[Public consultation]
02/03/2021

Comments on Guidelines 01/2021 on Examples on Data Breach Notification

EuroCommerce

EuroCommerce is the voice for over 5 million retail, wholesale, and other trading companies. Our members include national federations in 31 countries, Europe's 35 leading retail and wholesale companies, and federations representing specific retail and wholesale sectors.

Introduction

EuroCommerce welcomes the opportunity to provide comments on the European Data Protection Board's (EDPB) Guidelines 01/2021 on Examples on Data Breach Notification (the "Guidelines"). EuroCommerce appreciates the EDPB's efforts to provide clear guidelines for data controllers in regards to the obligation to notify a personal data breach to the competent supervisory authority. Data breach notification is a rapidly-evolving (and comparatively new) area of law set against – among other matters – the backdrop of bad actors who constantly change their methods of attack.

Moreover, security breaches and/or personal data breaches, are not only related to cybersecurity threats but also to other risks such as the risk of human errors or the threat of malicious use of a companies' services. The obligation to assess the risks related to a security breach and decide upon what measures to take requires cross-functional co-operation within a company and may also require co-operation with its suppliers. Due to the extent and variety of risks as well as the number of stakeholders that needs to be involved in the risk assessment process, such investigation will require sufficient time to investigate in order for the data controller to consider all risks and take the necessary measures before being able to conclude with a reasonable degree of certainty if a personal data breach has occurred, and thus becoming aware of a personal data breach. To facilitate for the data controllers' assessment, there is a great need of clear guidance on what information the risk assessments should include what the advisable measures could be and what is required by each stakeholder, including clarifications on the obligations of suppliers in case of a security breach.

In the light of the above, and as a positive contribution to the work of the EDPB, we are pleased to submit these comments for the EDPB's consideration, divided below into our (i) key points, (ii) specific comments and considerations, and (iii) requested clarifications to the Guidelines and key proposals.

EuroCommerce key points and proposals

1. Ensure harmonisation by including a roadmap with clear criteria on how to make risk assessments. It would be of great value if the EDPB could analyse the examples in the Guidelines and provide a roadmap with criteria, based on the experience of the supervisory authorities, that data controllers could use when conducting its risk assessment in connection with a security breach.

2. Amend paragraph 10 of the Guidelines and clarify that data controllers' obligations are limited to proportionate measures regardless of whether a risk later materialises. More specifically, it should be clarified that data controllers that (i) have used all *proportionate* means which are available to the data controller at the time of the security breach and (ii) *reasonably* have concluded that it is unlikely that the security breach will result in a risk to the rights and freedoms of the data subjects have satisfied their obligations under the GDPR, regardless of whether the risk later materialises or not.

3. Include a list of examples of security breaches that, in the EDPB's opinion, do not result in a risk for data subjects' rights and freedoms. Please note that EuroCommerce only asks that the EDPB includes examples where it is obvious that there is no risk for data subjects' rights and freedoms, e.g., an e-mail sent to the wrong recipient and where the e-mail does not contain any personal data other than the name and e-mail address of the sender.

4. Identify and include notification thresholds based on the experiences of the supervisory authorities. It would be helpful for data controllers if the EDPB could draw conclusions from the examples presented in the Guidelines and identify certain notification thresholds for personal data breaches. See example in paragraph 9.

5. Revise paragraph 9 of the Guidelines and clarify the data controllers' obligations. Not all security breaches are *per se* personal data breaches and the emphasis should instead be on prompt action to investigate a security breach and to take remedial action and notify, within 72 hours, when it can be established with a reasonable degree of certainty that it is a notifiable personal data breach.

6. Revise paragraph 8 of the Guidelines to better align with the requirements set out in the GDPR. We ask the EDPB to revise the wording of the paragraph to instead clarify that data breaches *may* be symptoms of a vulnerable, possibly outdated data security regime.

7. If preliminary notifications are required, the EDPB must clarify the process and consequences relating to such notifications. Notably, the EDPB must clarify:

a. what criteria need to be satisfied to trigger the obligation for a preliminary notification; this is essential to ensure a harmonised application of the GDPR;
b. what information such preliminary notification should contain;
c. at what time does the additional information need to be provided, e.g., if it still needs to be provided within the 72 hours; and
d. what happens if the data controller deems that the preliminary notification was incorrectly submitted? Will it be possible to withdraw the preliminary notification?

The EDPB's conclusions based on analysis of the examples

1. The aim of the Guidelines is to provide practice-oriented and case-based guidance regarding personal data breach notifications – a guidance that is both timely and very much appreciated. As the EDPB also points out, one of the most important obligations for data controllers is to investigate the security breach and evaluate the risks associated with the breach. Based on the evaluation, data controllers shall also implement appropriate technical and organisational measures to address them.

2. Considering these obligations, EuroCommerce has noted that the number of notified personal data breaches varies widely between EU member states. Moreover, independent guidelines from national supervisory authorities create legal uncertainty for data controllers. To ensure harmonisation on the assessment of security breaches and the obligation to notify personal data breaches, we welcome further guidance on the criteria to consider in light of the supervisory authorities' collected experience. Particularly, it would be of great value if the EDPB could analyse the examples in the Guidelines and provide a roadmap with criteria, based on the experience of the supervisory authorities, that data controllers could use when conducting its risk assessment in connection with a security breach.[1]

[1] As a reference, please see section 6.2.3 , Guide on personal data breach management and notification published by Agencia Española de Protección de Datos, https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf.

EuroCommerce proposal

Ensure harmonisation by including a roadmap with clear criteria on how to make risk assessments. It would be of great value if the EDPB could analyse the examples in the Guidelines and provide a roadmap with criteria, based on the experience of the supervisory authorities, that data controllers could use when conducting its risk assessment in connection with a security breach.

By criteria Eurocommerce refers to the objective qualification of the existence of risk or high risk based on the volume of personal data involved in the breach, the sensitiveness of the personal data involved due to the regulatory, operational or cultural reasons and exposure of the personal data (i.e. to the general public on the Internet, to a controlled number of service providers, etc.).

Materialised risks and use of sanctions (section 10 of the Guidelines)

3. In section 10 of the Guidelines, the EDPB states that "[*i*]*f a controller self-assesses the risk to be unlikely, but it turns out that the risk materializes, the relevant SA can use its corrective powers and may resolve to sanctions.*" This wording implies a strict liability for data controllers contrary to the obligations laid down in the General Data Protection Legislation ("GDPR"). According to the GDPR, data controllers do not have an obligation to notify the competent supervisory authority if it is unlikely that the data breach results in a risk for data subjects' rights and freedoms.

4. EuroCommerce asks the EDPB to acknowledge the fact that data controllers take the decision to notify based on information available to them at the time. If the suggestion is that these risk assessments will be reviewed with the benefit of hindsight, there is a great risk that this will create legal uncertainty causing data controllers to either notify all security breaches as personal data breaches or to not notify at all due to the fear or administrative fines.

5. EuroCommerce is of the opinion that neither of the above-mentioned scenarios are to the benefit of the level of data protection offered in the EU. We thus propose to clarify that data controllers that (i) have used all *proportionate* means which are available to the data controller at the time of the security breach and (ii) *reasonably* have concluded that it is unlikely that the security breach will result in a risk to the rights and freedoms of the data subjects have satisfied their obligations under the GDPR, regardless of whether the risk later materialises or not. It would also be helpful if the EDPB includes a list of examples of security breaches where there is no risk for the data subjects' rights and freedoms, e.g., an e-mail sent to the wrong recipient and where the e-mail does not contain any personal data other than the name and e-mail address of the sender.

6. However, if the EDPB suggests that the supervisory authorities should have the possibility to resolve to sanctions with the benefit of hindsight, EuroCommerce would like to stress the importance for supervisory authorities to be able to provide data controllers with real-time guidance in connection with the risk assessment conducted by a data controller. Such guidance would also need to be appropriately co-ordinated between the EU supervisory authorities to ensure harmonisation in the interpretation of the requirements.

7. Lastly, the key regulatory policy objective should remain to encourage timely notifications, instead of having those delayed by the need to complete every possible investigation. Emphasis should not be placed on punitive measures, but on how data controllers and supervisory authorities can collaborate to better protect data subjects. Sanctions should follow reckless and non-compliant behaviour; however, security breaches are an unfortunate fact-of-life and data controllers cannot be held directly and absolutely responsible for incidents that do not expose data subjects to a risk or when risks later materialise.

EuroCommerce proposals

Amend paragraph 10 of the Guidelines and clarify that data controllers' obligations are limited to proportionate measures regardless of whether a risk later materialises. More specifically, it should be clarified that data controllers that (i) have used all *proportionate* means which are available to the

data controller at the time of the security breach and (ii) *reasonably* have concluded that it is unlikely that the security breach will result in a risk to the rights and freedoms of the data subjects have satisfied their obligations under the GDPR, regardless of whether the risk later materialises or not.

Include a list of examples of security breaches that, in the EDPB's opinion, do not result in a risk for data subjects' rights and freedoms. Please note that EuroCommerce only asks that the EDPB includes examples where it is obvious that there is no risk for data subjects' rights and freedoms, e.g., an e-mail sent to the wrong recipient and where the e-mail does not contain any personal data other than the name and e-mail address of the sender.

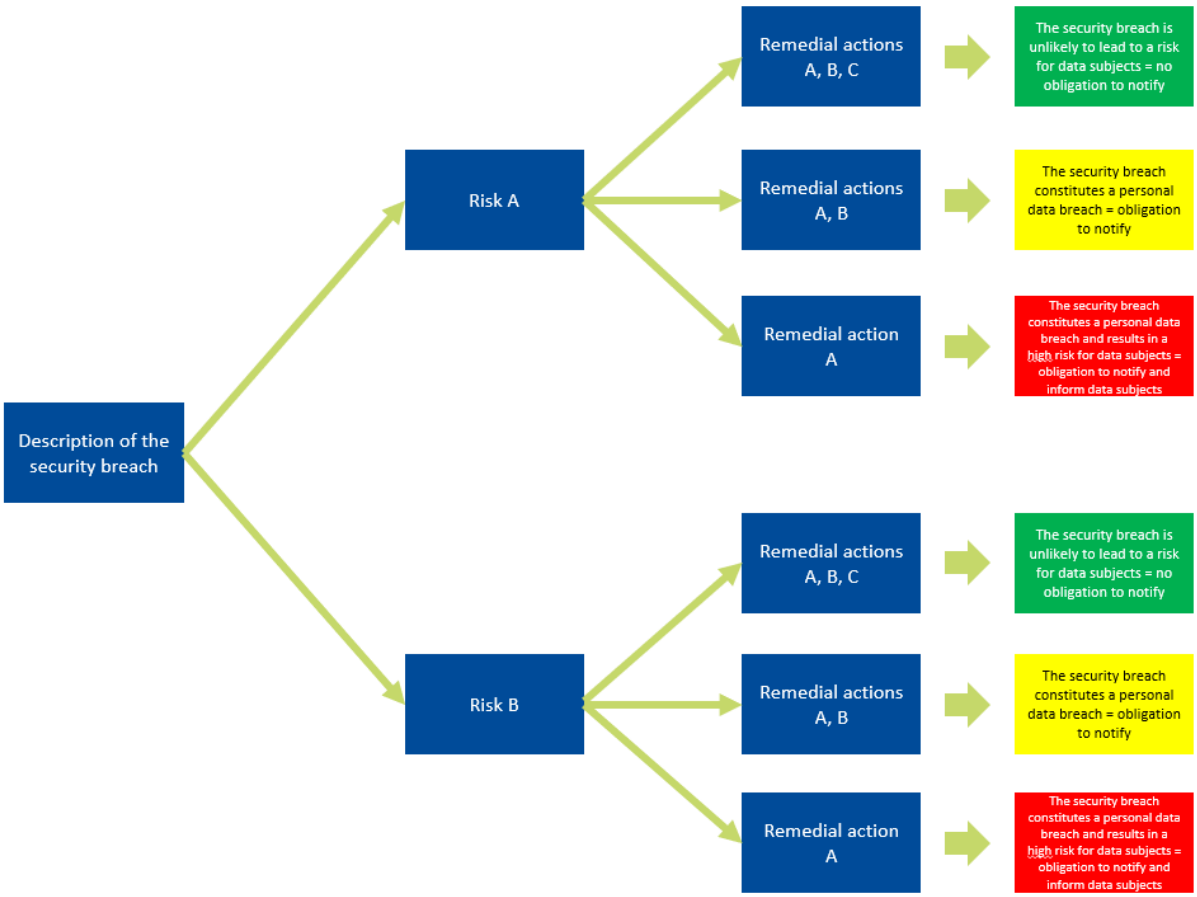
Further guidance on the notification obligation

8. The Guidelines helpfully provides a series of case studies which focus attention on the differing approaches data controllers may take to address a data breach, based on the sensitivity and volume of data compromised. However, further practical guidance would be welcomed in particular with regards to when the timeline for the notification obligation starts and the requirement to do a preliminary notification.

Clarification on when the timeline for the notification obligation starts

9. In connection with a security breach, data controllers must investigate the breach and assess whether the security breach constitutes a personal data breach which is notifiable to the competent supervisory authority. Based on the information, data controllers shall, in accordance with previous WP 250 guidance, notify the supervisory authority when they *with a reasonable degree of certainty* deem that the security breach constitutes a personal data breach. To satisfy this threshold, data controllers must conduct investigations to gather the information required to be able to make the assessment at all. It would be helpful for data controllers if the EDPB could draw conclusions from the examples presented in the Guidelines and identify certain notification thresholds for personal data breaches. A similar structure as presented below, would also help data controllers, and especially SMEs, to better understand what the key actions may be in a certain situation.

Example



10. Paragraph 9 of the Guidelines explores the complexities related to an investigation of a security breach but does not properly acknowledge the detailed forensic analysis that is often required before a data controller can make risk assessments in practice. The statement in paragraph 9 that *"controllers should make this assessment at the time they become aware of the breach … [and] not wait for a detailed forensic examination"* should thus be revised. Because not all security breaches *per se* are personal data breaches, the emphasis should instead be on prompt action to investigate a security breach and to take remedial action and notify, within 72 hours, when it can be established with a reasonable degree of certainty that it is a notifiable personal data breach.

11. Considering the above, EuroCommerce asks the EDPB to clarify that the obligation to notify arises, i.e., the data controller becomes aware of a data breach, when (i) the competent person(s) with the data controller receives information about the occurrence of a security breach, *and* (ii) has a reasonable degree of certainty that a data breach *has* led to a risk of compromising the rights and freedoms of data subjects. In relation to the circumstance presented in paragraph (i), the EDPB should especially acknowledge that there may be a practical delay between the first time an employee with the data controller becomes aware and a "person in charge" of data protection with the power to start an investigation and that delay in information from a data processor does not affect the data controllers' compliance with the notification obligation.

12. Lastly, paragraph 8 states that *"data breaches are problems in and of themselves, but they are also symptoms of a vulnerable, possibly outdated data security regime, [and] thus indicate system weaknesses to be addressed".* This is at odds with the GDPR, which requires data controllers to implement "appropriate" technical and organisational security measures, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing. Thus, under the GDPR, appropriate technical and organisational security will not completely extinguish all vulnerabilities in a system – and breaches will not *always* be indicative of a system weakness nor should lead to systematic enforcement. We ask the EDPB to revise the wording of the paragraph to instead clarify that data breaches *may* be symptoms of a vulnerable, possibly outdated data security regime.

EuroCommerce proposals

Identify and include notification thresholds based on the experiences of the supervisory authorities. It would be helpful for data controllers if the EDPB could draw conclusions from the examples presented in the Guidelines and identify certain notification thresholds for personal data breaches. See example in paragraph 9.

Revise paragraph 9 of the Guidelines and clarify the data controllers' obligations. Not all security breaches are *per se* personal data breaches and the emphasis should instead be on prompt action to investigate a security breach and to take remedial action and notify, within 72 hours, when it can be established with a reasonable degree of certainty that it is a notifiable personal data breach.

Revise paragraph 8 of the Guidelines to better align with the requirements set out in the GDPR. We ask the EDPB to revise the wording of the paragraph to instead clarify that data breaches *may* be symptoms of a vulnerable, possibly outdated data security regime.

Preliminary notifications

13. As stated in paragraphs 9-11 above, data controllers must be able to conduct proper investigations of a security breach before the timeline for data controllers' notification obligation is triggered. If, however, the EDPB is of the opinion that data controllers should not wait for a detailed forensic investigation and provide a preliminary notification even though the conclusion is yet to be made, further guidance is needed. Notably, the EDPB must clarify:

    a. what criteria need to be satisfied to trigger the obligation for a preliminary notification;

this is essential to ensure a harmonised application of the GDPR;
b. what information such preliminary notification should contain;
c. at what time does the additional information need to be provided, e.g. if it still needs to be provided within the 72 hours; and
d. what happens if the data controller deems that the preliminary notification was incorrectly submitted? Will it be possible to withdraw the preliminary notification?

14. The aim is to ensure that the process for preliminary notifications is harmonised and that data controllers, especially international data controllers, can take actions under a regime that provides legal certainty.

EuroCommerce proposal

If preliminary notifications are required, the EDPB must clarify the process and consequences relating to such notifications. Notably, the EDPB must clarify:

a. what criteria need to be satisfied to trigger the obligation for a preliminary notification; this is essential to ensure a harmonised application of the GDPR;
b. what information such preliminary notification should contain;
c. at what time does the additional information need to be provided, e.g., if it still needs to be provided within the 72 hours; and
d. what happens if the data controller deems that the preliminary notification was incorrectly submitted? Will it be possible to withdraw the preliminary notification?

Input to additional examples

15. It would be helpful if the Guidelines could provide further insight into complex supply chains and operating models that comprise of multiple data controllers (and even joint controllership). Additional case studies should explore the responsibilities and risk allocation in scenarios where multiple stakeholders (including separate data controllers, joint data controllers, and data processors) are involved.

16. The Guidelines should also provide additional case study context on the point at which data controllers can – reasonably – both end security breach investigations and begin to draw conclusions (particularly given the strain these investigations place on resources). For example, Case study 2 states that *"even after a thorough investigation that determined that the personal data was not exfiltrated by the attacker… the likelihood of a confidentiality breach cannot be entirely dismissed"*[2]. However, the requirement under the GDPR is not to fully mitigate every potential and theoretical risk. Investigations cannot practically continue forever, and we thus ask the EDPB to acknowledge that it would be sufficient if data controllers draw conclusions and make decisions with a *"reasonable degree of certainty"*.

On behalf of our collective members, we appreciate your consideration of these comments, and respectfully request that the EDPB address these concerns before adopting its final recommendations. We stand ready to assist the EDPB in its efforts to provide clarity on the obligations related to data breach notifications. We would be happy to provide additional constructive feedback or practical examples with respect to any of the issues above on which you would like further input. Please do not hesitate to contact Linda Leffler-Olsson (linda.leffler-olsson@shjuridik.se) or Savvina Papadaki (papadaki@eurocommerce.eu).

EU Transparency Register ID: 84973761187-60

[2] Case study 1, meanwhile, states that *an internal investigation…determined with certainty that the perpetrator only encrypted data, without exfiltrating it*, but goes on to say that the data controller should evaluate the potential risk of *exfiltration without leaving a trace in the logs of the systems*.