Warsaw, 18 December 2020

IAB Poland's comments

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

We welcome the EDPB's public consultation, as well as its decision to extend the period for comments until Dec 21, 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 the following areas of concerns and make a few initial suggestions to contribute to the public consultation which we believe the Recommendations should take into consideration.

1. General Remarks

● **Legal nature:** The EDPB published Recommendations 01/2020 rather than Guidelines. There's a distinction between Recommendations and Guidelines, especially from a legal perspective that should be explained.

● **Grace period:** While we recognize the submission of the Recommendations to public consultation, it's important to note the affirmation that they "will be applicable immediately following their publication". Due to the relevance of this subject and high implications for a wide range of industries and thousands of companies, the Board may wish to revisit the immediate effects of these Recommendations to consider appropriate measures to review the contributions it will be receiving during the public consultation period and provide data controllers the necessary time to implement the Recommendations.

● **Political agreement:** The Executive Summary also states that "*you 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 the 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 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.

● **Risk-based approach:** We encourage the Board to abide by and consider GDPR's risk-based approach, which is essential to any risk management strategy and thus business planning. Risk-based approach and allowing the data exporter to indicate the Data Transfer Assessment enable implementation of different level of technical and non-technical measures providing the legality of transfer. The types of technical and non-technical measures should be

adjusted to the level of risk for the data subjects whose personal data are transferred to a third country. Recommendation clearly show preference for the rights-based approach, despite the fact that the risk-based approach could become central to legality of transfers. The rejection of the risk-based approach by the EDPB is unjustified.

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.

● **Technological neutrality:** 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.

The list of technical measures is non-exhaustive and might offer room for other solutions but the examples put forward lead to the conclusion that the EDPB will accept the legality of transfers only if the data are rendered non-readable for the importer in the recipient country.

These technical measures are considered effective only if:

a) data are strongly encrypted and the importer does not have the key;

b) if data are pseudonymized and the importer has no way of identifying;

c) multi-party computation is provided.

On the other hand, the EDPB clearly rejects in Paragraph 87-91 two scenarios accounting for the vast majority of transfers to a third country:

a) first **it is not possible for a data exporter to use a hosting or a cloud service provider in order to have personal data processed according to its instructions in a third country**,

b) and, second **it is not possible for a data exporter to make personal data available to entities in a third country to be used for shared business purposes**.

The EDPB should consider the ability to implement technical measures other than strong encryption or strong pseudonymization in transfers where according to the data exporter assessment there is no high risk of violation rights of data subjects whose personal data are transferred to a third country. This technical measures could be further supported and reinforced by the contractual and organisational measures implemented by the data exporter.

The EDPB seems to reject the use of non-technical measures without technical measures being used simultaneously. The Paragraph 48 and 122 of the Recommendations reads as follows:

> *"Contractual and organisational 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). Indeed,*

there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes".

"As said, contractual measures will not be able to rule out the application of the legislation of a third country which does not meet the EDPB European Essential Guarantees standard in those cases in which the legislation obliges importers to comply with the orders to disclose data they receive from public authorities".

The EDPB seems to indicate that contractual or organisational measures may only complement but may not be a substitute for technical measures and the only function would thus be to strengthen the overall level of protection of data.

If data exporter could rely on the risk-based approach the non-technical measures should be considered as sufficient to provide transfers legality when according to Data Transfer Assessment there is a low risk of violation rights of the data subjects whose personal data are transferred to a third country.

If third countries are not considered as adequate then data transfers to them are lawful only if supplemental measures are adopted by the data exporter. The EDPB *Recommendations* seems to prohibit almost all such transfers when the personal data is readable in the third country.

The majority of exporters will find it very difficult to implement such measures. These exporters will have three choices:

a) continue operating as usual that will be fully in breach of the CJEU/EDPB requirements.

b) stop activities that involve international data transfers or localise data in Europe – solution that could incur substantial costs and disruption.

c) welcome the risk-based approach policy trying to supplement technical measures with contractual and organizational measures – despite the fact that the EDPB has expressed doubts about whether this might be sufficient.

● **Impact on fundamental rights, competitiveness and security:** EU organizations, especially SMBs, 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.

2. 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). Therefore, we suggest the Board to incorporate a clear explanation of the relevance of the principle of accountability in this context.

● 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 minimisation principle. However, the data minimisation principle is misapplied here. The data minimisation 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 focussed 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 in its Guidelines 2/2018 on derogations of Article 49 GDPR:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_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). In addition, Recital 20 and clause 2(b)(i) of the new draft SCCs recently published by the European Commission and also open for public consultation, refer to the specific circumstances of the transfer, including: the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred. In sum, 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 the likelihood as irrelevant 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.

3. 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. Therefore, we suggest the EDPB deletes this statement or to limit it in accordance with GDPR without creating additional obligations not enshrined in the law.

● 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.

4. Roadmap: Applying the Principle of Accountability to Data Transfers in Practice

● Paragraph 8 states that " the first step is to ensure that 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 unauthorised 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 unauthorised 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. Additionally, 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 unauthorised access to such data.

● Paragraph 11 refers to the principle of data minimisation 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 minimisation principle is misapplied here. The data minimisation 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 focussed on that transfer.

● Paragraph 42 seems not to take into consideration the risk-based approach characteristic of the GDPR, which is one of its fundamentals and 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, or simple service metadata would get the same treatment as special categories of data (racial, sexual orientation, political affiliation). 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, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. Such elements, data type and varying likelihood of risks, need to be factored into the Recommendations in order to align them with the GDPR.
- From a technical perspective, we note that while full copies of data can be stored in Europe, the free flow of metadata, logs, and identities is necessary to ensure a correct functioning of services in a digital economy as well as their security and reliability.
- 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 public authorities' access to 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 organisations 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 organisational 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 organisational 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.

5. 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 minimisation principle is once again isapplied. The data minimisation 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 focussed on that transfer.

6. Annex 2 - Examples of Supplementary Measures

● Paragraph 75 (a) states that "[p]ublic authorities in third countries may endeavour 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.

7. Technical measures

General Remarks

● We encourage the Board to consider a risk-based approach, essential to any risk management strategy.

- The Recommendations do not distinguish categories of data. IP addresses, simple service metadata, or service logs would get the same treatment as 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 any risk assessment in line with widely accepted international standards. 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, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. Such elements, data type, and the varying likelihood of risks need to be factored into the Recommendations to align them with the GDPR.
- The likelihood of probability is an objective factor, and probability is relevant if the GDPR's rules are applied in line with the principle of proportionality. Again, declaring likelihood as irrelevant could lead to a further interpretation that even public authorities' access to data would not be in line with EU standards.
- As previously mentioned, 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 organisations based on context and risk, rather than prescribe strict technical or procedural requirements.
- To be consistent with a risk-based approach, organizations would have to assess the risk of transferring data in the context of the specific situation. They may choose to perform these assessments based on the type of data processed, the purpose of the transfer, duration or frequency of the transfer, etc. Depending on the specific context, organizations may choose different types of technical measures instead of solely relying on customer-controlled keys. For instance, sensitive business information could be protected by access management controls limited to a business function (like HR), regardless of the employees' location accessing the data. While in other scenarios, access management with geolocation controls would be more suitable.

● We encourage the Board to consider a new approach to technical measures.

- 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 technological measures.

- Technical requirements should state clearly, for each category of personal data, what type of threat organizations should protect against. We suggest the Board clarifies that organizations are free to use any combination controls, provided that they can demonstrate that those controls can neutralize the stated threat. Examples of technical controls, in addition to encryption, might include access controls, escorted access, and policy systems.

● We suggest the Board consider improvements to its approach to encryption and remote access.

- The Recommendations call for "flawless" implementation and references other terms that are not generally accepted in the encryption world. The Board may wish to consider aligning the definitions and controls outlined in international standards and industry-accepted encryption terms.
- The Recommendations represent a technically infeasible view on how encryption works in practice. In paragraphs 79, 84, and 89, the Board suggests that in most cases, organizations can only rely on encryption as a safeguard if the data never appears in an unencrypted form in the third country and if the decryption keys are held within the EU (or another adequate country). We want to caution about potential unintended consequences of use cases 6 and 7:

  ■ Routine business operations such as sending emails or messages, using online collaboration tools, videoconferencing, or processing payments require data to be available by the SaaS provider in decrypted format. Without global SaaS, EU organizations' ability to compete in a global market will diminish due to a lack of flexibility and overhead. Further, EU businesses operating internationally (or aiming to) have typically staffed or outsourced support operations to "follow the sun" that necessitate clear-text access. If employees outside of Europe cannot have remote access, there will be gaps in operations in all sectors- from small businesses that use ecommerce platforms to big organizations -will be not accessible for customers and internal users.

  ■ SaaS has a critical role to play in enabling EU businesses to flourish. Today a boutique design firm in Italy can engage with and sell to clientele in the United States because of it. This is possible due to the seamless communication and collaboration SaaS tools that are built on the backbone of the internet. Attempts to restrict such communication and free flow of data can have seriously etrimental effects to SMBs. The current set of recommendations will increment

  ✓ **Technology Divide** - Typically, (not IT-specialised) SMBs lack the tech savvy and expertise that large corporations possess. The Internet and SaaS technologies have helped level that playing field and have enabled SMBs to thrive in the face of stiff competition. SMBs turn to technology providers for rich features that help them communicate smoothly, collaborate seamlessly, break down physical/geo barriers and ultimately grow their business. The Recommendations will widen the divide - e.g. SMBs are unlikely to have the know-how to manage encryption keys. Moreover the lack of access to encryption keys will mean SMBs can no longer rely on tech provider expertise for the best/latest/greatest features that tech has to offer. They will lose out to larger corporations's tech expertise

and this will ultimately result in a huge divide with the best of technology being accessible only to large corporations/ businesses.

- ✓ Cost of Technology - SMBs usually thrive when the costs of operating their business are low. With the current set of recommendations, there is the risk of the consideration set of technology providers drastically reducing. This lack of competition will result in higher prices. Moreover the current recommendations will require companies to deal with significantly high net new costs of implementation. All this will mean a drain of valuable resources from the SMB industry and result in only large enterprises being able to afford the best of technology.

■ We also note that the Recommendations may force EU companies to use less sophisticated, secure, and reliable services at the expense of fundamental rights, e.g., by exposing sensitive data to cybercriminals using less robust platforms. Fighting cybercrime requires global data training datasets, including personal data e.g., IP addresses of potential criminals. If companies must restrict/localize these threat models, they will have blind spots, and EU data subjects are much more vulnerable to a malicious actor. These security implications impact EU rights and freedoms much more so than the likelihood of a downstream 702 FISA request on such data. Security measures are usually reliant on exposure to attacks/vulnerabilities to "learn" how best to deal with them. As an example, a phishing attempt originating in any single country in the world is useful information for an anti-spam model to identify & prevent similar phishing threats in other parts of the world. By restricting free flow of information we render machine learning models useless thereby greatly compromising security. This will ultimately lead to a proliferation of malicious activity.

.

- 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. In particular, the Board may wish to consider

■ Access management and approval (e.g., Fine-grained controls allow administrators to set roles and policies governing exactly who within an organization has access to what data and preventing employees on the provider side from accessing data without explicit approval by the customer).
■ Supervised access to personal data by an authorized European third party to ensure that personal data is only processed according to customer instructions.
■ Further, in line with a risk-based approach, the Board may wish to call out limited circumstances during which this plain text access is acceptable and outline mitigation measures to ensure that the access to that plain text data is temporary and that any clear text data access is terminated (or the plain text data is destroyed) and a certification is made that the access was for specific purposes and the data was not provided to third parties.
■ Confidential computing can potentially evolve in this direction with providing systems where there is no law enforcement access and no administrative access.

● We suggest the Board elaborates on its legal assessment around remote access. GDPR and the ruling focus on EU personal data transfers, i.e., data storage in a third country.

However, the use cases outlined in the Recommendation go far beyond this, making in practice that any potential non-EU access becomes illegal. One may wonder if any EU-originated website or digital service containing personal data must be blocked from being used from third-countries. This will prevent EU organizations from exporting their services overseas, not be in line with the spirit of the GDPR, and ultimately undermine other fundamental rights such as the right to conduct a business. 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.

● In addition to the use case of remote access for business purposes, the Board may wish to consider supervised access to personal data by an authorized European third party as an effective supplemental measure to ensure that personal data is only being processed to provide the service contracted and that the actions performed do not transfer the data out of the EU.

● 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 pseudonymised data", the EDPB "considers pseudonymisation 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, as well as to clarify its understanding of the concept of "data in the clear".

● 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.

Kind regards,

Włodzimierz Schmidt
CEO & President of the Board

Związek Pracodawców Branży Internetowej IAB Polska
ul. Puławska 39/77 02-508 Warszawa tel. +48 22 415 54 44 fax + 48 22 212 87 74
www.iab.org.pl