CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC

PRAGUE, 21 DECEMBER 2020

Comments on EDPB Recommendations 01/2020 (Supplementary Measures)

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

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

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

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

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

Main points:

Risk-Based Approach

The EDPB's Recommendations 01/2020 on "supplementary measures" 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 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 legislations in 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.*

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

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

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.

Recommendation: *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.*

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 EDPB 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).

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 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 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

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

lower cyber security standards or compromise the resilience of its critical infrastructure by hampering access to security solutions and measures.

Recommendation: *The EDPB Recommendations should consider 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 considered. For instance, contractual and organizational measures should be considered to sufficiently help guaranteeing the protection of personal data transferred. Technical measures should not be a "must have" to mitigate risks; they should, without any satisfactory technical measures as defined by the EDPB (which are not possible to implement for all entities because of lack of resources, budget or simply because it does not match their organization to store decryption keys only in EU), be deemed as potentially sufficient to mitigate the risks of unauthorized "massive and disproportionate" access in practice. In some instances, such will be the case (depending on laws applicable, on categories of data processed, on documentation provided).*

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 examples, in paragraphs 10, 31 and 33, the EDPB refers to the necessity to consider "all actors participating in the transfer". This means that exporter, assisted by 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 seem 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. Transfers being structural ones, a Data Transfer Impact Assessment should be submitted by-default based on a data mapping for structural & permanent transfers presented to a DPA, on request.*

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.

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

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.

Recommendation: 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. EDPB guidelines should create consistency on the process in case of enforcement: first a warning, then, should no solution be found, a formal notice, and, if the controlled entity is not in a solution-making/accountable mind-set only, decision of fining. **The level of fines should be framed by the EDPB guidelines in advance.**

Further Concerns

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 of depriving both its industry champions and dynamic SME 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 Recommendation 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.

Risk of blocking international trade: The risk-based approach that the GDPR was built around should be reflected in the guidelines. Unless the guidelines are modified they risk rendering data flows illegal and blocking international free trade. Data flows should not be illegal unless the EU Commission and EU DPAs identify a real risk of "massive & disproportionate" access to data in the country/region in question and per categories of data transferred. For example, only personal data that could possibly enter Foreign Intelligence Surveillance Act (FISA) scope in the US should be further checked.

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 refers to C-362/14 (Schrems I), paragraph 45 and this type of gaining access by a third party is not a "disclosure by

transmission, dissemination or otherwise making available", instead it is a "collection" of data by the third party.

● Paragraph 75 (b) states that "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 carries any obligation in relation to such access unless to the extent it is a result of a failure to uphold security measures in line with Art 32. The third party may be in direct violation of the GDPR by gaining this unauthorized access but not the entity whose system has been accessed in that way. Once again, these types of scenarios will not even be "transfers" in many cases. In Footnote 14 the EPDB refers to C-362/14 (Schrems I), paragraph 45 and this type of gaining access by a third party is not a "disclosure by transmission, dissemination or otherwise making available", instead it is a "collection" of data by the third party.

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

● Paragraph 79 states that "the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved". The Board may wish to provide more clarity of the implications of it. It is unclear as to why this third condition is a requirement for the measure to be considered an effective supplementary measure.

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

● Paragraph 80, which refers to Case 2 "transfer of 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.

Suggestions for specific text changes:

Paragraph Reference	**Recommendation**	**Justification**
13	Change "is also considered to be a transfer" to "may be a transfer" and cite to *Lindqvist*.	CJEU Case C-101/01 (*Lindqvist*) sets out in more detail when the mere possibility of access from outside the EEA may be a transfer.
42	Change "legislation publicly available" to "publicly available law" in the first sentence and change "legislation" in the second sentence to "law".	The law in some countries will consist of more than legislation, including caselaw and other binding rules.
42	Delete ", and not rely on subjective factors such as the likelihood of public authorities' access to your data in a manner not in line with EU standards". This change should also be made in the executive summary, in the first paragraph on page 3.	The clause doesn't comport with the GDPR's risk-based approach, and conflicts with paragraph 135 of the recommendations ("Adoption of strict data security and data privacy policies, based on EU certification or codes of conducts or on international standards (e.g. ISO norms) and best practices (e.g. ENISA) with due regard to the state of the art, **in accordance with the risk of the categories of data processed and the likelihood of attempts from public authorities to access it**.")
44	Replace "and/or" with "and".	Legislation should always be evaluated in light of binding interpretations.
44	In the last sentence in the box, delete "technical" from the phrase "additional supplementary technical measures".	The statement that FISA 702 can only be avoided by technical measures is not rooted in *Schrems II*.
48	Insert "covert or involuntary" into the phrases "will generally not overcome <u>covert or involuntary</u> access to personal data by public authorities" and "render ineffective <u>covert or involuntary</u> access by public authorities".	Organizational and contractual measures can defend against improper access via legal process, against which a data importer can defend through legal defenses.

70	Add “in relation to your data transfers” after “your assessment of the legal situation in the third country”.	This clarifies that the supplementary measures are applied on a case-by-case basis.
79	Add “on its own” to the final phrase “the encryption performed on its own provides an effective supplementary measure”.	This clarifies that in this case the technical measures are sufficient.
80	Add “on its own” to the final phrase “the pseudonymisation performed on its own provides an effective supplementary measure”.	This clarifies that in this case the technical measures are sufficient.
84	Revise the first sentence of Use Case 3 to read “A data exporter controller or processor wishes to transfer data to a destination recognized as offering adequate protection (including an EEA member state)”.	This recognizes that the risk of surveillance exists when data is transferred from EEA member state to EEA member state.
86	In point 5 of Use Case 5, penultimate sentence, replace “where such exploitation would not respect the essence of the fundamental rights and freedoms of the data subjects” with “where such exploitation would not ensure a level of protection essentially equivalent to that guaranteed within the EU”.	The reference to essence of fundamental rights and freedoms introduces a different standard from the rest of the recommendations, and one that is different from the focus of *Schrems II*.
86	In point 5 of Use Case 5, final sentence, add to the end “where such access does not provide a level of protection essentially equivalent to that guaranteed within the EU”.	
89	Add “technical” in the phrase “do not constitute a supplementary technical measure”.	The technical measures described in Use Case 6 could be combined with other supplementary measures (contractual or organizational) to meet *Schrems II* requirements.
91	Add “technical” in the phrase “do not constitute a supplementary technical measure”.	The technical measures described in Use Case 6 could be combined with other supplementary measures (contractual or organizational) to meet *Schrems II* requirements.
115	Add to the end of the second bullet the phrase “but in each case only to the extent that and as soon as it is no longer liable to jeopardise the	The conditions on notification are taken from paragraph 91 of CJEU Cases C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others*).

	tasks for which those third-country authorities are responsible".	
116	Change "consent" to "agreement".	The phrase "express or implied consent" could be misread to suggest that consent from a data subject under the GDPR can be merely implied.
117	In the third bullet, change "plant text" to "plain text".	
124	Delete "covert or official" from the first sentence.	By their nature, covert surveillance will not generate requests from public authorities. There may, however, be both unofficial and official requests, and both should be covered by internal policies.
124	Delete "which should be based within the EEA," and change "composed by experts" to "composed of experts".	There is no reason why teams dealing with government requests for data must be in the EEA. As a practical matter, it may be necessary to have individuals in the requesting country to evaluate the demands.
128	Change "if such inability would lead to a decrease of the level of protection" to "if such inability would lead to the failure to provide an adequate level of protection".	A decrease in the level of protection may not rise to the level of a failure to meet the required adequate level of protection.
136	Add "essentially" to "an <u>essentially</u> equivalent level of protection".	The CJEU standard is essential equivalence.
137	Add "essentially" to "an <u>essentially</u> equivalent level of protection".	The CJEU standard is essential equivalence.