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

Paragraph 42

> 'if you still wish to envisage the transfer, you should look into other relevant and objective factors, and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards.'

A history of lack of excessive access to data, showing the lack of likelihood of future excessive access, *is* an objective factor. It may objectively demonstrate that the type of data held by that recipient is not a type of data that public authorities wish to access. A proven low risk of access is an objective factor that should be considered, along with the nature or type of data in question.

Paragraph 44

> 'As a consequence, if the data importer or any further recipient to which the data importer may disclose the data falls under 702 FISA, SCCs or other Article 46 GDPR transfer tools may only be relied upon for such transfer if additional supplementary technical measures make access to the data transferred impossible or ineffective.'

The above sentence should be clarified to account for encryption and other types of pseudonymization, or indeed anonymization, such that 'make access to the data transferred impossible or ineffective' reads 'make access to the data transferred impossible or ineffective because any third country authorities who access the data cannot read the transferred personal data in intelligible form'.

Paragraph 53 'the data that you have already transferred to that third country and the copies thereof should be returned to you or destroyed in their entirety by the importer' should not apply where an EU processor transfers to a non-EU controller. The same point applies elsewhere, such as to paragraph 53.

Paragraph 62

> 'You must monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in the third country to which you have transferred personal data that could affect your initial assessment of the level of protection and the decisions you may have taken accordingly on your transfers.'

But why should it be necessary to monitor laws or regulations in third countries in cases where *technical* measures such as encryption have been deployed against authorities reading transferred personal data in intelligible form?

Paragraph 78 could also mention Article 5.1.f.

Use Cases

A general observation is that it would be helpful please to include more use case examples which illustrate the use of a combination of technical and organizational measures and consideration of a combination of technical and organizational as well as legal measures.

Thank you for mentioning MPC. It would also be helpful to include a use case involving TEEs as more and more cloud service providers are offering confidential computing services, whereby even the provider cannot see what data is being processed within the TEE or how.

Use Case 1 Paragraph 79

> 'can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them'.

The above is expressed in very absolutist terms, as is 'flawlessly' in Paragraph 79.4. However, 100% guarantees are not achievable in real life. Life is not 100% risk-free, and 100% guaranteed security is impossible. Even Articles 5.1.f and 32 require technical and organizational security measures to be '*appropriate*' to the risks, they do not go so far as to require guaranteed 100% security. The GDPR itself is meant to use a risk-based approach. If third country nation state resources and capabilities must *always* be considered to be available in relation to *all* types of data and importers, even importers and/or data whose nature is not of interest to authorities, then it could be argued that very few encryption techniques could be considered robust enough,

even to protect personal data that is stored and accessible *only* in the EU. Certain nation states could hack, and some *have* hacked, EU servers to access data. Even if personal data is stored *only* in paper form, buildings, rooms and safes can be broken into and the data stolen, including by third country nation states.

Likewise, in Use Case 3 Paragraph 84.3 'decryption is only *possible* outside the third country in question' is expressed in very absolutist terms, as is '*guaranteeing*' in Use Case 4 Paragraph 85.4, 'ruled out' in Use Case 3 Paragraph 84.10, and 'tamper-proof' in Paragraph 106. Please consider taking a more risk-based approach, where the measures must be appropriate to the risks in light of the nature of the data, the nature of the importer, etc.

Use Case 2 Paragraph 80 in 'it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information', 'the algorithm or' should be deleted. Also, changing "repository" to "key" would be more accurate. As the EDPB must know, it is the key (digital or otherwise) that the exporter must retain. In cryptography, under Kerckhoff's principle, *algorithms* should not be secret or controlled only by one person, but instead the algorithm should be public and only the key kept secret.

Use Case 3 Paragraph 84.10 in'the existence of backdoors (in hardware or software) has been ruled out', 'networking' should be inserted before 'hardware' and 'software' both. If the exporter's hardware *generally* has backdoors, transit through third countries will not be its main concern!

Use Case 4 Paragraph 85

Sub-paragraphs 1 and 2 are unclear in the way they refer to 'exempt' and 'exemption'. Are they supposed to refer to third country laws that *permit* the third country importer to access the transferred personal data and related keys and credentials? That is *not* the same as third country laws that impose a duty of professional secrecy on the recipient and it must be the case that the latter is what matters, see GDPR Article 45.2.a 'professional rules', *together with* encryption of the data before transmission.

Sub-paragraph 3 'the data importer does not employ the services of a processor in a way that allows the public authorities to access the data while held by the processor'.

It is unclear what 'in a way that allows' means, please provide concrete examples of how a processor could be employed in a 'way' that could allow such access. Also, 'third country' should be inserted before 'processor' as the importer could employ the services of an EU processor.

Sub-paragraph 5 'the decryption key is in the sole custody of the protected data importer' is impossible because the exporter must also have the decryption key if symmetric encryption is used. That statement should be clarified.

Sub-paragraph 6 'the data exporter has reliably established that the encryption key it intends to use corresponds to the decryption key held by the recipient' assumes symmetric encryption. It is appreciated that this use case is only one exampe, but asymmetric encryption using different public/private keys should be permitted.

Final sentence 'then the EDPB considers that the transport encryption performed provides an effective supplementary measure' should be corrected. The use case example refers to encryption before and decryption after transmission, which is not 'transport encryption' such as TLS.

Use Case 5 Paragraph 86.5

> 'there is no evidence of collaboration between the public authorities located in the respective jurisdictions'.

If evidence of collaboration between authorities is a factor that must be considered, then evidence of an authority's previous access to such data held by a processor, or the lack thereof, should *also* be considered as a relevant factor. Some types of data are by their nature not of interest to authorities.

> 'Similarly, public authorities of either country should not have the authority to access personal data held by processors in all jurisdictions concerned.'

The above sentence is unclear, what is meant by 'authority to access' here, legal right under the laws of all relevant jurisdictions? Should there not be a carve out for cases where such 'authority' does not exceed what is necessary and proportionate in a democratic society?

Use Case 7 contains a contradiction. Paragraph 90.2 refers to the importer using data 'for its own purposes' whereas paragraph 91 refers to 'In the given scenarios… provision of the service by a processor'. If the importer in the 'given' scenario uses data for its own purposes, it is not providing a service as a processor. Also, the nature of the data should be relevant here because, for instance, human resources data is unlikely to be of interest to authorities compared with communications or payments data.

Paragraph 100(4) please clarify whether 'sufficiently detailed information on all requests of access' *includes* even access requests that do *not* exceed what is necessary and proportionate in a democratic society?

Paragraph 105 refers to on-site audits or inspections, but how can physical on-site audits effectively verify if data was disclosed to public authorities? Actually, how can even remote audits verify this issue? Even review of access logs would be very intrusive and would only reveal accesses by the importer's staff, not to whom (if anyone) the staff member disclosed the accessed data.

Paragraph 109

> '- The clauses should provide for a quick mechanism whereby the data exporter authorizes the data importer to promptly secure or return the data to the data exporter, or if this is not feasible, delete or *securely encrypt* the data'

The references to 'secure' and 'securely encrypt' should be clarified. This is because, if *symmetric* encryption is used, the importer still holds the decryption key. It seems that this paragraph must envisage changes in law authorizing 'hacking' by the third country's authorities of data held by the importer without the importer's consent or perhaps even knowledge, in which case the references make some sense.

Paragraph 115

> '- Such information on the protection conferred by EU law and the conflict of obligations should have some legal effect in the legal order of the third country, such as a judicial or administrative review of the order or request for access, the requirement of a judicial warrant, and/or a temporary suspension of the order to add some protection to the data.'

Please clarify the above, as 'information… should have some legal effect' makes little sense. It seems 'should have some legal effect' should be clarified to read 'should cover protective measures that have some legal effect'.

Paragraph 117

> '- In some situations the data subject may not be in a position to oppose the access or to give a consent that meets all the conditions set out under EU law (freely given, specific, informed, and unambiguous) (e.g in the case of employees)'

First, the above sentence is under 'Conditions for effectiveness' but it does not reflect a *condition*, it is more of a note. Second, there needs to be exceptions where consent of the data subject is not required e.g. the data is required for prevention or detection of serious crime/terrorism and the request does not exceed what is necessary and proportionate in a democratic society. 'plant text' in the sentence following the above should be 'plain text'.

Paragraph 123 'case by cases' should be 'case by case'.

Paragraph 124 please explain the justification for why the team 'should be based within the EEA'. There may be people who understand relevant EU laws and have professional duties to act properly but who are based *outside* the EEA.

Paragraph 128 'thereof' should be 'thereon'.