

Feedback for:

Recommendations 01/2020 on measures that
supplement transfer tools to ensure compliance with
the EU level of protection of personal data
Adopted on 10 November 2020

Source:

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasures_restransferstools_en.pdf

My company delivers consultancy on the technical level for public cloud computing projects. For almost all projects when we discuss international data transfers, we face the vendor's argument "all servers are on EU territory. There is no data transfer outside EU". For example, Microsoft states that servers hosted Office 365 data are in Amsterdam, and the service is GDPR compliant. In fact, the formal entity that governs such servers is Microsoft Corp. and is covered by FISA 702 and Cloud Act to some extent. Both regulations are extraterritorial. That means that the company must comply with data disclosure orders regardless of the physical localization of servers/data.

Sentences like

"4. The principle of accountability, which is necessary to ensure the effective application of the level of protection conferred by the GDPR also applies to data transfers to third countries ..." (page 7)

can be confusing.

I'm aware that GDPR Article 44 state that:

"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, ..."

Source: <https://gdpr-info.eu/art-44-gdpr/>

However, in the common understanding, "transferring data to a third country" is associated with "physical" data movement, which is not correct, I think.

Proposed changes:

Include an explicit definition, what the "international data transfer" means.

and/or

extend sentences like mentioned above with "... an international organization governed by 3rd country's law jurisdiction ..."

I appreciate clear statements about encryption and cryptographic keys access by "data importer" (Use Case 6, page 26). This addresses the other most overused argument "data in the cloud are encrypted, and everything is OK".

Best regards,

Michał Jędrzejczak

m.jedrzejczak@b2itconsulting.eu

[linkedin.com/in/michalje](https://www.linkedin.com/in/michalje)