AMETIC's comments to the EDPB's recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

AMETIC represents the digital sector in Spain. Our members supply both goods and services, as well as digital content and services.

We consider the flow of data to be a fundamental part of the economy. In fact, data flows between the US and Europe represent approximately $ 1.3 trillion a year. At the same time, we are fully aligned with the objective of increasing citizens' trust in digital services, ensuring an adequate level of protection, especially in relation to privacy and other fundamental rights and freedoms. Our members are truly committed to protect their users and increase their trust in the services provided.

We would like to emphasize that we are in a globally interconnected economy. Digitization is a highly relevant factor that allows a greater connection between companies and users and customers. In this sense, data transfers are a reality that not only affects large companies but also the thousands of small and medium-sized companies that make use of cloud services, social networks or online video-conference systems, among others, that allows them to start and develop their businesses and in which they trust international suppliers around the world. Today, practically no organization, irrespective of sector, would be able to do business, let alone take part in international trade, without the ability to transfer data cross-borders. **Data flows play an invisible but structural role in the delivery of products and services that EU citizens rely upon in day-to-day life.**

We welcome the EDPB's public consultation period on the Recommendations 01/2020 to discuss supplementary measures to promote compliance with the EU Court of Justice's recent decision in *Schrems II*, as this is an important issue and an opportunity for stakeholders across all industries to provide input. Nevertheless, the EDPB has given interested parties until only 30 November to provide their views. We believe it is too short in light of the ramifications such guidance will have on the EU's relationship with the rest of the world and the lack of any industry consultation in the almost 5 months that have elapsed since the date of the CJEU ruling.

Among the points that our association might wish to raise with the EDPB are the following:

- **The Recommendations are overly prescriptive and place a heavy burden on organizations that may not always have the capability to achieve and maintain compliance.** They 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.
- **The Recommendations will impact on fundamental rights, competitiveness and security.** As said in the above paragraph EU organizations, especially SMEs, will struggle to implement EDPB's Recommendations. The cost of reinventing the way advanced internet-based services operate is high and would take time to develop. EU businesses' ability to compete in a global market will be significantly diminished if they cannot utilize modern digital services. Further, we note that the Recommendations may force EU companies to use less secure and reliable services that meet the EDPB's Recommendations, but at the expense of fundamental rights, e.g., by exposing sensitive data when breaches occur or rendering data unavailable to data subjects.
- **The Recommendations undermine and will damage EU businesses and EU citizens rights and opportunities** by failing to adopt a proportionate and risk based approach and by not acknowledging the importance of other fundamental rights and freedoms, including the right to freedom of expression and information (Articles 11 and 7 of the EU Charter of Fundamental Rights) and freedom to conduct a business (Article 16 of the

Charter). The right to the protection of personal data must co-exist and be balanced against these other fundamental rights.

- **The Recommendations also ignore the recent CJEU case law that confirms that Member State national security can justify serious interference with individuals' rights. The Recommendations essentially require organizations to implement specific technical measures in order to rely on the SCCs in many cases and preclude reliance on organizational, contractual and other measures.** In doing so, the Recommendations depart significantly from the wording of the GDPR and the CJEU *Schrems II* ruling – neither of which prioritized technical measures over and above other types of measures, such as organizational, contractual or legal.
- 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.
- ***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.

We would like to point out the following suggestions:

1. *The Recommendations should consider GDPR's risk-based approach*

We consider this approach essential to any risk management strategy and thus business planning. Currently, the Recommendations do not distinguish categories of data; therefore, service metadata, configuration checks, or logs that may contain identifiable information would get the same treatment as gender, medical status, sexual orientation, political affiliation, or religion data. The risks inherent to those to the rights and freedoms of natural persons are very different. Also, the Board eliminates the possibility to take the likelihood into account, which is a fundamental part of the GDPR (art 24, 25, 32, 34) and Recitals (75, 76, 77, 90) and any risk assessment in line with widely accepted international standards.

Given the rapidly changing technological landscape, we encourage the Board to establish clear technical requirements rather than prescribing technical solutions and rely on

external market standards to ensure that organizations implement effective technical measures. Technical requirements should state clearly, for each category of personal data, what type of threat organizations should protect against. We suggest the Board state that organizations are free to use any combination of technical, legal, and organizational controls, provided that they can demonstrate that those controls can neutralize the stated threat.

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 organisations 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 organisation 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), organisations 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 in order 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 organisations from engaging in these commonplace and essential business activities.

In reality, most EU organisations 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 organisations 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.

Besides, the Executive Summary also 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." The Board may wish to consider the further doubt this will cast on the future of most all data transfers from the EU to any third country that doesn't have an Adequacy agreement under the GDPR. Therefore, a near-term EU-US political agreement on an "enhanced Privacy Shield" is vital to both economies and this must be addressed urgently by EU policymakers. This will bring not only necessary 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, in particular during COVID-19.

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 organisational 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 be based on the assumption 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 honour 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.

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 organisations 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 organisation.

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 organisations to rush through changes to their data transfer practices—making it far less likely that organisations address these issues carefully and precisely.

In order to ensure that international transfers of personal data can be maintained in a way that guarantees legal certainty and the fundamental rights and freedoms of all EU citizens and organizations, we suggest that:

- The EDPB considers extending the period for consultation, due to the relevance of this subject and high implications for a wide range of industries and thousands of companies.
- The EDPB ensures that the appropriate channels of communication are created to enable all relevant stakeholders whose interests are going to be affected (including economic, health and surveillance authorities at the EU and Member States level) to enter in constructive dialogue with them.
- The EDPB to understand the need to avoid an overly restrictive approach and to adopt a pragmatic one. It is essential to keep a holistic view in a matter like this one and to balance data protection rights with the economy, scientific research, social well-being, development of other fundamental rights and freedoms and security in the EU.
- The EDPB works towards enabling transfers rather than prohibiting them.
- The *Recommendations* to encourage organizations to take into account 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 organisations to adopt any supplemental measures.
- the EDPB to 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 organisations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorised access.
- the *Recommendations* to 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 organisations 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).
- 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 organisations to address these issues thoughtfully, while also encouraging good-faith, collaborative solutions to these quite difficult legal and technical issues.

In addition, we would like to point out a more specific contribution to the Recommendations:

1. Executive Summary

- In the executive summary as well as throughout the text, the 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. Generally, the 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 Art. 5 (1).

- In the first step "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.
- In the second step, 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_derogati o ns_en.pdf
- In the third step, 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 also 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." The Board may wish to consider the further doubt this will cast on the future of almost all data transfers from the EU to any third country that doesn't have an Adequacy agreement under GDPR.
    - Therefore, as previously raised by a wide range of trade associations from different industries and sizes, a near-term EU-US political agreement on an "enhanced Privacy Shield" is vital to both economies and this should be addressed by EU policymakers. This will 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.

2. 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. E.g., 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, so the accountability principles as enshrined in Art 5 (2), would have to be applied very loosely to make it relevant for 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.

3. 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)". The Recommendations need to add guidance 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 makes reference 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. The data minimization principle puts 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. In conclusion, 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.

- 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".
    - The Board should 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 has to 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.
    - Last but not least, the types of scenarios described would not even be "transfers" in many cases. In Footnote 14 the EPDB makes reference 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)". The Board may wish to reconsider 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.

4. 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. The data minimization principle puts 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.

5. 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 makes reference 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 endeavour 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 carry 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 makes reference 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 actually 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.