Comments on public consultation version of Guidelines 5/2021 – on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

Paragraph 5, 17 and 24 – very helpful – could be expanded

In my view, the most helpful part of EDPB's statement are paragraphs 5, 17 and 24 - where EDPB stresses that controllers (and processors) must comply with GDPR regardless of where data is processed. A reference to article 3 might be added in all those paragraphs.

In addition, it would be helpful it the final version included a few statements initially on the interplay between article 24/32 (the latter is mentioned several times), chapter 3 and chapter V, e.g. supplementing the following lines with further guidance:

- All controllers and processors are obliged to implement appropriate measures to ensure a level of security appropriate to the risk, in line with article 32, regardless of where data is processed. Among the many relevant factors to consider are legislation regarding government access, both territorial and extraterritorial rules. The controller and processor must thus know their data processing operations and supply chains sufficiently, so they can address relevant risks, including those stemming from conflicting norms (GDPR vs. third country laws) for personnel and entities that have key influence in the supply chain.
    - These requirements will also apply to controllers operating in a third country, but who are subject to GDPR according to article 3 (2). |
- For transfers to *processors* in third countries, the EU-/EEA-based controller will still be responsible for making sure that appropriate measures are taken to ensure a level of security appropriate to the risk (article 32) and for compliance & documentation (article 24).
- For transfers to *controllers* in third countries, the "essentially equivalent" test will include all parts of GDPR, including information security.

Paragraph 7 – the definition of a transfer seems to be too wide

The current draft has a strong focus on *confidentiality* in its definition, where one of the criteria for a "transfer" is that the exporter "discloses by transmission or otherwise makes personal data, subject to this processing, available**".**

The definition seems to blur the concept of a transfer, both by focusing on loss of confidentiality ("discloses") and by indicating that *potential* transmissions are also included ("otherwise makes … available").

I suggest that those parts of the definition are omitted. I refer to these points:

1) GDPR chapter V only uses the term "transfer".
2) A central characteristic of transfers in general is that the transferee gets *actual* control of the object. That is in line with the etymology of the word, trans (across), ferre (bear, bring), and dictionary definitions (move, copy to another, make over the possession or control). Until data has been accessed by (and thus copied to) the transferee, the potential data exporter is in full control of the data. For traditional goods a transfer would require that it has been sent/transmitted and that it has been received by the receiver. If the definition should

include data that only is on offer (is *available/accessible*), it is a large step away from the traditional meaning of the word.

3) The stated rationale for chapter V, as indicated in article 44, is to assure protection of data *after* it has been transferred to the third country ("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, ….” emphasis added). To widen the definition so it also covers situations where no data is transferred to a third country (or international organization), seems to lack basis in these motives.
4) Article 32 compels both the controller and the processor to take appropriate measures to ensure a level of security appropriate to the risk, including the risk of unauthorized disclosure (ref 32 (2)). It is hard to see how a wider definition of transfer will give a higher level of data protection.

The draft refers to the Lindqvist decision (in footnote 6), but it does not elaborate on which parts of Court’s decisions that motivates the draft’s definition of a transfer.

It is far from obvious that the Lindqvist decision supports a wide definition of “transfer”. CJEU did not define "transfer" in the judgement. It merely concluded that Mrs Lindqvist's actions did not constitute a transfer (para. 70). Parts of the judgement clearly indicate that an actual transmission of data, i.e. more than a potential transmission, is foreseen, see para 59 ("transmission of ... data"), and para. 61 ("personal data which appear on the computer of a person in a third country"). However, CJEU only assessed Mrs. Lindqvist's actions, and not the subsequent actions of the hosting provider. CJEU stated (para. 71) that since it concludes that *Mrs. Lindqvist's* actions should not be considered a transfer, and “It is **thus** unnecessary to investigate whether an individual from a third country has accessed the internet page [from the web server/hosting provider]…” (emphasis added).

Regardless of what definition the final guidelines suggest, I hope the legal reasoning is explained, including which paragraphs of the Lindqvist decision that is considered to support the definition.

Paragraphs 15 to 16 (example 5) – possibly a corner case?

Regarding example 5, I suggest that the final guidelines include any prerequisites for its conclusion, e.g. whether the remote access and transfers must be maintained without the assistance of a third country controller/processor. Network operators are typically established in their country of operation, but satellite data transmissions might be a relevant alternative that does not include processing by third country entities.