2 March 2021

EBF_045089

EBF response to the European Data Protection Board’s consultation on the Guidelines 01/2021 on Examples regarding data breach notification

Key points:

- The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board’s consultation on the draft guidelines on examples regarding data breach notification.
- It is important to be precise **and consistent on the meaning and interpretation of the term financial data in the final Guidelines.** The level of impact (risk to the data subjects) will differ depending on the attributes of financial data. Throughout the draft Guidance, the approach to the risk to the data subjects is an emphasis on the type of data present and a case-by-case assessment. This is not consistent with how the term “financial data” is used.
- The final **Guidelines should recognize the difficulty in determining both the impact of the risk and the probability of risk to the data subjects due to the subjectivity and fluidity of these matters,** not simply in judging how affected rights and freedoms are, but also evaluating the actions and intent of those involved (e.g., are erroneous recipients of personal data malicious / likely to misuse data, or essentially trustworthy?).
- A **reference to industry-accepted security standards and best-practices** (such as ISO 27002, NIST Cybersecurity Framework, COBIT 5…) would be welcome in the Guidance in relation to organisational and technical measures for preventing/mitigating different types of attacks.

EBF position:

The EBF welcomes the European Data Protection Board (hereafter ‘EDPB’) draft guidelines on the examples regarding Data Breach Notification. You will find below both general and detailed comments on the draft guidelines.

I. General comments

a. Provided examples

We note that the examples in the draft Guidance **are largely focused on external threats** with a few cases reserved to human errors, mainly relating to sending errors (Section 4 and Section 6), while lacking other internal processing examples. This is in spite of the reference to the Guidelines on Personal data breach notification under Regulation 2016/679, WP 250[1], footnote 13: "*It should be noted that a security incident is not limited to threat models where an attack is made on an organization from an external source but includes incidents from internal processing that breach security principles.*"

There is often less clarity on how these types of incident should be assessed and further examples would be welcome, such as a case of too wide access rights for employees (not based on a "*need to know*" principle), both IT technicians (developers/operators/system administrators) and business users.

We would also suggest including more examples in the "grey areas." For example, to further elaborate Case Number 3 – Ransomware with backup and without exfiltration in a hospital – but with fewer data subjects and a shorter time to restore all data and consequently, no cancelled procedures.

Additional guidance on the situation described in the WP 29 Guidance[2] regarding the situation that personal data is made unavailable for a period of time (pp.8-9) would also be welcome.

Finally, **including a workflow/summary of general conclusions of the different examples/typologies** in the draft Guidance (e.g., all high-risk data breaches must be reported to the SA, all no risk data breaches will not be notified to the SA) would be helpful.

b. Determining the risk

In general, the number of affected data subjects is mentioned in several places throughout the Guidance (e.g., paragraph 80) as a factor when determining the risk. **We question whether the number of affected data subjects is a factor for determining "the risk to the rights and freedom of natural persons"** and thus whether this should play a role when determining whether a data breach is high risk for the individual data subject.

In this regard, it would be useful to include guidance on the impact to data subjects to understand what does high risk entail. However, we note it should still be possible to distinguish based on the type of Personally Identifiable Information (PII).

The ENISA *Recommendations for a methodology of the assessment of severity of personal data breaches*[3] uses data processing context, ease of identification, and circumstances of the breach to assess the risk to the data subjects. These recommendations could be enhanced/revisited to help assess the risk to the data subject. Including other parameters could also be considered e.g., difference between public disclosures, internal processing error, trusted recipients.

In the event that the number of data subjects is considered as a determining factor, we would recommend establishing specific ranges. For example, in Case 1 it refers to dozens of data subjects without determining whether it is a "large" or "low" number, while in Case 9 it is determined "*The data breach only concerned **about two dozen costumers**, hence the quantity of data affected can be considered as low*."

We would also like to underline that, in the context of the risk analysis, **the probability that the risk will *not* occur is not sufficiently taken into account**. For example, in paragraph 74 (Case No.08) and paragraph 119 (Case No.16), the scenarios are formulated

[1] https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827

[2] Ibid.

[3] Recommendations for a methodology of the assessment of severity of personal data breaches — ENISA (europa.eu), 2013

in such a way that the Guidance starts from the assumption that in those cases, the risk will occur.

c. Notification to Supervisory Authorities

Regarding notification to SAs, the EDPB appears to take a stricter approach at times in relation to mandatory notifications, which need to be made promptly. On the other hand, examples have been given of cases where no notification needs to be made.

Regarding the timing of the notification, recognition is **helpfully given in the guidance to not being able to fully assess the risk arising from a breach until the root cause and continued presence of vulnerabilities has been established**.

The point is also made that the notification to the SA **does not need to be postponed, as the full risk assessment can happen in parallel to notification, with the information provided in phases**: *"The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject."* While this is a well-understood point, it **is also important to note in the draft Guidance the difficulty in determining both the impact of the risk and the probability of the risk to the data subjects due to the subjectivity and fluidity of these matters, not simply in judging how affected rights and freedoms are, but also evaluating the actions and intent of those involved** (e.g., are erroneous recipients of personal data malicious / likely to misuse data, or essentially trustworthy?).

d. Additional comments

Finally, the Guidance seems to take **an overly simplistic approach to the application of encryption to data that is at rest**. There are numerous Cases in the guidance which presume that *any* data which is at rest can be encrypted. This is not always possible or advisable for data which undergoes regular processing. It must also be noted that even encrypted data at rest can be breached – if the attacker obtains access to the encryption keys or accesses the data through approved channels which hold the keys.

II. Comments by case number/section

a. Introduction

According to Paragraph 5, data breaches can be categorized *"according to the following three well-known information security principles:*

- *"Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.*
- *"Integrity breach" - where there is an unauthorised or accidental alteration of personal data.*
- *"Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data."*

The Guidance categorizes all the examples up to Case 12 with one of these three principles. Yet the cases after that do not indicate which one of the three principles it would fall under. It would be helpful to include this categorisation in all Cases.

Paragraph 12 states that "*The training should be regularly repeated, depending on the type of the processing activity and the size of the controller".* In this sense, we consider that frequency of training and awareness campaigns **should not depend on the "size of the controller".** An SME should also train its employees on a regular basis.

b. CASE No. 01: Ransomware with proper backup and without exfiltration

We would recommend mentioning in Paragraph 19 that, when assessing the risk, the controller should also investigate the "method of infiltration" (besides the type of malicious code). The need to investigate the "method of infiltration" is included in Case 2, which is a similar Case (Paragraph 27). We therefore propose to include this action under Case 1 as well.

c. CASE No. 03: Ransomware with backup and without exfiltration in a hospital

Specifically, on paragraph 39, any public communication or announcements **would need to be balanced against the advice and guidance from Law Enforcement Agencies about the attack, especially the timing of the announcement**. If poorly timed, public announcements could reduce the chance of apprehending the cybercriminals. In general, public communication creates a situation of heightened alarm. The claims services of entities in question and the relevant SA could be significantly overloaded due to the exercise of rights of data subjects and others who are not data subjects but who "claim" as a precaution. Therefore, we would suggest for the final Guidelines **to present public communication as an option that should be carefully weighed. It may represent bigger risks if adopted without further thought simply because it is mentioned in the Guidance.** We would therefore recommend adding the following text*: "whereas public communication and announcements may be appropriate in certain circumstances, it should be noted that they may also entail risks: further attacks or attacks while the breach is still being resolved (not closed yet) and risk containment/mitigation actions are ongoing."*

d. CASE No. 04: Ransomware without backup and with exfiltration

In paragraph 43, the draft Guidance writes "*The nature, sensitivity, and volume of personal data increases the risks further, because the number of individuals affected is high, as is the overall quantity of affected personal data. Beyond basic identity data, identity documents* ***and financial data such as credit card details*** *are involved too.* ***A data breach concerning these types of data presents high risk in and of themselves****, and if processed together, they could be used for – among others - identity theft or fraud."* Stating that financial data present a "*high risk in and of themselves*" requires additional clarification. **What does the term "financial data" entail?** Currently, only "such as credit card details" is mentioned. Yet there is a broad category of information that can fall under the term "financial data".

This is further addressed below in the comments on paragraph 63 and 64.

e. Section 2.5: Organizational and technical measures for preventing/mitigating the impacts of ransomware attacks.

In addition to the specific measures mentioned in Paragraph 49, **a reference to industry-accepted security standards and best-practices (such as ISO 27002, NIST**

Cybersecurity Framework, COBIT 5…) could be included in the Guidance. We would recommend the same for:

- Section 3.4. Organizational and technical measures for preventing/mitigating the impacts of hacker attacks (paragraph 70)
- Section 4.3 Organizational and technical measures for preventing/mitigating the impacts of internal human risk sources (paragraph 84)
- Section 5.3 Organizational and technical measures for preventing/mitigating the impacts of loss or theft of devices (paragraph 105)

Coming back to paragraph 49, when listing the advisable measures, the Guidance establishes the need to "*Ensure that all reasonable IT security measures are in place*". Instead of referring to "reasonable IT security measures", we would recommend referring to "***appropriate security measures proportionate to the risks the company is exposed to***", as this takes into account **a risk-based approach.**

f. CASE No. 05: Exfiltration of job application data from a website.

The description of Case 5 establishes that "*The (malware) toolkit was discovered only a month after its installation*". The word "only" implies that a month could be an acceptable period to discover the toolkit. In this regard, we would recommend deleting "only." Security measures should have been implemented by the controller to detect the installation of the toolkit before one month.

g. CASE No. 06: Exfiltration of hashed password from a website

Technical terms linked to password security (e.g., 'salt') should be defined in order for the context to be understood by all stakeholders.

h. CASE No. 07: Credential stuffing attack on a banking website

Overall, additional context and introduction on Case 7 is necessary as the common denominator is difficult to find.

Paragraph 63 of the draft Guidance reads "*It is important to mention that controllers handling sensitive data,* ***financial information****, etc.* ***have a larger responsibility in terms of providing adequate data security, e.g. having a security operation's centre and other incident prevention, detection and response measures. Not meeting these higher standards will certainly result in more serious measures during an SA's investigation."*** The section in bold seems to imply that the data controller per se has a larger responsibility if they process financial information which is equated to sensitive (special categories) data. As mentioned above, **we would recommend being precise in the Guidance on the meaning and interpretation of the term financial data**.

The level of impact (risk to the data subjects) will differ depending on the type of financial data. Throughout the draft Guidance, the approach to the risk to the data subjects is an emphasis on the **type of data present** and a **case-by-case assessment**. **This is not consistent with how the term "financial data" is being treated where a broad brush is applied.**

Similarly, in paragraph 64, the draft Guidelines write that "*The breach concerns financial data beyond the identity and user ID information, making it particularly severe. The number of individuals affected is high."* Once more, a nuanced definition of financial data is not provided, and no explanation given as to why financial data makes a breach particularly severe.

Understanding what the term financial data is meant to entail is further complicated with its use under Case No. 16 where the Guidance writes "***payment data (bank details), economic and financial data***". It seems to indicate that payment data (bank details) and economic data is distinct from financial data without offering accompanying explanations. **There should be consistency in the terminology used.**

In paragraph 65, draft Guidance states that *"The breached data permits the unique identification of data subjects and contains other information about them (including gender, date and place of birth), furthermore it can be used by the attacker to guess the customers' passwords or to run a spear phishing campaign directed at the bank customers."* The unique identification of the data subject by the attacker can only be done due to the other information. Email address was not among the leaked data - it seems that spear phishing would not be very likely in this case.

Finally, in paragraph 68, the rationale for informing all 100,000 data subjects is unclear. The breach does not seem to pose high risks in respect of those individuals. Additional details on why a notification is necessary would be welcome.

i. CASE No. 08: Exfiltration of business data by a former employee

In this example, the specific amount of personal data obtained is not given, but the guidance suggests "the quantity of data affected is usually also low or medium" and states that no financial or special category data was included. The example notes that the breach will not result in a high risk to the rights and freedoms of natural persons, yet determines a notification to the SA is needed, on the basis that the controller does not have any kind of reassurance on the intentions of the employee and cannot rule out 'grave abuse' of the stolen data.

As it stands**, this example is confusing, as limited detail is given as to how much data was obtained.** The example states that the employee had legitimate access to the information during the course of their employment and it is implied that the employee's intention was to set up his own independent business using contact details taken from his previous role. Whilst this could be perceived as potentially intrusive, **not enough information is explored as to the subsequent harming of rights and freedoms that justifies this being a reportable data breach. We recommend providing more detail around this element of the example.**

In an example such as this, it might be helpful for the EDPB to point to **member state law on the unlawful obtaining of (personal) data as a key point of reference for controllers in this situation.**

j. CASE No. 09 – Prior measures and risk assessment

In this example, the relationship between the insurance agent and the sender of the Excel file is not clear, **specifically on whether there is a data controller/processor relationship between the two.** We would suggest making these types of details more explicit in the final Guidance.

This example also raises questions of similar situations and if their evaluation would be the same (that there is no risk to the data subjects' rights and freedoms and no need to report a data breach to the SA and data subjects). For example, in the case of:

- Where an email is sent to another client, which is not obligated by professional secrecy, but is a trustworthy company and has a long-term cooperation with data controller. The representative of the company has notified about the email themselves and confirmed that email with personal data is deleted.
- If the excel file in question would be sent to a natural person, who is also in relation with the company and he/she reported that he/she received file which is not addressed to him/her and confirms that he/she deleted the email with personal data.
- If the excel file in question would be sent to a natural person, who does not have any relation with the company, but himself/herself reported that he/she received the file which is possibly not addressed to him/her and confirms that he/she deleted the email with personal data.

Considering these questions, **can the controller use the approach of a trusted party?** If the wrong recipient can be considered as a trusted party, e.g., the recipient confirms the deletion of the data and that he/she will treat the received data with confidentiality etc., can this fact be taken as a risk mitigating measure requiring no notification to the Supervisory Authority?

k. Section 5, Lost or stolen devices and paper documents

Paragraph 86 establishes "if there is not backup for the stolen database". Since the Case is referring to lost or stolen devices, we would suggest referring to "stolen information".

l. CASE No. 13: Snail mail mistake

The advice in paragraph 108 appears to contradict itself. **Should the recipient of the data return the data at the controllers cost *or* destroy it?** They cannot do both.

Additionally, Paragraph 109 establishes that "*communication of the breach to the data subjects cannot be avoided, as their cooperation is needed to mitigate the risks*". However, in the table below, the option "Communication to data subjects" is not selected. The table could indicate that notification to data subjects is recommended. In paragraph 109 the draft Guidelines do not include why the SA should not be informed - only that it does not pose a high risk to the data subjects. We would welcome a clarification.

m. CASE No. 14: Sensitive personal data sent by mail by mistake

The term 'sensitive personal data' is often used to refer to 'special categories of personal data' under Article 9 GDPR, sometimes collectively with criminal offence data under Article 10 GDPR. It would be useful to clarify that this is not the intended meaning here, so as not to imply that social security numbers or similar identification codes are not covered by Articles 9 or 10. We recommend including a footnote to clarify this. **Indeed, the word 'sensitive' is used several times in the guidance so a more general clarification would be helpful.**

n. CASE No. 16: Snail mail mistake

Under the mitigation and obligations (6.4.2), the "notification to SA" is selected. However, the **rationale of why the notification needs to be made is not explained** in the example. We would recommend adding an accompanying explanation.

In addition, **when comparing Case 13 and Case 16, it is not clear why the breach needs to be notified to the SA in the latter but not in the former**. The inclusion of vehicle registration, insurance rates, mileage and date of birth does not seem to materially change the risk factor to a mis-mailing breach. **This creates an unnecessary degree of subjectivity in the draft Guidance whereby one is breach is reportable to the SA and one is not**. Both examples seem low risk and unlikely to require notification to the SA, unless there were some reason to think that the data might be misused, such as a threat from the accidental recipient of the data.

If these two cases do indeed involve different levels of risk, this should be explained further in the final Guidance and the type of misuse of concern should be specified.

Furthermore, in paragraph 119, the draft Guidance writes: *"The effects on the affected person are to be regarded as medium, since information not publicly available such as the date of birth or vehicle registration numbers, and if the insurance rate increases, a not insignificant claim, which could also have been an accident, was disclosed to the unauthorized recipient."* The conclusion that a rate increase which may or may not stem from a claim which may or may not stem from an accident seems odd - in combination that is provide additional risk to the data subject.

o. CASE No. 17: Identity theft

It would be helpful to add some additional detail to this example in order to clarify some key points:

- The example lists this breach as 'high risk' but, in many cases, when firms send billing notifications by email, they in fact only advise the recipient that a bill is available behind the firm's online portal. To access the information in the bill, the recipient of the email would need to log into the online portal. This largely removes the risks identified in the guidance. **It would be useful for the guidance to make a distinction between these two methods of providing a bill by email.**
- The guidance does **not consider the nature of the relationship between the client and the individual 'posing' as the client.** There is clearly a significant difference in the risk level posed by a current partner, an ex-partner or an unknown individual seeking to change the billing address. It would be useful for the guidance to clarify the relationship applicable in this example scenario.
- Paragraph 124 does not specify the breached information**. "Billing information" is much too broad** to assess the possible risks for the data subject.

Another measure to reduce the risk of this scenario arising would be, where details are changed or updated for a data subject, that the confirmation of the change is communicated to both the address on record and the new address provided to ensure transparency. Yet it must be noted that this measure could pose its own risks as well, e.g., if a physical statement is sent to both the old and the new address, then a protected address might be disclosed.

Overall, in the case of identity theft, a case study of identity theft caused by the data subject would be appreciated, as these are lacking in the guidelines.

p. CASE No. 18: Email exfiltration

Overall, the case is much too complex and specific to be related to one's own organization and thus would benefit from broadening its circumstance towards a case related to a hack.

ENDS

For more information:
Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu