Thank you for these useful recommendations regarding the transfer of personal data outside the EEA.

Our observation is as follows:

Step 3 of the EDPB six-step roadmap consists for the data controller to assess the effectiveness of the Article 46 GDPR transfer tool on which the controller relies, in the context of a specific transfer.

If assessment under step 3 has revealed that relevant Article 46 GDPR transfer tool is not effective, then the data controller must implement appropriate supplementary measures in order to ensure that the data transferred is afforded in the third country a level of protection essentially equivalent to that guaranteed within the EU (step 4).

The EDPB specifies that the data controller must identify on a case-by-case basis which "supplementary measures" could be effective.

In that sense, the EDPB provides in Annex 2 a non-exhaustive list of examples of supplementary measures that data controllers could consider when reaching Step 4 "Adopt supplementary measures".

Nevertheless, we note that the EDPB indicates that in the scenario where the processor in a third country access to the data in clear in order to execute the task assigned, the EDPB is - considering the current state of the art - incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.

In other words, as soon as the processor has access to the data in clear (no matter how minimal the data may be) such a data transfer does in no event meet the essential equivalence standard that EU law requires.

The EDPB adds that it does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.

This conclusion seems to us to be a very severe interpretation.

Taking into account the circumstances of the processing (*e.g.* category of data processed, technical and organisational measures implemented), do other technical supplementary measures (than fully encryption; *i.e.* the processor may not under any circumstances have access to the data in clear) not ensure an essentially equivalent level of protection to the EU?

Let's just take a very common example ('use case') to illustrate our question:

We could imagine a call centre delocalised in French-speaking countries outside the EEA where data are only hosted in EEA (not in the country of the processor), data are encrypted in transit and unencrypted data are only accessible on the importer's premises (through remote desktop protocol accessible only from a fix IP address) by very limited personnel of the importer. Furthermore, access to data is exclusively allowed in reading mode (since technical measures preventing local data retrieval

are implemented). The data accessible to the call center operator to handle the call (customer data) is not of a particularly sensitive nature.

In such a case, if the third country's laws or practices does not provide an essentially equivalent level of protection to the EU, are such supplementary measures able to ensure such protection? If not, which supplementary measures would be sufficient?

Thank you in advance for your action in this regard.

21 December 2020