CRANIUM
PRIVACY & SECURITY

Dear Sir/Madam,

As a company specialized in privacy, security and data management, we have been reading the EDPB recommendations with great interest.

First and for all we want to thank you for the efforts made and further clarification provided with regard to supplementary measures for transfer tools. However, in reading the recommendations we do have a couple of questions and practical remarks:

1. The EEG (EDPB European Essential Guarantees) recommendations offer a guidance for the exporter and importer in order to assess whether or not the powers of public authorities in the third country justifiably interfere with the obligations of the importer to ensure essential equivalence. Legislation that is publicly available is being indicated as the main basis for this assessment (42). However, if this is lacking, the assessment shall be completed based on other elements obtained from other sources as indicated in 43 and annex 3. Also here, reference is made to 'legislation': how does this need to be interpreted? Does this refer to a broader sense of the word 'legislation' as compared to the reference made in 42?

2. Parties are encouraged to work together in order to determine the appropriate supplementary measures with regard to the transfer. However, some big tech companies (Microsoft, AWS, Google, Facebook, Apple...) are usually not eager to enter into a negotiation or discussion with the exporter. In practice, this would mean that an alternative would need to be looked for as no essentially equivalent level of protection can be guaranteed. This will not always be reasonably feasible.
   Is there any intention on European level to put pressure on those parties e.g. in order to organise their services such that personal data of EU citizens remain within datacenters in the EU and cannot be accessed (not technically nor legally) from the relevant third country?

3. With regard to use case 2 Transfer of pseudonymized Data: For pseudonymization to be considered an effective supplementary measure it is mentioned under 80, point 4. that the exporter should establish that the pseudonymized personal data cannot be attributed to an identified or identifiable natural person even if cross referenced with any information that the public authorities of the recipient country may possess. The question rises how the exporter (even if supported by the importer) will, in practice, be able to know which data the public authorities of the third country may hold allowing for the identification of the data subjects.
   The same question rises with regard to use case 5, 85., point 6.

4. Use case 6: if the powers granted to the public authorities of the third country to access the transferred data is disproportionate, the conclusion is that there are currently no effective technical measures to ensure an essentially equivalent level of data protection. Taking into account that contractual and organizational measures are not sufficient without the implementation of technical measures, in practice this would mean that it is currently not possible to transfer personal data in the clear at all to a country that does not provide for an essentially equivalent level of data protection? What reasonable alternatives does the EDPB have in mind in this case?
   The same concern applies, mutatis mutandis, to use case 7, described under 90.

5. Furthermore, under case 7 reference is made to infringements on 'data subject rights', is this to be interpreted as the privacy of the data subjects in general or the data subjects rights such as the right to access, erasure etc. ?

6. Regarding the transparency obligations suggested under 99 – 102:
   - We understand that this can be a means to ensure that the exporter remains aware of any changes that might result in the transfer mechanisms or any additional measures no longer being able to guarantee an essentially equivalent level of protection. However, it is also mentioned that it should help the exporter to meet its obligation to document the assessment and if necessary, desist from concluding the contract. This includes that the information would already be provided by the importer before the contract is concluded, while the suggestion in the guidelines would be to include the obligation in an annex to the contract.
   - Moreover it is not entirely clear why this transparency obligation can only apply when the legislation in the third country complies with the EEG.

   Would it be possible to provide some more clarification on this?

7. 109: Reference is made to a specific threshold agreed between exporter and importer in order for the importer to be able to already take measures without waiting for the exporters instructions. What would be a kind of threshold the EDPB had in mind?

8. Under 116 the express or implied consent of the exporter and/or data subject is suggested. In practice it could be difficult if not impossible for the importer to obtain the consent from the data subject as the importer does not have a direct contact with the data subjects. Alternatively, if the consent would be obtained by the exporter, we suppose that the general conditions for consent still apply and thus, the consent should be obtained for a specific access to the data?

Thank you in advance for your response and further clarification on the above questions and remarks. We are interested to know and see what will be the next steps on this issue.