



To: *European Data Protection Board*

2nd March 2021

Dear EDPB Members,

Feedback in respect of: EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification.¹

Centro Studi di Informatica Giuridica (CSIG) Ivrea-Torino is a non-profit interdisciplinary association active since 2005 (www.csigivreatorino.it).

CSIG Ivrea-Torino wishes to thank you for preparing Guidelines 01/2021 and welcomes the opportunity to present our feedback.

- Among the organizational measures indicated as good practice it would seem appropriate also to mention:
 - The provision of a data *breach response plan* (roles, responsibilities and procedures for responding to incidents) [recitals 87 and 32(1)(d)];
 - the preparation of formalized operating procedures with processors and sub-processors with regard to the methods of communication and operational support in cases of breach.
- Methodological support for the identification of "high risk":
 - It should be, for such assessment, mandatory to refer to the list provided by the SAs ex Art. 35(4) GDPR (to be considered mandated also for evaluation on the occasion of data breaches?);
 - It should be useful to provide numerical indications as examples in principle as an indicative reference for the application interpretation of the concept of "large scale".
- Records of personal data breaches: do you consider it appropriate to suggest the certification of the certain date of these records?
- We also want to suggest to include cases or examples of how communication would be mandatory but should instead be postponed in order to take into account the legitimate interest of law-enforcement authorities where any disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

The President of CSIG Ivrea-Torino

Mauro Alovisio

¹ https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_it