Comments - EDPB draft recommendations 01/2020

I suggest that chapter 2.3 of the draft should be expanded to include guidance on the relevance of whether the data is transferred to a third country *processor* or a *controller*. Currently the text only very briefly mentions the relevance of this nuance (para 33 second bullet point).

I submit the following observations for possible inclusion in a revised draft:

- GDPR chapter V regulates both transfers to controllers and processors in third countries. These two types of transfers differ when it comes to the requirements according to chapter V, since processors and controllers have different responsibilities in GDPR.
  - For transfers to **processors** in third countries, the processing is still within the responsibilities of the same controller as before the transfer took place. The controller is still subject to the full force of GDPR and can be sanctioned for any breach of GDPR rules. The only legal responsibility which GDPR explicitly puts on the processor, is that measures are implemented to ensure a **level of security** appropriate to the risk (art 32, the responsibility is shared with that of the controller, and the processor is also subject to instructions from the controller, art 28). Thus, the reference to "essentially equivalent" level of protection must focus on article 32.
    - Information security measures should protect against threats against confidentiality, integrity, and availability breaches (cf. art 32 (2)), regardless of the threat's cause. A threat may be realised through legal (e.g. acts of minor negligence), illegal actions or acts of God/nature; the *legality* of actions leading to a breach is not a decisive factor according to GDPR article 32, the relevant question is whether the actual level of security is appropriate to the risk, or not. Whether the attacker is a national security service (i.e. legal according to national law) or a cybercriminal, and whether the attack is carried out on site or at a distance, is irrelevant *per se* when assessing whether the processing is appropriately secured. However, such factors will often help to assess the *likelihood* of attack, since attackers that are hard to identify and punish might be more motivated for attacks.
    - All possible paths to security breaches are thus relevant, and should be appropriately assessed, including their likelihood of occurrence, as required by article 32 (1).
  - For transfers to **controllers** established outside the EEA, the term "essentially equivalent" must take into account all relevant parts of GDPR, including articles in chapter 2 to 4, and also whether data subjects have effective legal remedies within the third country.