Position to the **EDPB Recommendations on Supplementary Measures**

On 10 November, the European Data Protection Board (EDPB) issued, for public consultation its *Recommendations* on measures to promote compliance with the EU Court of Justice's recent decision in *Schrems II*. The Court in *Schrems II* held that organisations that rely on standard contractual clauses (SCCs) to transfer data outside the EU may need to adopt additional safeguards to protect personal data from access by public authorities in third countries.

The American Chamber of Commerce in Slovakia (AmCham Slovakia), AmCham Czech Republic and the Slovak Alliance for Innovative Economy (SAPIE) represent more than 700 companies ranging from multinational corporations to local SMEs in Slovakia and Czech Republic. We welcome the EDPB's public consultation period on the Recommendations 01/2020 to discuss supplementary measures as this is an important issue and an opportunity for stakeholders across all industries to provide input.

We would like to point out several areas of concerns and propose several suggestions to contribute to the public consultation which we believe the Recommendations should take into consideration.

Overall evaluation

Although many were hopeful that the EDPB would provide data exporters with a "toolbox" of pragmatic, practical measures that would help them comply with the Court's decision, the proposed *Recommendations* do the opposite by proposing a prescriptive, non-risk-based approach that goes far beyond the requirements of *Schrems II*. Rather than follow the Court's instruction to take the context of a transfer into account, the EDPB has adopted a restrictive, absolutist interpretation of EU law that would place insurmountable obstacles to transfers of personal data outside the EU.

If the *Recommendations* are adopted in their current form, any organisation that uses an online service to process and transfer personal data—including email, hosted applications, or any other online service—could face fines up to 4% of its annual turnover, irrespective of whether public authorities in any third country ever access the data in question. They also will require EU organisations to undertake their own costly analyses of the laws and practices of dozens of non-EU countries (i.e., those not subject to an EU adequacy decision), which will be unrealistic for most small and medium-sized enterprises, research institutions, and others.

As a result, the *Recommendations* will make it highly risky for EU companies to engage in commerce with non-EU customers or partners, for researchers to share information with foreign colleagues, for companies with non-EU offices or personnel to communicate with them online, or to engage in countless other routine and necessary operational tasks. If adopted, they will force many aspects of EU commerce and society into a pre-Internet era, and/or isolate Europe from the global economy. The potential negative effects on EU competitiveness, innovation, and society are enormous.

Moreover, it is far from clear that all third countries that have an adequacy decision from the European Commission—or indeed that all EU Member States—provide a level of data protection that is "essentially equivalent" to that set out in the GDPR and EU Charter of Fundamental Rights. By focusing only on non-adequate jurisdictions, the *Recommendations* threaten to create an unequal international playing field for data protection, where data exporters are required to apply different rules to different jurisdictions even where similar levels of data protection exist between them. Such discriminatory treatment of different jurisdictions is also likely to invite retaliation by jurisdictions whose companies are placed at a competitive disadvantage in European markets by the EDPB's actions.

The EDPB Recommendations should take into account that the access to industry-standard IT security measures is essential for any business processing data. The access to state-of-the art security services must be factored into any risk assessment of transferring data to a third country. The recommendations should also clarify that for all scenarios outlined in the use cases (especially use cases 6 and 7), many other factors can be taken into account. For instance, contractual and organizational measures should be considered to sufficiently help guaranteeing the protection of personal data transferred.

The detailed analysis which seems to be required by the ruling in the light of the EDPB Recommendations goes beyond what can reasonably be expected from companies.

While the risk assessment needs to be performed before transfers take place, it should be possible to analyse the risk prior to commercializing/using a service, and not prior to each transfer. This is paramount to maintain the smooth delivery of cloud services.

Main concerns:

A guidance impossible or extremely onerous to comply in practice, disproportionate and damaging EU citizens and businesses

- The EDPB Guidance places extremely onerous obligations on organizations to comply in practice since it imposes a specialist multi-jurisdictional legal advice and an expensive and time-consuming implementation.
- The EDPB Guidance undermines and will damage EU citizens and organizations of all sizes and sectors, based on a disproportionate approach against the Charter and the EU objectives.
- The collective impact of this EDPB guidance will be a dramatic reduction in personal data transfers from the EU depriving EU organizations and its citizens of fundamental rights to trade and communicate with those outside the EEA.
- EDPB guidelines create legalistic fiction targeting mainly big US IT companies but letting all SMEs, microbusinesses & startups of this world in a complete incapacity to comply (lack of budget, time, expertise).

EDPB Recommendations do not take into consideration CJEU recent surveillance case law and post-2016 US surveillance changes

- The EDPB Guidance does not take into account that US surveillance laws and practices have evolved since 2016 (which is the framework analyzed in the Schrems decision).

- The EDPB Guidance obviates that the US and the EU share common values and interests, in terms of respect human rights, the rule of law and the cybercrime collaboration.
- The EDPB does not consider the recent CJEU case law that confirms that national security can justify serious interferences with individuals' rights.
- According to the CJEU 6 October 2020 decision, UK, FR, BE do not meet the bar of the "essentially equivalent test" because of disproportionate surveillance systems.

A proposal that puts organizations in an impossible situation, inappropriately focuses on technical safeguards and contradicts EU Member States surveillance requests

- The EDPB Guidance puts forward safeguards that are unworkable. Day-to-day processing would be prohibited at enormous cost to EU organizations and ultimately citizens.
- The EDPB Guidance inappropriately focuses on specific technical measures.
- The EDPB requires strong encryption while EU Member States try to impose backdoors to encrypted communications for surveillance purposes.
- In contradiction with the CJEU, the EDPB Guidance seeks to prohibit reliance on SCCs for transfers to key US service providers.

An unjustified overly restrictive interpretation contrary to CJEU and GDPR goals (i.e., to enable transfers rather than avoiding them)

- A balanced interpretation is not necessarily a restrictive interpretation.
- Some of these derogations are not and cannot be "exceptional", as wrongly construed by the EDPB, such as the performance of international communications or international money transfers. In any event, the EDPB Guidance fails to distinguish between the business transfers and the transfers due to governmental access requests, which are exceptional by nature.
- The EDPB should take this opportunity to holistically revisit the overly narrow interpretation of the derogations in the light of the *Schrems II* ruling and that the goal of GDPR provisions on international transfers was to enable them rather than prohibit them.

Principal suggestions:

1. ***The Recommendations should allow data exporters to take account of the full context of a transfer.***

In *Schrems II*, the Court indicated that data exporters should consider the full context of a transfer when evaluating its legality—specifically, that transfers should be evaluated "in the light of all the circumstances of that transfer" (¶¶ 121, 146) and "on a case-by-case basis" (¶ 134). Several passages in the *Recommendations*, however, appear to foreclose this contextual approach. For instance, they state that, if the data importer falls within the scope of certain national security laws, the data exporter must use additional technical measures (text box before ¶ 45)—even, presumably, if the data importer has never faced an order under those laws and the data is of no conceivable relevance to national security (e.g., an employee's menu preferences for a holiday party). Other passages similarly suggest that the likelihood that a public authority will ever access the data is irrelevant (¶ 42).

Restricting transfers of data even where the context shows there is virtually no risk to data subjects will harm every corner of the EU economy and society. EU researchers sharing health data with foreign partners to fight COVID-19, EU companies engaging in routine communications with employees outside the EU, and even simple commercial transactions with non-EU entities would all be fraught with substantial risk. Nothing in the *Schrems II* judgement requires this draconian outcome.

Rather than discourage EU organizations from considering contextual factors, the *Recommendations* should encourage organizations to consider the real-worlds risks of a transfer, including the relevance of the data to law enforcement agencies and the likelihood that such agencies would request access to the data. If these real-world risks are low, which they are for most categories of data, the *Recommendations* should not require organizations to adopt any supplemental measures.

2. The Recommendations should propose technical measures that are workable in practice.

The *Recommendations* propose a non-exhaustive list of technical measures that data exporters can use to supplement the safeguards in the SCCs. Unfortunately, the *Recommendations'* case studies on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice.

For instance, the *Recommendations* suggest that organizations can rely on encryption as a safeguard in most cases only if the data never appears in an unencrypted form in the third country and if the decryption keys are held only within the EU (or an adequate jurisdiction) (see, e.g., ¶¶ 79(6), 89(2-3), 84(11)). They also suggest that encryption almost never provides sufficient protection where data is accessible "in the clear" in the third country, including where an EU organization uses an online service that may process the data in the third country (¶¶ 88-89), or where employees or others in the third country can access the data on a shared IT system (e.g., human resources data) (¶¶ 90-91).

Moreover, because the *Recommendations* state that even remote access by an entity in a third country to data stored in the EU constitutes a "transfer" (e.g., footnote 22, ¶ 13), organizations in many cases would need to apply these technical safeguards to EU-stored data as well. This fact underscores the impracticality of the *Recommendations* and their incompatibility with other important EU interests, such as promoting open global trade and research necessary to protect vital interests (for instance in the context of the COVID-19 pandemic). At a time when policymakers across the world, including in Europe, are pressing companies to provide greater access to encrypted communications in order to help governments more effectively fight terrorism and other threats, the proposed *Recommendations* would appear to penalize companies for making such access possible.

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

In reality, most EU organizations would not be able to cease these activities entirely while still remaining economically competitive. Instead, many would likely turn to other legal mechanisms, such as the derogations set out in Article 49 of the GDPR. Because organizations adopting this approach might transfer data to non-adequate jurisdictions without even adopting SCCs (to say nothing of additional safeguards), this outcome would leave EU data subjects worse off, because their data would be subject to fewer protections than they are today. However, the EDPB also noted that such derogations (which would include data subject consent) must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive.

To avoid these consequences, the EDPB should revise the *Recommendations* to ensure that the proposed technical measures are workable in practice and should leave it to data exporters to determine whether any particular measure adequately protects the transferred data. The *Recommendations* should not prohibit all access to data in the third country; doing so will discourage organizations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorized access.

3. The Recommendations should clarify that contractual measures may provide sufficient safeguards.

Although the *Recommendations* propose a non-exhaustive list of contractual measures that can offer additional safeguards, they also include language suggesting that contractual or organizational measures on their own (i.e., without additional technical measures) cannot provide the level of data protection that EU law requires (¶ 48). This position appears to assume that the mere theoretical possibility of access by third-country authorities—even if the practical risk of such access is vanishingly small—renders a transfer unlawful.

This position adopts an overly restrictive reading of the *Schrems II* judgement. The Court in *Schrems II* held that transfers of data to third countries should be prohibited only "in the event of the breach of [the SCCs] or it being impossible to honor them" (¶ 137). This language, and similar passages elsewhere in the judgement, suggest that, so long as the data importer does not in fact disclose data to third-country authorities (or, if it does make such a disclosure, that it notifies the data exporter accordingly), then the parties may rely on the SCCs (¶ 139). Under this reading, it is clear that contractual measures alone can provide the additional safeguards needed to safely transfer data to a non-adequate jurisdiction.

To align with the *Schrems II* judgement, the *Recommendations* should remove all language suggesting that contractual measures alone are insufficient safeguards to satisfy EU law. The *Recommendations* should instead articulate several possible contractual measures that EU organizations may consider when transferring data to a non-adequate jurisdiction, then leave it to data exporters and importers to evaluate which measures are appropriate in context and "in the light of all the circumstances of that transfer" (*Schrems II*, ¶¶ 121, 146).

4. ***The Recommendations should make clear that enforcement by supervisory authorities will be measured and appropriate.***

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

Notwithstanding these facts, the *Recommendations* imply that supervisory authorities should move directly to "corrective measure[s] (e.g. a fine)" if they determine that a data transfer does not comply with the *Recommendations* (¶ 54). This focus on sanctions will lead EU organizations to rush through changes to their data transfer practices—making it far less likely that organizations address these issues carefully and precisely.

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

5. ***EDPB / European Commission should provide clear assessments of risks presented in each country and continuously monitor any changes***

This would allow exporters to have reliable information and ensure appropriate protection of their personal data.

Problematic aspect: **Shifting of responsibility from the European Commission to individual companies**

In summary, the EDPB requires that all controllers and processors (1) assess whether the legal framework of the importing country presents any risks to data protection, (2) assess whether the practice of public authorities (even if not outlined in law) in the importing country presents any such risks, (3) if any such risks have been identified, assess whether they may be considered as "justifiable interference" and (4) continuously monitor any changes to the previous questions.

Such questions are typically part of the assessment conducted by the European Commission as part of an "adequacy decision". Given that the average time for adequacy takes up to 28 months (reference: https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-and-brexit-is-there-a-need-for-an-adequacy-decision.html#:~:text=Keep%20in%20mind%20that%20the,be%20revoked%20at%20any%20time), it seems practically impossible for companies to be able to conduct such assessment as part of their business as usual activities. Such assessment may be further complicated in case multiple countries are involved in the processing.

6. ***Provide clear recommendations for small and medium enterprises on how to ensure compliance relating to international data transfers***

We regard the Recommendations as imposing a very significant compliance burden on all market players.

The requirement to assess each importing jurisdiction, although theoretically laudable, imposes a burden that only a few companies will be able to meet.

As such, the EDPB creates a compliance framework which will favor the biggest and most successful companies, as these may have the necessary resources to meet the extensive assessment requirements. On the other hand, small or medium enterprises are likely to face a choice between (a) refusing to comply, (b) looking for efficiencies without full compliance or (c) expending significant budgets on obtaining appropriate documentation. We would appreciate the EU Commission to prepare templates "ready to use" for start-ups (no modules) which require hours of work to adapt."

Moreover, impact on legal certainty is significant. Although the overall goal aims to increase the protection of individuals, a significant side effect is a decrease of legal certainty of exporters. Setting a high compliance burden may result in fatigue and compliance errors. In addition, although the EDPB Guidelines contain many helpful recommendations, small and medium enterprises will likely be unable to comply with all steps (in particular assessment and ongoing monitoring). As such, companies will face legal uncertainty as to the validity and compliance of their data transfers, which may result in significant fines or even restrictions of transfers.

7. **EDPB should c*onsider outlining recommendations relating to other risks***

Problem: Undue focus on disclosures to public authorities & missing data subject rights

The EDPB Guidelines seem to focus predominantly on one specific risk – namely the disclosure of personal data to public authorities. Although this is definitely a very important factor, the Guidelines do not contain consideration of situations without such access. For instance, we consider that exporters would benefit from clarification on how to efficiently ensure the compliance with rights of data subjects (such as right of access or deletion) and consequently strengthen the protection of individual's privacy.

8. ***Clarifying access by other public authorities should be considered***

Unclear definition of "Public Authority" is highly problematic.

The EDPB Guidelines focus on access by public authorities, however, they do not differentiate between the various types of such authorities. We understand that key focus access by law enforcement, however, it remains unclear whether the same scrutiny applies to companies regulated in the healthcare, finance, aviation, automotive or other sectors. Public authorities in these sectors may require access to personal data as part of various approval procedures or ongoing safety monitoring procedures.

We understand that access by public authorities other than law enforcement does not pose the same level of risk. Such access is linked to increase in safety, quality of service and additional public benefits, as has been absolutely clear under the current response in the Covid-19 pandemic (e.g. cooperation to approve vaccines).

Comments to the respective parts of the Recommendations

General comments

- The EDPB published *Recommendations* 01/2020 rather than *Guidelines.* There is a distinction between Recommendations and Guidelines, especially from a legal perspective that should be explained.

- Due to the important impact of the subject for a wide range of companies, the Board may wish to reconsider the immediate effects of these Recommendations in order to allow due considerations to the contributions received through the public consultation..

- A near-term EU-US political agreement on an "enhanced Privacy Shield" is needed to bring not only more legal certainty for business, but also the maintenance of a wide range of services and products used by EU citizens as data flows are ubiquitous in our way of life.

Comments on the **Executive Summary**

- **T**he Recommendations heavily rely on the principle of accountability in Art. 5 (2), without explaining in any detail how that principle is relevant to the subject matter of international data transfers. Art. 5 (2) explicitly relates to the principles laid out in Art 5 (1). The lawfulness principle is only referring to Art 6 GDPR not to Art. 44 et seq and the other principles are even more removed from international transfers.

- On "know your transfers", the EDPB states that "[y]ou must also verify that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country". This is apparently a reference to the data minimization principle.

- However, the data minimization principle is misapplied here. The data minimization principle considers the amount of data in relation to a processing *purpose,* but not in relation to every *processing activity* done for that purpose. If data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, the principle is being met, including for all processing done for that purpose. So, if a transfer is part of a processing operation undertaken for a specific purpose, there is no separate test under the purpose limitation principle that is focused on that transfer separate from the other processing activities.

- The Board notes that "[o]nly in some cases of occasional and non-repetitive transfers you may be able to rely on one of the derogations provided for in Article 49 GDPR". The Board may wish to provide more details about it in order to avoid oversimplification: Recital 111 differentiates among the derogations by expressly stating that the "contract" and the "legal claims" derogations (Article 49 (1) subpar. 1 (b), (c) and (e)) shall be limited to "occasional" transfers, while such limitation is absent from the "explicit consent derogation", the "important reasons of public interest derogation", the "vital interests' derogation" and the "register derogation" pursuant to Article 49 (1) subpar. 1 (a), (d), (f) and, respectively, (g). Finally, the EDPB itself called out these differences:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

- The Board notes that one should "not rely on subjective factors such as the likelihood of public authorities' access to data". Likelihood is a very relevant factor that the GDPR relies on in multiple places such as Recitals 75, 76, 77, 88 and 90 as well as Art. 24 (1), 25 (1), 32 (1) and 34 (4). Likelihood in the sense of probability is also not a subjective factor, it is an objective factor and probability is relevant if the GDPR's rules are applied in line with the principle of proportionality and its risk-based approach. Declaring likelihood of public authorities' access to data also means that even if public authorities' access to the data in a manner not in line with EU standards is *highly likely,* it would have to be disregarded.

- The Executive Summary states that "[y]ou may ultimately find that no supplementary measure can ensure an essentially equivalent level of protection for your specific transfer. In those cases where no supplementary measure is suitable, you must avoid, suspend, or terminate the transfer to avoid compromising the level of protection of the personal data. You should also conduct this assessment of supplementary measures with due diligence and document it." This may cast further doubt on the future of almost all data transfers from the EU to any third country that does not have an Adequacy agreement under GDPR.

Comments on: Accountability in Data Transfers

- Paragraph 3 states that "[c]ontrollers and processors must also be able to demonstrate these efforts to data subjects, the general public and data protection supervisory authorities". However, GDPR does not create any obligations of controllers and processors vis-a-vis the general public when it comes to the demonstration of internal accountability programs.

- Paragraph 4 states that the principle of accountability "also applies to data transfers to third countries since they are a form of data processing in themselves". As mentioned above, the recommendations should specify on which basis it concludes that the accountability principle is relevant in the context of international transfers. Generally, these recommendations apply the accountability principle very loosely, turning it into an amorphous concept, whereas the language of Art 5 (2) very clearly limits that principle to the controller's compliance with the Art. 5 (1) principles.

Comments on: **Roadmap: Applying the Principle of Accountability to Data Transfers in Practice**

- Paragraph 8 states that data "you are fully aware of your transfers (know your transfers)". Further guidance is required on the types of transfers that are out of the scope of this exercise, because they are not attributable to the controller or processor conducting the exercise:

    - Transfers to a data importer in a third country that is subject to the GDPR, e.g. by virtue of Art. 3 (2) or Art. 3 (3) should be out of scope, since the GDPR continues to apply at the point of destination of the transfer.

- Transfers that are attributable to the data subject. For example, in many cases, it is the data subjects themselves that initiate the transfer, such as by sending an Email, publishing a post, sharing a document, traveling to a third country and taking remote access to data stored by their provider in the EEA etc. Those types of transfers are not attributable to the provider of the service and are therefore not in scope of his obligations under Chapter V of the GDPR.

- Transfers attributable to a third party. In many places the Recommendations refer to actions by third parties in third countries by which they gain unauthorized access to personal data, as if these actions would create obligations under Chapter V of the GDPR for the controllers or processors whose date security measures have been breached by those actions of that third party. However, if a breach of security leads to unauthorized access by a third party in a third country, such as in a case of hacking by that third party, any resulting transfers is not attributable to the entity operating the data processing operation that has been hacked. These types of scenarios will not even be "transfers" in many cases. In Footnote 14 of the Recommendations the EPDB refers to C-362/14 (Schrems I), paragraph 45 where a transfer is referred to as a "disclosure by transmission, dissemination or otherwise making available". However, controllers or processors storing data in their systems are not “disclosing” data to third parties that gain unauthorized access to such data.

- Paragraph 11 refers to the principle of data minimization and that it must be verified "that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country". As previously mentioned, the data minimization principle is misapplied here.

- We suggest rephrasing paragraph 31 to clarify that the actors participating in the transfer are the (i) controller; (ii) processor; and (iii) processor's direct sub-processors processing data in the third country.

- We suggest adding to paragraph 33 that the likelihood of public authorities’ access in the specific case of a transfer scenario can complement the other factors for assessing the risk of the transfer.

- Paragraph 42 seems not to take into consideration the risk-based approach characteristic of the GDPR, which is essential to its effectiveness and balanced implementation, and widely accepted in international standards.

    - In particular, the Recommendations do not distinguish categories of data. For example, IP addresses would get the same treatment as health data. Clearly the risk inherent to those to the rights and freedoms of natural persons are very different. Also, they eliminate the possibility to take the likelihood into account, which is an essential part of any risk assessment.

    - As indicated by GDPR (recital 75) the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the

reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage. Such elements need to be factored into the Recommendations.

- Likelihood in the sense of probability is an objective factor and probability is relevant if the GDPR's rules are applied in line with the principle of proportionality. Declaring likelihood as irrelevant could lead to further interpretation that even if public authorities' access to the data would not be in line with EU standards.

- Finally, the CIPL White Paper A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision (https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii__24_september_2020__2_.pdf) brings meaningful recommendations of possible measures that can be deployed by organizations based on context and risk, rather than prescribe strict technical or procedural requirements.

- Paragraph 43 provides examples of elements that could be used to complete an assessment with information obtained from other sources. It states that "[e]lements demonstrating that a third country authority will be able to access the data through the data importer or through direct interception of the communication channel in light of reported precedents, legal powers, and technical, financial, and human resources at its disposal".

  - We suggest the Board to consider that such an interception is not attributable to the data exporter as the data exporter would not be doing this transfer. The data exporter must uphold security measures in line with Art 32 GDPR, but he/she does not have an obligation to establish valid transfer mechanisms, for transfers that occur when third parties overcome those security measures and take access to the data at issue. The third party may be in direct violation of the GDPR when doing this interception, but it cannot thereby put the controller or processor in violation of the GDPR, too.

  - Suggesting that these types of activities undertaken by third parties are attributable to a controller or processor would potentially change the risk profile under the GDPR in a fundamental way.

  - Finally, the types of scenarios described would not even be "transfers" in many cases. In Footnote 14 the EPDB refers to C-362/14 (Schrems I), paragraph 45 and this type of interception by a third party is not a "disclosure by transmission, dissemination or otherwise making available", instead it is a "collection" of data by the third party.

- Paragraph 48 states that "[c]ontractual and organizational measures alone will generally not overcome access to personal data by public authorities of the third country (where this unjustifiably interferes with the data importer's obligations to ensure essential equivalence)". We suggest the Board reconsiders its position here as organizational measures in particular can indeed serve to narrow such access to a degree where it meets the principle of proportionality and is limited to what is strictly necessary. The EDPB should acknowledge that as a possibility. We

recommend amending paragraph 48 taking into consideration that a holistic view and a risk assessment can lead to the result that contractual and organizational measures alone can sufficiently protect the data subject. Further, a reference to contractual and organizational measures in paragraph 33 should be included.

Comments on: Conclusion

- Paragraph 65 states that "[y]ou must also check that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country." The data minimization principle is, once again misapplied.

Comments on: Annex 2 - Examples of Supplementary Measures

- Paragraph 75 (a) states that "[p]ublic authorities in third countries may endeavor to access transferred data in transit by accessing the lines of communication used to convey the data to the recipient country", which implies that the resulting transfer is attributable to the exporter. The Board may wish to provide clarification, as it could imply that access by a hacker would be considered a disclosure by the controller or processor who has been hacked. In line with what has been said above, this is a transfer attributable to those public authorities; it is not a transfer that is attributable to the entities relying on these lines of communications. These types of scenarios will not even be "transfers" in many cases. In Footnote 14 the EPDB refers to C-362/14 (Schrems I), paragraph 45 and this type of gaining access by a third party is not a "disclosure by transmission, dissemination or otherwise making available", instead it is a "collection" of data by the third party.

- Paragraph 75 (b) states that "[p]ublic authorities in third countries may endeavor to access transferred data while in custody by an intended recipient of the data by either accessing the processing facilities themselves". Similar to the point made above, unless that access is somehow authorized by the data exporter or the intended recipient it is not a transfer attributable to the data exporter or the intended recipient. If any third party in a third country gains unauthorized access to the processing facilities, short of obligations under Art 33 and 34, neither the intended recipient nor the data exporter carries any obligation in relation to such access unless to the extent it is a result of a failure to uphold security measures in line with Art 32. The third party may be in direct violation of the GDPR by gaining this unauthorized access but not the entity whose system has been accessed in that way. Once again, these types of scenarios will not even be "transfers" in many cases. In Footnote 14 the EPDB refers to C-362/14 (Schrems I), paragraph 45 and this type of gaining access by a third party is not a "disclosure by transmission, dissemination or otherwise making available", instead it is a "collection" of data by the third party.

- For the two use cases relying on encryption, the Board may wish to clarify that there may be other ways encryption can be used effectively and that encryption measures can change over time. Otherwise, an assumption may be made that these two use cases are the only use cases where encryption can be effective.

- Paragraph 79 states that "the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved". The

Board may wish to provide more clarity of the implications of it. It is unclear as to why this third condition is a requirement for the measure to be considered an effective supplementary measure.

  - It also concludes that, under these conditions the EDPB "considers that the encryption performed provides an effective supplementary measure". Again, under these conditions, the personal data is not even transferred to the third country in question, since no "information related to an identified or identifiable individual" is becoming available or has been "disclosed" (see C-362/14, paragraph 45) to anyone in that third country.

- Paragraph 80, which refers to Case 2 "transfer of pseudonymized data", the EDPB "considers pseudonymization performed provides an effective supplementary measure". However, under conditions described by the Board, the personal data is not even transferred to the third country in question, since no "information related to an identified or identifiable individual" is becoming available or has been "disclosed" (see C-362/14, paragraph 45) to anyone in that third country.

- Paragraph 84 brings Case 3 "encrypted data merely transiting third countries", and it states as one of the conditions if "decryption is only possible outside the third country in question". Once again, the Board should consider this specific condition could result in no transfer to a third country. Another time, under these conditions, the personal data is not even transferred to the third country in question, since no "information related to an identified or identifiable individual" is becoming available or has been "disclosed" (see C-362/14, paragraph 45) to anyone in that third country.

- Paragraph 86 brings the Case 5 "Split or multi-party processing", in which "[p]rior to transmission, it splits the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part". Another case in which, under these conditions, the personal data is not even transferred to the third country in question, since no "information related to an identified or identifiable individual" is becoming available or has been "disclosed" (see C-362/14, paragraph 45) to anyone in that third country.

- Paragraph 88 brings the Case 6 “Transfer to cloud services providers or other processors which require access to data in the clear”. The Board may wish to address those cases in which the data can only be seen in clear text by a machine that does the processing and not by a human.

- The Board should reconsider all the use cases it presents. In the Executive Summary the EPDB itself says that in cases where the law or practice of a third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools, the Court still leaves open the possibility for exporters to implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law. None of the Use Cases provided are filling any such gaps, since they fall into two categories:

  - Use Cases 1-5 describe measures that prevent the transfer entirely since no "information related to an identified or identifiable individual" is becoming available or is being "disclosed" (see C-362/14, paragraph 45) to anyone in a third country.

- Use Cases 6 and 7 are cases where a transfer in violation of the GDPR is already assumed, so that the ineffectiveness of supplementary measures is essentially a foregone conclusion.

- Due to the wide-ranging impact that use cases (as 6 and 7) will have on a vast number of companies – the majority of those in the EU using software and cloud services provided in third countries, including SMEs, but also on almost all multinational companies sharing HR or business client data, include in all Use Cases, and specifically Use Cases 6 and 7, that these are theoretical examples based on a limited set of factors, and that the reality can bring about many more factors that exporters and importers will have to take into account. This is especially important because (i) Use Cases 6 and 7 reflect a negative outcome for various cloud-based business applications and for the reality of necessary data sharing within multi-national companies; and (ii) the EDPB mentioned that the Recommendations will serve as guidance for supervisory authorities' enforcement of the GDPR.