Comments on the draft Guidelines 1/2021 of the European Data Protection Board

This paper exclusively reflects the views of its author.

On 19 January 2021, the European Data Protection Board published its draft Guidelines 1/2021[1] *"on Examples regarding Data Breach Notification"* (hereinafter referred to as Draft Guidelines or Draft).

The Draft Guidelines intend to provide *"practice-oriented, case-based guidance"* regarding data breaches. Since, however, the interpretation of the term "personal data breach" given in the *Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)* and in *WP29 Opinion 03/2014 on breach notification* is based on something else but not on the GDPR, the Draft remains controversial.

1. Interpretation of the term "data breach" in the GDPR

According to Article 4(12) of the GDPR "*'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".*

It is clear that the definition has three elements:

a) the cause: "a breach of security",
b) the effect(s), i.e. one or more of the following negative consequences:
   - the accidental or unlawful destruction of personal data transmitted, stored, or otherwise processed,
   - the accidental or unlawful loss of personal data transmitted, stored, or otherwise processed,
   - the accidental or unlawful alteration of personal data transmitted, stored, or otherwise processed,
   - the unauthorised disclosure of personal data transmitted, stored, or otherwise processed,
   - the unauthorised access to personal data transmitted, stored, or otherwise processed,
c) the causality between the cause and the effect(s): "leading to".

It is also clear that an event cannot be considered "personal data breach" (as per the GDPR) if any of the above elements [i.e. either the cause, or the effect(s), or the causality] is missing (does not occur):

   - if an event is not a "breach of security", the case will not be personal data breach, even if any of the above-mentioned effects has happened,

[1] See at the following link https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

- no “breach of security” will constitute a “personal data breach” but only those that “lead to” the said effects,
- only the five specified effects will constitute “personal data breach” (if caused by a breach of security), other negative effects cannot be regarded as personal data breach, not even other effect(s) caused by the “breach of security”. Therefore, for example, the fact that the data subject cannot have access to his/her data while the data controller has, cannot be considered a personal data breach since such effect is not mentioned at all in Article 4(12): paragraph 6 of the Draft is, therefore, legally erroneous when it refers to “loss of control over their data” by the data subjects.

Therefore, the interpretation given by the EDPB/WP29 is not in accordance with the GDPR (briefly: it is legally erroneous). Especially the classifications “confidentiality breach”, “integrity breach” and “availability breach” are misleading because the controllers may think that any of the said “breaches” constitutes a personal data breach, while only those effects can be taken into account which are mentioned *expressis verbis* in Article 4(12): since the GDPR is “R” (regulation), the controllers do not have any other obligations than those prescribed in the GDPR, and the EDPB has no authority to extend the scope of any of the provisions of the GDPR (cf. “rule of law” principle vis-à-vis the huge amount of fines): the EDPB cannot overrule the intention of the legislator.

Having regard the GDPR, controllers can, therefore, distinguish between “personal data breach” and (for example) “data processing irregularity”, the latter meaning any event where either the “breach of security” or—more frequently—the effects did not happen.

2. Application of the provisions of the Articles 33 and 34 of GDPR

It is also clear that Articles 33 and 34 are applicable if the controller established that a “personal data breach” (as explained above) has taken place (in other words: if the said event is not a “personal data breach”, Articles 33 and 34 do not apply). If an event does not constitute a “personal data breach”, the controller is not obliged to send notification to the supervisory authority, nor to communicate anything to the data subjects.

Regarding the existence of risks, according to the provisions of the Articles 33 and 34, the following types/severity of risks can be established:

- no risk, if the exception in Article 33(1) — *“unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons”* —applies,
- risk, if the exception in Article 33(1) does not apply,
- high risk [as per Article 34(1)].

It is not clear, therefore, what the Draft means—in paragraphs 74, 107 and 115—by “low risk”. Is it “no risk” or “risk” in accordance with the GDPR? What does “medium” risk/effect mean in paragraph 119? The Draft should use the terms of the GDPR instead of coining new ones.

3. Assessment of the given examples

(a) All cases should be reclassified according to the effects and the types of risk prescribed in Article 4(12) and Articles 33-34 of the GDPR.

(b) From Case No. 01 (subchapter 2.1) and Case No. 08 (subchapter 4.1), one could conclude that the controllers applied state-of-the-art security measures or all possible measures that the controllers could take under the given circumstances. If, against this background, the Draft writes about "personal data breach", it should add that the GDPR requires the controller to do more than the "state-of-the-art", in other words: the GDPR obliges the data controller to do the impossible, violating the principle of *"nemo potest ad impossibile obligari"*. Does a kind of *culpa in contrahendo* exist in data protection legislation?[2]

(c) In Case No. 01 (subchapter 2.1), the Draft did not establish any negative effects [as per Article 4(12)], therefore this case cannot be "personal data breach" at all.

(d) According to Case No. 02 (subchapter 2.2), there are several contradictions between the statement of facts and the explanation:

- the statement of facts says that *"the perpetrator only encrypted the data, without exfiltrating it"*, while paragraph 28 states the opposite (or at least challenge it), and paragraph 32 talks about *„loss of personal data"*,
- paragraph 30 contradicts paragraph 28,
- the statement of facts says nothing about *"transferring employee's payments"*, while paragraph 34 emphasises this as a factor making the case of high risk.

(e) In Case No. 03, paragraph 37 classifies the breach as an example of *„unavailability of the data"*, while such an effect cannot be corresponded to effects regulated by Article 4(12): „loss of data" means that the data get out of the (physical) possession of the data controller.

In the same case, it should be justified what the point is in informing all patients the data of whom are recorded in the compromised systems even if most of them did not affected by the consequences of the case at all due to the fact that they are not active patients at the moment of the case and the fact that the perpetrator did not exfiltrate any data. In other words: only those patients should be informed of the personal data breach whose rights were actually affected by the breach. So, the "risk" should be assessed from the perspective of each and every patient, not theoretically.

(f) In Case No. 04 (subchapter 2.4), the Draft should explain how the controller should inform its clients *"on a person-by-person cases"* (paragraph 47) if the controller does not have backup (see title of the case).

[2] See the recent case before the Polish Data Protection Authority where it was established that the root cause of the event was the *„mistake of a customer who provided the wrong e-mail address"*. The DPA failed to explain why it would not have been a „breach" if the controller had followed the advice of the DPA (i.e. verification of the e-mail address or encryption): the e-mail would have been sent to wrong addressee *necessarily and unavoidably*, irrespective of the implementation of any technical and organisational measures as advised, and the „breach" would have occurred. Imposing high fine for this is a nonsense. – https://edpb.europa.eu/news/national-news/2021/polish-dpa-warta-failure-notify-personal-data-breach-without-undue-delay_en

(g) In Case No. 05 (subchapter 3.1), paragraphs 51-53 seem to be general statements and not ones tailored to the case, therefore the justification of high risk is missing from paragraph 55.

(h) In Case No. 06 (subchapter 3.2), if paragraph 56 states that *"this case presents no risk"*, why does paragraph 59 cogitate over the need of informing data subjects? According to Article 34 communication of personal data breach is obligatory in the case of "high risk", and the controller is not obliged to consider the communication if there is no risk at all.

(i) In Case No. 07 (subchapter 3.3), paragraph 68 fails to take into account Article 34(3)(b) of the GDPR, according to which the controller does not have to communicate the personal data breach to the data subjects, if *"the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise"*. Since the paragraph 67 clearly states that the controller did adequate measures, there is no need to communicate the personal data breach to the data subjects as suggested by paragraph 68.

(j) Case No. 09 (subchapter 4.1) is completely legally erroneous. At the moment of the "breach of security", the employee had authorisation to have access to the clients' contact data. Therefore, one of the key elements of the definition of "personal data breach", i.e. "unathorised access" as an effect, is missing. Making an extra copy may be considered (unlawful) data processing activity by the employee—but the concrete case is rather a breach of the employee's contract of employment.

(k) In Case No. 12 (subchapter 5.3) the Draft lacks the backup in the case of the paper file. Does it mean that, in the light of data minimisation, controllers should double their files, in this case their logbook (paragraph 99), as well as they should create more data processing activities (paragraph 102)? The question how the personal data breach should be communicated to the data subject in the absence of the (stolen) logbook should also be answered.

(l) Paragraph 105 advises measures (for example *"turn[ing] on the functionalities of highly mobile devices that allow them to be located in case of loss or misplacement"*) that are advised against since it would represent continuous surveillance of employees. The same paragraph fails to provide the controllers with advices regarding paper files.

(m) What does constitute "sensitive" data in Case No. 14 (subchapter 6.2)? The social security number is not sensitive data *per se* in the light of Article 9 of the GDPR. Anyway, where in the GDPR should one find the term "sensitive data" as such?

(m) In the statement of facts of the Case No. 17 (subchapter 7.1) nothing refers to the fact that the perpetrator got the personal data of the offended data subject from "publicly available information". That might have come from other sources (the garbage, for example. See paragraph 119).

4. Other remarks

a) Paragraph 24 says that *"The GDPR states that a personal data breach shall be notified without undue delay and, where feasible, not later than after 72 hours. Therefore, it could be determined that exceeding the 72-hour time limit is* ***unadvisable*** *in any case, but when dealing*

with high risk level cases, even complying with this deadline can be viewed as ***unsatisfactory*** (emphasis added).*"* According to the GDPR: (a) exceeding the 72-hour limit is not "unadvisable" but a "violation of law", (b) complying with the 72-hour deadline is not "unsatisfactory" but fully in line with the GDPR, since the regulatory authority has no immediate task to do with the notification (and in the case of a high risk case, the controller has lots of other things to do to mitigate the consequences of the personal data breach). The EDPB should stop creating new obligations that are not in the GDPR.

b) Paragraph 58 says that *"Some user names could be regarded as personal data"*: does it mean that the EDPB has accepted the so-called relative approach of personal data?

c) It is not clear what EDPB considers "sensitive data" in paragraphs 51, 63, 65, 73 and 131, and in Case No. 14, because it is clear from the statements of facts that in these cases the term "sensitive data" is used in different meaning than "special categories of personal data", while in paragraph 79, and in Cases No. 12 and 15, the "sensitive data" corresponds to the term of "special categories of personal data".

* * *

In sum, the Draft Guidelines have serious deficiencies, and should be thoroughly reconsidered, by taking into account, first, the GDPR (as it was published).

Zsolt Bártfai