their reasoning. For the moment, the supplementary measures, and Use Cases such as 6 a 7 in the Annex, which already preclude certain situations, do not reflect a risk based approach or the different situations faced by businesses in their day to day activities.

   **A holistic risk-based approach would include:**

   - **Taking into account the level of security depending on the type/number etc. of data transferred and providing the company a margin of discretion in this respect.**
   - Recognizing that the **data type should be a factor in risk assessments.** Stricter safeguards could be needed for transferring higher risk data, with reliance solely on SCCs appropriate for lower risk data types.
   - The **likelihood** that data will be accessed inappropriately should be factored into risk assessments.

[3] For example, Article 27(1) of the Latvian Personal Data Processing Law which prescribes that the data subject does not have a right to receive information if it is prohibited to disclose in accordance with the laws and regulations regarding national security, national protection, public safety and criminal law, as well as for the purpose of ensuring public financial interests in the areas of tax protection, prevention of money laundering and terrorism financing or of ensuring of supervision of financial market participants and functioning of guarantee systems thereof, application of regulation and macroeconomic analysis.

- Clarifying that firms can **group similar transfers together to assess collectively**.

Taking the above, Use Cases 6 and 7 could still achieve a suitable level of protection, depending on the full assessment of risk in relation to the transfer.

In **terms of tools and flexibility,** encryption should also include the option to encrypt the communication channel of data, as an alternate (or if appropriate in tangent) to encrypting the personal data itself. The Use Cases should be updated to include this as well as the clarification that data on "secure" arrival to data exporter, where necessary, may be reviewed in clear format.

2. Finally, easy-to-use modular instruments for legal or technical safeguards for data protection would also be helpful for companies. If a company uses these standard instruments, this should in principle be sufficient to ensure data protection. Better aligning the Recommendations with the **appropriate and proportionate level of security as set out in Article 32.**

3. Third, we **encourage DPAs to play an active role in helping companies to make the assessment of third country legislation for transfers.** The role of supervisory authorities in developing guidance to help data exporters is mentioned in the executive summary but this should **be reinforced.** DPAs should at least **publish a first level assessment of third countries legislation for data exporters to have a common basis (particularly on key jurisdictions),** thereby helping to limit the fragmentation between EU countries and allowing them to only focus on assessing the specificities of their activities and processing, if any, as well as circumstances of the transfer. This could be a classification of a high/medium/low risk rating and firms would use this Guidance to inform their holistic risk assessment, as per the first recommendation. Moreover, a **collaborative approach is needed among European DPAs to ensure that recommendations to companies/help with their risk assessments is provided in advance, is coherent and does not lead to fragmentation.**

   Collaboration with the European Commission with regards to helping data exporters in the assessment of third country legislation is also important. **Examples of practical tools which the Commission could provide to data exporters include:**

   - **Providing a centralized IT tool** that can be used by any organisation to carry out the risk assessment through set risk criteria and **research/analysis of local legislation.** This analysis could be the same "first level assessment of third countries" mentioned above. Depending on the specific responses to the questions by the organisations, **a specific risk rating is provided for the organisation**. **This could start with a list of priority countries and gradually progress.** The Commission could also consider either outsourcing or creating a body to conduct periodic updates of the first level assessments for third countries.
   - Providing a living platform for data exporters to access: **(i) third country laws and materials: and (ii) a record of entities which have been subject to data subpoenas from their public authorities** (so that the warrant canary is rendered meaningful).
   - Following the examples of security notices on travel countries issued by national governments, **the EC could publish data protection notices on certain third countries**. This guidance would enable companies to make a legal assessment in Step 3.

As creating a platform could take some time, flowcharts, using the first level assessment of third country legislation for data exporters to have a uniform basis, could be published for data exporters to use. The Commission and DPAS may also take appropriate steps **to develop an international cooperation mechanism**, also engaging stakeholders, to facilitate the effective enforcement of legislation for the protection of personal data, pursuant to principles set forth in Article 50 of GDPR.

DPAs should also have further options available to them other than to cease processing, for example, it might be in position to leverage and share know-how that it may have received from similar organisations.

4. It should be clear that the analysis of the law and practice of the third country shall be performed by the data importer and validated by the data exporter only if the data importer communicates all relevant documentation in the language of the data exporter.

Finally, given **the level of impact of such guidance on the business and organisation of data exporters/controllers, we emphasize the need for a meaningful grace period of at least two years**, **therefore allowing for a sufficient period of time to elapse to enable businesses to implement the relevant procedures and measures.** A case by case assessment of transfers, determining the relevant supplementary measures (if step 4 is required) and making, for example, contractual changes, requires a lot of time, human and financial resources and involves many parties. **This is also important given the publication by the European Commission of the new draft Standard Contractual Clauses, which will also need to be implemented.**

## 4. Practical examples of the impact of Recommendations to day to day operations of banks

Members would like to flag everyday situations(potentially) faced by a bank with regards to transferring data to third countries. These situations illustrate the potential risk to bank's operations, both for clients and internally of the proposed measures (technical, contractual, and organisational) and the subsequent need to ensure a risk based approach to international transfers.

- An EU firm pension provider for its EU based employees of a US-headquartered company. Payroll for the EU staff is carried out in the US and the EU pension provider is required to share data directly with the US company for the purposes of processing pension contributions.

  Given that the US company would need access to the data in the clear, the Recommendations would suggest that the US company would need to shift the processing of payroll and pension data of the EU employees to the EU (assuming that the data would be within scope of FISA powers, which is unclear). Given the nature of the data and the likely low level of interest for US authorities, it would seem very disproportionate to force this processing to be moved to the EU, even assuming that this would not simply render the processing impossible.

- Typically, personal data transmitted to data importer is in itself encrypted however in relation to some security/anti-malware solutions. Due to nature of the task, data may be directly accessed from a bank's servers using an encrypted communication channel. If the importer is requested to undertake analysis, data is sent by the bank securely, but the importer will need to analyse the data on its systems. Therefore, data is decrypted and analysed in "raw" clear format once received at

their end. Subsequently, controllers should continue to implement appropriate controls based on the circumstances. Therefore, in terms of flexibility, encryption tools should include the option to encrypt the communication channel of data as an alternate tool (or if appropriate in tangent) to encrypting the personal data itself.

- SaaS or IaaS where the infrastructures and the applications are under management of third parties, with access from extra-EEA for administrative purpose (e.g., bug fixing, trouble shooting, application maintenance, deployment of new software / an application) despite that data are typically located in EEA datacentres. The administrative users of third parties could technically be able to access data in the clear (for example through application or infrastructure debug / trouble shooting), despite the BYOK / CMEK adoption, and/or automatic deploy procedures in place (leverage on applications that are always able to decrypt data to show data in the clear to users). **Due to the nature and widespread use of Software-as-a-Service, none of the EDPB proposed supplementary measures would be sufficient to enable banks to use them, regardless of the measures,** e.g., additional approval steps before allowing the processor's support team access to personal data. **Not enabling banks to use Software-as-a-Services would greatly impact the products and services provided to banks' customers.**

**ENDS**

## ANNEX 1 – Detailed comments on Use Cases

### Use Case 1: Data storage for backup and other purposes that do not require access to data in the clear

- **Some requirements imposed around data encryption are unrealistic in practice.** For example, the requirement that the encryption algorithm must be robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities such as "the computing power" for brute-force-attacks. **This information about computing power is almost impossible to obtain.** The EDPB also seems to assume that it is possible for the data exporter to keep the encryption keys under its control. In practice however, this will often not be possible. Further Guidance on what is considered "under data exporter's control" would be welcome in this regard.
- Data storage for backup and other purposes that do not require access to data in the clear. Banks typically adopt accepted international standards encryption algorithm (e.g., TLS, AES256, SHA2, PKCS11 standard) before and during transmission for this use case, applicable for example in case of backup of database. **We would recommend to mention compliance with international standards as an example of compliance with the measure "conform to the state-of-the-art".**
- Both in this Use Case and Use Case 2, **a number of the conditions stipulated go beyond the standard stated in Article 32** which balances controls with the "cost of implementation as well as risk of varying likelihood and severity for the rights and freedom, the controller and processor shall implement appropriate technical and organisation methods to ensure a level of security appropriate to the risk". Language such as: "strongly encrypted", "robust against cryptanalysis", and encryption algorithm is "flawlessly implemented" requires a standard higher than what is appropriate. **It also ignores a risk based assessment and that often ICT data importers typically offer banks technology with pre-installed security solutions.** We therefore suggest to soften such language.

### Use Case 2: Transfer of pseudonymised Data

- The applicability of this use case is limited for banks as the use of pseudonymisation does not consider that**, in many cases, this may not be possible due to the requirements of the counterparty receiving the data to process it,** for example in case of:
    - Simulated phishing email campaign for awareness that requires email list and nominative of the data subjects to send emails customized with details of the employee and analyse the answers, if any;
    - Worldwide DDOS prevention services that require client IP address (considered personal data) to allow cybersecurity protection from these kind of cyber-attacks;
    - Paperless technologies to allow digital signature require document and clear data access to the provider.
- The provision to "take into account any information that the public authorities of the recipient country *may"* possess is disproportionate. **How would data exporters determine what information public authorities *might* have access to.**

- Conditions 1-4 provide for the adoption of suitable measures to make it impossible, for the data importer and, therefore, for the authority of the destination country, to re-identify a natural person through data transferred by the data exporter, since, with the described pseudonymisation of the data, the data importer would never be aware of the identifiers referable to the interested parties. On the basis of the above and without prejudice to Recital 26 of the GDPR, clarifications are required regarding the need, in compliance with all the conditions referred to in Use Case 2, of (i) if appropriate, to appoint the data importer responsible for the processing, pursuant to Article 28 of the GDPR and (ii) sign the standard contractual clauses referred to in Article 46 (2), lett. c) of the GDPR.

**Use Case 3: Encrypted data merely transiting third countries**

- It is not always possible to understand the geographical routing "*the data is transported over the internet, and the data may be geographically routed through a third country not providing an essentially equivalent level of protection*". Banks typically adopt accepted international standards encryption algorithm (e.g., TLS, IPSEC) during transmission for this use case. We would recommend to include a reference to international standards as an example of compliance with the measure "*conform to the state-of-the-art*".
- Further to the comment above on implementing additional measures on adequacy decisions, the use case describes encryption safeguards appropriate for data routed **through a non-adequate country in transit to an adequate one**. The EDPB seems to indicate that additional safeguards may be in any case necessary. We would recommend further clarification on this point.
- We would welcome clarification on, if all the conditions described in Use Case 3 are met (with particular reference to the application of end-to-end encryption mechanisms) and considering that personal data are transferred to a data importer located in a country where an adequate level of protection is guaranteed pursuant to the GDPR, the need to sign the standard contractual clauses pursuant to art. 46 (2), lett. c) of the GDPR.

**Use Case 4: Protected recipient**

- Compliance with all the conditions listed in Use Case 4 makes it impossible for the authorities of the destination country to access the personal data transferred by the data exporter. On the basis of the above, it is considered that the end-to-end encryption key, even if kept by the data importer, is adequately protected against unauthorized use or disclosure by state-of-the-art technical and organizational measures and that, consequently, the data importer will not be able to access the data and re-identify the interested party, clarifications are requested regarding the need, if all the conditions referred to in Use Case 4 are met, of (i) if applicable, appoint the data importer responsible for the treatment, pursuant to art. 28 of the GDPR and (ii) sign the standard contractual clauses referred to in art. 46 (2), lett. c) of the GDPR.

**Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear**

Transfer to cloud services providers or other processors which require access to data in the clear (paragraph 88) provides that, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption, even taken together, do *not* constitute a supplementary measure, that ensures an equivalent level of protection if the data importer is in possession of the

cryptographic keys. **This means that the transfer of data in clear to a cloud service provider should not be allowed.** The consequence is that the data cannot be transferred to cloud service provider unless they are anonymized.

**This may impact several services that require few personal data, in order to properly run (e.g., IP Address, business e-mail address, user id). The most frequent example would be the "user provisioning" services, i.e., services used for allowing the user to login to those services, provided in SaaS (Software as a Services), PaaS (Platform as a services) or IaaS (Infrastructure as a services) form. Therefore, the use of login data (in clear) are needed, in order to ensure the provision of such cloud services. We highlight the need to review this use case with a proportionate approach.**

Similar consideration could be made with reference to Use Case 7 (paragraph 90), where a data exporter makes personal data available to entities in a third country, to be used for shared business purposes. **This approach may cause a huge impact on the business between banks and third parties outside the EU (e.g., call centres, back office services, etc…).**

**For more information:**
Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu

**About the EBF**

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu