ADIGITAL

contribution to the European Data Protection Board public consultation

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

I. Introduction

Adigital is the Spanish Digital Economy Association. Formed by a network of more than 500 associates from key sectors, it aims to promote and support the development of the digital economy in Spain through the development of information society services, ecommerce, digital marketing and communication, digital content, mobile applications and other related activities.

Adigital would like to raise very strong concerns following the publication of the European Data Protection Board (EDPB) Draft *Recommendations* 01/2020 on measures that supplement transfer tools to ensure compliance with the European Union (EU) level of protection of personal data (the *Recommendations*), currently open to public consultation until 21st December 2020. In this sense, the EU Court of Justice's recent decision 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.

Adigital endorses strong protections for personal data, including when data is transferred to third countries. However, we have substantial concerns about some potential interpretations of the *Recommendations.* The European Convention on Human Rights and the GDPR provide important and valuable protections for personal data. Aspects of the EDPB's *Recommendations* provide helpful guidance in terms of how to ensure those protections are respected in relation to transferred data. Unfortunately, however, other aspects appear to go much further, and suggest a range of unworkable measures that would block or significantly impair data transfers, with little (if any) added benefit for EU data subjects.

Hence, 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.

Finally, it is important to mention some of the data provided by the recent survey launched by Digital Europe on the impact of Schrems II which results demonstrates that European companies are important users of SCCs. Moreover, the data demonstrates that 85% of companies surveyed are using SCCs, thus making them the most widely used mechanism for data transfers. According to the results it is clear that many companies are not prepared to comply with the CJEU ruling. Namely, only half of the companies estimated to use SCCs have reevaluated their use as required by the Schrems II ruling.

The survey shows that companies of all sizes, including 70% of small and medium enterprises, rely on SCCs. More specifically, 75% of the companies using SCCs are headquartered in the EU and only 13% of the respondents transfers correspond to US- headquartered.

By industry sectors the following rely on SCCs for the transfers of personal data: information, media and telecommunications sector (37%); manufacturing sector (22%) ; professionals, scientific and technical services (15%), amongst others.

II. General comments

As previously mentioned, the ability to transfer data internationally is an inherent part of the global economy's operations and social exchanges. In fact, organisations of all sectors within the EU, whether public or private, EU multinationals and SMEs, heavily rely on the possibility to transfer personal data to third countries in order to be able to provide their services in the EU and around the world. Today, practically no organisation, 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.** Thus, cross-border transfers of personal data are an integral part of the day-to-day operations of most organisations in Europe. Companies in a diverse range of sectors, including healthcare, transport, retail, and financial services, as well as public sector bodies, routinely rely on the standard contract clauses ("SCCs") and binding corporate rules ("BCRs") to transfer data. These transfers take many different shapes and forms, involving many different types of data, different processing purposes, and different recipients in different locations. In many cases, the transferred data is of no conceivable interest to third-country national security authorities. **The *Recommendations* don't reflect the importance of the specific circumstances of a transfer,** however. Instead, they suggest that organisations must adopt further safeguards any time there is even a theoretical possibility that data may be accessed. Because there is a theoretical possibility that data may be accessed almost any time a company uses the Internet to communicate with people outside the EU, or shares IT functionality with non-EU entities, this means additional safeguards will need to be employed in almost every business transaction—regardless of the risk of access.

The Recommendations fail to have regard to this reality and that the overly burdensome and prescriptive approach it sets out is likely to have very **far-reaching negative impacts on the fundamental rights and freedoms of EU citizens and of EU organizations and on the EU economy** and way of life more generally. Moreover, they reflect a failure to take into account any of the other rights and freedoms enshrined in the Charter of Fundamental Rights as well as other legitimate interests, including the present and future of the EU economy, the social well-being and health of EU citizens and EU security that requires a global approach.

The Recommendations are overly prescriptive and place a heavy burden on organisations that may not always have the capability to achieve and maintain compliance. For example, the roadmap requires a detailed analysis of the characteristics of every transfer, an assessment of all applicable local laws - this is a highly complex assessment requiring specialist multi-jurisdictional legal advice, to be routinely re-evaluated, which many businesses will not have available to afford. In addition, the cost of implementing some of the actual recommended safeguards would make many businesses unviable or prohibitively onerous.

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 Charter) 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 specifically call for additional supplementary measures that make access impossible or ineffective in the third country. In practice, this would prohibit any EU business from relying on many global service providers that provide communication services (e.g., email, videoconferencing, posts, etc.) or money transfers that must access communications or related personal data to deliver these services.

Further, the safeguards proposed in the *Recommendations* are disproportionate. The Draft *Recommendations* not only require that safeguards be applied where there is a theoretical possibility of access; they go further, and state that, generally, organisational and contractual measures won't suffice to overcome access to personal data by public authorities and instead **technical measures are required—again, without giving any consideration to the context of the transfer and the level of risk involved.** Thus, it proposes a non-exhaustive list of technical measures that data exporters can use to supplement the safeguards in the SCCs. 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. Unfortunately, the *Recommendations'* case studies on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice.

The *Recommendations* indicate that, to be sufficient, technical measures must impede all government access to data (e.g., para. 48), including through encryption of data that is "flawlessly implemented" and resistant to cryptanalysis (e.g., Use Case 1). It is unclear how a company can "flawlessly" implement encryption, or effectively prevent a foreign government, with all its resources and tools, from accessing data. Further, the suggestion that data must

always be encrypted at rest, with all encryption keys held solely in the EU (or other adequate jurisdiction), is practically impossible. Any use of data, such as sending emails or texts, processing customer payments, or engaging in business collaborations, requires data be available in a decrypted format. By applying these extreme safeguards to transfers regardless of risk, the *Recommendations* will disrupt many transfers that are low or no-risk, and in many cases make transfers impossible altogether, including in cases where the transfer of data would be tremendously beneficial to the data subject or society more broadly, such as the transfer of health data, when subject to significant safeguards, as is necessary to address the global health crisis.

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, paragraph 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.

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 organisations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorised access.

Ultimately, the EDPB *Recommendations* will undermine, rather than enhance, privacy as cross-border data flows are an integral part of today's global economy. They will continue after the *Recommendations* are finalised. If the EDPB imposes significant hurdles on the use of the SCCs (and other measures under GDPR Article 46), data exporters may well try to rely on the derogations set out in Article 49 of the GDPR. In contrast to the SCCs and similar mechanisms, the Article 49 derogations include very limited safeguards to protect EU data subjects.

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, Adigital strongly encourages the EDPB to:

- **Be clear that context matters**. The *Recommendations* should explicitly acknowledge that, in determining whether and what safeguards to apply, data exporters can and should consider the specific circumstances of the transfer —including the likelihood, based on documented expert analysis, that third-country national security authorities will in fact access the data, the scale and frequency of the transfers, the type of recipient, the purpose of processing, the nature of the personal data transferred, and other relevant factors.
- **Risk-Based Approach:** The *Recommendations* should adopt the risk-based approach of the Schrems II Decision of the ECJ (Judgment in Case C-311/18) and the corresponding fundamental principle enshrined in the GDPR. The exporter (assisted by the importer) should be able to factor in all relevant subjective or objective criteria to assess the risk of a transfer to a third country on a case-by-case basis. This should include the likelihood of access, interference or request by a foreign government. Likelihood and precedents based on experience cannot be the only factor, but exporter and importer should be able to predict the realistic risk of specific transfers based on prior access requests of public authorities[1]. The likelihood based on the (objective) amount of executed access requests by public authorities is a key component of the

[1] European Court of Justice (ECJ) emphasized that evaluating the validity of a transfer must take into consideration "all the circumstances of the transfer" (See Schrems II, Paras. 112, 113, 121, 146, 203.3).

risk assessment, as the realistic risk of being subject to such a request varies significantly based on the business model of the exporter and importer (data transfers for business purposes vs. social networks), and the data category (business data vs. private information).

***Recommendation*:** Add 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. Clarify paragraph 42 to set forth that, when legislation in a third country may be lacking, likelihood of access cannot be used as the sole criteria to determine the risk but needs to be factored in the assessment.

- Also, the importance of contractual and organisational measures should not be overlooked. While contract verbiage does not bind third countries' authorities by nature, any importer's commitment to challenge, redirect or pushing back a government request, as well as and transparency measures to inform the exporter / controller of any such request, is of paramount importance to determine whether interference will effectively take place. Thus, not only technical, but also a combination of contractual and organizational measures can ensure an essentially equivalent level of protection for data subjects in practice[2].
- Organisational measures such as ISO certifications are also certified mechanisms under GDPR and the global nature of these standards can efficiently help global businesses assess and comply with relevant privacy laws, particularly if the standard is updated to address specific issues such as local surveillance laws.

  Recommendation: Amend 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, include a reference to contractual and organizational measures in paragraph 33.
- **Security and Encryption:** Hampering data flows is not only detrimental to companies, big and small, whose activities include transborder data processing but also more importantly, to the security of data.
- Global cloud service providers offer cutting-edge security services, currently protecting sensitive data from attacks by state-of-the-art protection measures. The Recommendations could incentivize data controllers to prefer less secure service providers only because of local processing, over those which process data also in third countries to avoid complex risk assessments and monitoring obligations, which would be especially challenging for SMEs. This would considerably lower security standards, which in some cases could have life threatening consequences (e.g. if a maintenance team of specialists located in the US needs to intervene and access data to solve a critical incident happening at night in an EU-based hospital).

[2] Cf. also ECJ Judgement, Schrems II, Paras. 137, 148.

- While encryption can provide strong protection against access to data, including bulk data collection by governments, it can only serve as one of several potential measures to protect personal data in transition and "at rest" (i.e. when stored on a cloud provider's servers). The reason is that encryption might impact certain processing activities, e.g. certain operations in the course of a SaaS offering, when datasets are analysed, or other computations are carried out, to render a specific service to the client. Moreover, the general requirement to apply comprehensive encryption to all stages of the data processing would result in companies having to implement very costly encryption methods even in cases where the risk (taking into account all factors, including the likelihood of access) is very low. Such encryption measures would be disproportionate, and particularly burdensome for SMEs.
- Most importantly, strict prohibitions of decryption at any point in the processing undermines IT security as technologies such as packet inspection hinder the transfer of malicious traffic and to absorb DDoS attacks. Decryption of the packets is necessary to do this analysis. If this measure is prohibited, many businesses would struggle to maintain a high level of IT security, significantly damaging the resilience and security of the IT network and critical infrastructure.
- With growing digitization comes a growing number of cyberattacks. ENISA specifically highlighted the increasing number of phishing campaigns and ransomware attacks on healthcare systems since the beginning of the COVID-19 crisis[3]. The reality of today's cyber threat landscape means that Europe cannot afford to lower cyber security standards or compromise the resilience of its critical infrastructure by hampering access to security solutions and measures.

  ***Recommendation*:** The 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 recommendation 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.
- **Enforcement and Compliance Issues:** We appreciate the pragmatic effort of the EDPB to clearly outline the process to be undertaken, illustrated with examples, but some aspects of the Recommendations remain disconnected from the reality of the industry and are extremely burdensome, especially for small and medium enterprises. For example, in paragraphs 10, 31 and 33, the EDPB refers to the necessity to consider "all actors participating in the transfer". This means that an exporter, assisted by an

[3] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

importer, would be required to list the full chain of sub-processors potentially in an infinite way, which in practice, in complex supply chains is close to unfeasible.

Recommendation: 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.

- Analysing applicable laws in the third country will be difficult to implement. **The detailed analysis which seems to be required by the ruling in light of the EDPB Recommendations goes beyond what can reasonably be expected from companies.** For example, the analysis made by Advocate General Saugmandsgaard Øe in his opinion of December 2019[4], based on the thorough assessments of the Irish DPC and the Irish High Court, is not the type of exercise that can realistically be performed by a company, specifically SMEs, before they start processing data in third countries. This is especially true in light of the obligation to continuously monitor all relevant aspects of the transfer, which will impede swift provisioning of services, including, for example, simply updating databases that benefit from the cloud delivery models.

  Recommendation: 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.

- **Further Concerns**

  ***Risk of non-compliance*:** The EDPB has highlighted that DPAs will be responsible for enforcing the Recommendations. 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 – DPAs may find themselves in a challenging position that may lead to inconsistent enforcement and compliance and will severely affect the European Economy.

  Recommendations: 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 multinational companies; and (ii) the EDPB mentioned that the Recommendations will serve as guidance for supervisory authorities' enforcement of the GDPR.

  Risk of limiting access to emerging technologies: At a time when Europe seeks to reinforce its capacities in high-performance computing, which will be crucial to tackle current and future challenges from pandemics to climate change, the EU runs the risk

[4] Case C-311/18, 19 December 2019.

of depriving both its industry champions and dynamic SMEs and start-up ecosystem from accessing cutting-edge technology that is available in third countries such as supercomputers, quantum computers, etc. Also, vaccines and treatments against SARS-CoV-2 could have been developed at speed because developers had access to large volumes of electronic health data and to supercomputers that rapidly searched for medicines that could be repurposed for COVID-19 treatments.

***Risk of disruption and inefficiencies in applying internal policies*:** While we understand the need to operationally implement a solid and appropriate governance to address the consequences of a government requests for access, we believe that this governance should be adapted to the likelihood of government access requests, based on experience and precedents. Also, companies should be able to freely assign and locate the teams involved in this governance, even outside of the EEA, as long as companies comply with GDPR requirements. While we understand the Recommendations in paragraph 124 to locate such teams in the EEA, possibly to limit unnecessary transfers when handling such government access requests, this is not reflective of how multinational operate most effectively: in some cases, especially when it comes to challenging government requests, teams located in the third country may be best placed to address and react to government requests.

- **Replace the Use Cases in Annex 2 with a toolbox of safeguards from which exporters can choose depending on the nature of the transfer.** The proposed one-size-fits-all approach to safeguards isn't workable, and it isn't necessary. Instead, the Draft *Recommendations* should identify a list of potential safeguards, but be clear that data exporters should be free to choose whatever safeguards they deem most appropriate based on the context of the transfer.
- **Clarify how a combination of safeguards (technical, contractual, and organisational) can be effective.** In some cases, technical safeguards can be the most effective additional safeguard, for example to avoid covert surveillance under authorities such as the U.S. Executive Order 12333. In other cases, organisational safeguards can be effective, such as to challenge orders. And contractual safeguards can buttress these measures by imposing liability on data importers to comply. To the extent that the Draft *Recommendations* can be read to conflict with such an approach, they should be revised.
- **Understand the need to avoid an overly restrictive approach and to adopt a pragmatic one.** It is essential to keep an 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. 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. For instance, 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 organisations from considering contextual factors, the *Recommendations* should encourage organisations to take into account the real-world 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.

- **Extend the period for consultation and to ensure 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.
- **Work towards enabling transfers rather than prohibiting them.**
- **The *Recommendations* to provide practical and workable guidance** that will allow for businesses and organisations to take steps to ensure that they can continue to transfer data in a manner which respects the essence of EU data subjects' GDPR rights without ignoring other Charter rights of EU organisations. The EDPB should refrain from including impossible standards such "flawless implementation" of certain safeguards which simply do not reflect the nature of technology or reality.
- **The *Recommendations* to explicitly state that GDPR and the ruling in *Schrems II* permit reliance on a combination of measures** – and make clear that there is no hierarchy of measures.
- **Align with the European Commission's** pragmatic and more realistic approach for the new set of SCCs
- **Recognize that EU and Member States institutions should swiftly negotiate with their United-States counterparts** a new mechanism to replace the "Privacy Shield", taking into account all economic and fundamental rights and freedoms, which are not absolute and that the EU and the US share common values and interests, in terms of respect human rights, the rule of law and the cybercrime collaboration.

Finally, Adigital deplores that the drafting of the *Recommendations* did not include any form of dialogue with concerned industry stakeholders. While we recognize the submission of the *Recommendations* to public consultation, it's important **to emphasize 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 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*.

Moreover, the EDPB published *Recommendations* 01/2020 rather than Guidelines. There's a distinction between *Recommendations* and Guidelines, especially from a legal perspective that we consider the EDPB should explain.

III. Specific comments on the *Recommendations* text

Accountability in Data Transfers

- **Paragraph 3** states that "controllers 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.

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 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. 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 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, unauthorised reversal of pseudonymisation, 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 inline 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* 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 "elements 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 "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)".

- 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.

- **Paragraph 54** implies 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*. 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.
  - 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 organisations to address these issues thoughtfully, while also encouraging good-faith, collaborative solutions to these quite difficult legal and technical issues.

Conclusion

- **Paragraph 65** states that "you 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 misapplied. 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 focused on that transfer.

Annex 2 - Examples of Supplementary Measures

- **Paragraph 75 (a)** states that "public 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 "public 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 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 "prior 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.