Spolek pro ochranu osobních údajů

Comments on the EDPB's draft "Guidelines 01/2021 on Examples regarding Data Breach"

We are grateful for the opportunity to present our comments to the recently published EDPB draft Guidelines 01/2021.

General comments

We welcome these published EDPB draft Guidelines 01/2021 for public consultation. The document accurately reflects practical experience already gained with the assessment of the personal data breaches in the post-GDPR period and provides very useful guidance on how to assess them and to correctly respond to them in the light of the GDPR requirements. It does so by presenting the most common scenarios representing different areas of personal data breaches. This approach makes the document very practical and useful.

The only point for consideration we would like to mention is the fact that the level of complexity of the expected incident management rules and procedures and level of expertise might be difficult to implement in small and medium businesses.

Specific comments

- Point 8 of the draft Guidelines - "*Data breaches are problems in and of themselves, but they are also symptoms of a vulnerable, possibly outdated data security regime…*"
  The statement seems to be too far reaching. **We suggest to rephrase the wording in a less definite way (keeping room for considering the nature of the breach): *"may be also possible symptoms" or "they may also indicate vulnerability...".***
  Cases of breaches typically caused by individuals´ misconduct or inattentiveness, would not necessarily indicate a vulnerable or outdated system.

- Section 5.4 (page 25), point 105 – the **available measures suggested seem to have been inserted by mistake**. They should be related to case *No. 12 Stolen paper files with sensitive data,* which they don't (they relate to *"loss or theft of device"*).

- Points 110 and 114 - both points suggest without further specification that in case of personal data sent by email by mistake, *"the introduction of additional control mechanisms need to be considered".* In both scenarios the incident was caused by a human error. We expect employees should be regularly trained on how to handle personal data, and among other topics, on how to avoid causing typical types of breaches like sending an email by mistake to a wrong email address. That we perceive as the main mitigating measure. **However, introducing "stricter rules for sending such messages" - is not sufficiently specific.** It is not clear what qualifies

as "such message". In case No. 14, the wrongly sent email affected a large number of data subjects - is that the criteria, or is it the types of data, or both?
Moreover, the case is called *"sensitive personal data sent by email by mistake",* however, the list of data affected does not contain sensitive personal data items (it contains name, email, address, postal address and SSN of a job seeker).
In case No. 15, the case does not seem to be in any way "specific". Again, it is not clear what makes it "such message" in the meaning of point 115 of the draft Guidance.

We believe the guideline should be more specific in what qualifies as "such message" under point 110 and 114 of the draft Guidance.
Also, no recommended "stricter rules" on sending "such" messages are suggested.

We are grateful for the opportunity to provide our comments on the draft Guidelines and hope that our comments might contribute to bringing a practical feedback on a draft document we find in general very useful.

Prague, 28 February 2021

JUDr. Vladan Rámiš, Ph.D.
Chairman of the Committee
Spolek pro ochranu osobních údajů

Alice Selby, LLM, Ph.D, CIPP/E
Member of the Committee
Spolek pro ochranu osobních údajů