EADPP european association of data protection professionals

02 March 2021

To the European Data Protection Board
Brussels

Feedback of the European Association of Data Protection Professionals (EADPP) on the Guidelines 01/2021 on Examples regarding Data Breach Notification

Dear Sirs,

The European Association of Data Protection Professionals (EADPP) hereby provides its feedback pursuant to the above published initiative.

The EADPP was founded in November 2018 and is a not-for-profit association for and by data protection professionals.

The primary aim of the EADPP is to facilitate, organise, structure, and represent all data protection professionals applying the European privacy law in the context of their professional activities.

For any information or clarification in relation to our feedback, please contact Ms. Maria Raphael, Chair of EADPP, at the email address chair@eadpp.eu.

Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021, Version 1.0		
Section: Introduction		
1	Par 4	As both Controller and Processor must be able to recognize a data breach, we propose to amend the text as follows: *"As part of any attempt to address a breach the controller **and processor** should first be able to recognize one. The GDPR defines a "personal data breach" in Article 4(12) as "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".*
2	Par 5	As the data breach could fall under all three mentioned categories of data breaches or be a combination of some categories of data breaches, we propose to have the following sentence added:

Address: Robert Schumandomein 2
6229 ES Maastricht, The Netherlands
email: info@eadpp.eu
website: eadpp.eu

		It must be taken into consideration that a data breach can concern either one category or more categories simultaneously or combined.
3	Par 7	As the data breach could occur on the processor side and the GDPR requires the processor to notify the controller, we propose for the following text to be added: *"**Also, the GDPR requires the processor to notify the controller without undue delay after becoming aware of a personal data breach.**"*
4	Par 10	Par. 10 reads as follows: *"If 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".* In some cases, the materialization of the risk is highly dependent on the vulnerabilities existing in the systems of other controllers, while the controller making the assessment has no visibility relating to these vulnerabilities. Therefore, we recommend the EDPB to include the following text: *"**Any sanction resolved upon by SA should also take into consideration the overall response of the controller, the information available to the controller when the assessment is made, as well as the external factors unforseen at the time of the assessment (e.g. vulnerabilities in the systems of other controllers which made possible the materialization of the consequences)**".*
5	Par 11	As the data breach could occur on the processor side, we propose to amend the text as follows (please refer to bold words): *'Every controller **and processor** should have plans, procedures in place for handling eventual data breaches. Organisations should have clear reporting lines and persons responsible for certain aspects of the recovery process."*
6	Par 12	As the data breach could occur on the processor side, we propose to amend the text as follows (please refer to the bold words): *"Training and awareness on data protection issues **for** the staff of the controller **and processor** focusing on personal data breach management (identification of a personal data breach incident and further actions to be taken, etc.) is also essential for the controllers **and the processors**. This training should be regularly repeated, depending on the type of the processing activity and size of the controller **and the processor**, addressing latest trends and alerts coming from cyberattacks or other security incidents."*
7	Par 13	-As the data breach could occur on the processor side, we propose to amend the text as follows (please refer to the bold words): *"The principle of accountability and the concept of data protection by design could incorporate analysis that feeds into a data controller's **and data processor's** own "Handbook on Handling Personal Data Breach" that aims to establish facts for*

		each facet of the processing at each major stage of the operation. Such a handbook prepared in advance would provide a much quicker source of information to allow data controllers ***and data processors*** *to mitigate the risks and meet the obligations without undue delay. This would ensure that if a data breach was to occur, people in the organisation would know what to do, and the incident would more than likely be handled quicker than if there were no mitigations or plan in place".* -We would also like to invite EDPB to propose and address the minimum content of the "Handbook on Handling Personal Data Breach".

Section: RANSOMWARE		
8	Art 2.1.1. Par 18	Having a separate backup will of course help mitigate the consequences of a ransomware event as the controller will not need to collect again the data. Nevertheless, to be helpful, the backup should be physically separated and dislocated from the main one, in line with the international security standards (e.g., cloud services information security and business continuity rules).
9	Art 2.1.2. Par 25	As it is of the utmost importance to prevent future ransomware events, it is necessary to investigate/identify the breach causes and methods used by the perperators. We propose to amend the text as follows: *"In this case, following a detailed impact assessment and incident response process, the controller determined that the breach was unlikely to result in a risk to the rights and freedoms of natural persons, hence no communication to the data subjects is necessary, nor does the breach require a notification to the SA. However, as with all data breaches, it should be documented in accordance with Article 33 (5). The organisation may also need (or later be required by the SA) to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.* ***Within the frame of this update and remediation, the organisation should thoroughly investigate the breach and identify the causes and the methods used by the perpetrator to prevent any similar events in the future****."*
10	Art 2.2.2. Par 33	We consider that the the mere possibility of delays in the orders' delivery to customers and non retrievability of a considerable amount of meta-data is not itself a reason to require a notification to the SA.
11	Art 2.2.2. Par 35	As it is of the utmost importance to prevent future ransomware events, it is necessary to investigate/identify the cause of the breach and the methods used by the perpetators. We propose to amend the text to the following: *"This case serves as an example for a ransomware attack with risk to the rights and freedoms of the data subjects, but not reaching high risk. It should be documented in accordance with Article 33 (5) and notified to the SA in accordance with Article 33 (1). The organisation may also need (or be required by the SA) to update and remediate its organizational and technical personal data security handling and risk*

		mitigation measures and procedures. ***Within the frame of this update and remediation, the organisation should thoroughly investigate the breach and identify the causes and the methods used by the perpetrator to prevent any similar events in the future.*** *"*
12	Art 2.3.2. Par 40	As it is of the utmost importance to prevent future ransomware events, it is necessary to investigate/identify the cause of the breach and the methods used by the perpetrators. We propose to amend the text to the following: *"This case serves as an example for a ransomware attack with high risk to the rights and freedoms of the data subjects. It should be documented in accordance with Article 33 (5), notified to the SA in accordance with Article 33 (1) and communicated to the data subjects in accordance with Article 34 (1). The organisation also needs to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.* ***Within the frame of this update and remediation, the organisation should thoroughly investigate the breach and identify the causes and the methods used by the perpetrator to prevent any similar events in the future****."*
13	Art 2.4.1. Par 41	Due to the need to promote the most effective backup solution, we propose to amend the text as follows (please refer to the bold passage): *"The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.5. Though a backup was in place, it was also affected by the attack. This arrangement alone raises questions about the quality of the controller's prior IT security measures and should be further scrutinised during the investigation, since in a* ***well-designed backup regime, multiple backups must be securely stored without access from the main system, otherwise they could be compromised in the same attack. Furthermore, ransomware attacks may lie undiscovered for days slowly encrypting rarely used data. This can render multiple backups useless, so backups should also be taken periodically and isolated increasing the likelihood of recovery albeit with increased loss of data".***
14	Art 2.4.2. Par 47	As it is of the utmost importance to prevent future ransomware events, it is necessary to investigate/identify the cause of breach and the methods used by the perpetrators. Also, in practice, there are cases when a public communication would create confusion among the data subjects or even prompt them to perform certain changes not effectivelly needed and, therefore, trigger additional unwanted consequences on such data subjects. We propose to amend the text to the following (please refer to bold passages): *"Aside from documenting the breach in accordance with Article 33 (5), a notification to the SA is also mandatory in this case (Article 33 (1)) and the controller is also obliged to communicate the breach to the data subjects (Article 34 (1)). The latter could be undertaken on a person-by-person basis, but for individuals where contact data is not available, the controller should do so publicly* ***provided that such communication would not be susceptible to trigger additional negative consequences on the data subjects****, e.g. by way of a notification on its*

		website. In the latter case a precise and clear communication is required, in plain sight on the homepage of the controller, with exact references of the relevant GDPR provisions, ***or, depending on the situation, a precise short communication on the homepage of the controller including a link to a dedicated page/website where all relevant information is added****. The organisation may also need to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.* ***Within the frame of this update and remediation, the organisation should thoroughly investigate the breach and identify the causes and the methods used by the perpetrator to prevent any similar events in the future****."*

Section: INTERNAL HUMAN RISK SOURCE		
15	Proposal for an additional case	**Addional Case No. 13.a** The employees are accessing for personal purposes or gain the personal data of the clients to whom they had access to in order to perform their daily tasks. Two examples of this type of breach are: • An employee accessed the account of a client, making some pictures with his phone and providing the financial information to the client's former partner enabling the latter to obtain certain benefits from the dispute. The controller identified the breach following the complaint received from the former partner. • An employee accessed repeatedly the account of his partner, client of the controller, verifying the traffic data from a certain period in order to confirm some personal suspicions. As he did not find the information he was looking for, no further actions were taken by the employee in this respect, while the data was not disclosed or downloaded in any way. The controller identified the breach following warnings raised by the IT system used and an internal investigation was performed. These types of cases are very relevant for controllers acting in areas such as banking, financial institutions, telecom, vouchers issuance, etc. While in the first example the controller needs to inform both the SA and the data subject, in the second ones, only the documentation of the breach should be needed. In such cases, usually the controller is able to identify the unauthorized access but not able to fully prevent it as the employee has in his job description the usage of the personal data of the clients and of the related systems for legitimate business purposes. Among the controls implemented to discourage such behaviour and to protect the personal data: (i) the employee is bound by confidentiality obligation; (ii) proper access rights are in place, (iii) mandatory data protection training;

		(iv) alerts in the systems trigger an internal investigation are started; (v) the printing and print screen functions are disabled; (vi) disciplinary actions against the employees breaching confidentiality etc. From our perspective, any employee acting intentionally beyond the obligations imposed by his employment agreement, using data for personal gain/purpose (not for legitimate business purpose) becomes a controller in his own name. In this context, the employee is the one deciding on the purpose and means of processing the personal data far beyond any purpose established by the controller.
16	Art 4.2.1. Par 75	Our comment is related to the sentence "*It might need to involve immediate legal action to prevent the former employee from abusing and disseminating the data any further.*" We propose to invite controllers and processors to include in the employment agreement clauses that impose on the employee confidentiality obligations during and after the termination of the employment and prohibit the employees during and after the employment to collect, process, abuse and disseminate the personal data as well as provide for remedies that are avaialble to the employers if and when the employee breaches his/her obligations.
17	Art 4.2.1. Par 78	Unfortunately, breaches of this kind, cannot be completely avoided regardless of the safeguards implemented by the controller and, therefore, we propose the following amendment (bold words): *"Unlike the previous case, here the breach does not derive from* ***an intentional*** *action of an employee, but from an unintentional human error caused by inattentiveness. These kinds of breaches may be avoided* ***or decrease in frequency*** *by a) enforcing training, education and awareness programs where employees gain a better understanding of the importance of personal data protection, b) reducing file exchange through e-mail, instead using dedicated systems for processing customer data for example, c) double checking files before sending, d) separating the creation and sending of files".*

Section: MISPOSTAL		
18	Par 106	Such types of human errors are possible through various means and not only by email communication. There are cases where these errors are the result of physical delivery, for example during the pandemic, there was a significant increase in online purchases followed by a high rate of erroneous invoices which were not related to the purchased items.

Section: OTHER CASES – SOCIAL ENGINEERING		
19	Par 124 - 128	In practice, these types of social engineering cases are successful after sufficient information is gathered by the attacker in the online environment, usually via

		social media, and many recurrent calls are made by the attacker to the call center of the controller. One way to avoid such social engineering cases is to have in place more accurate identification methods, including particular biometric identification (such as via client voice) or video identification of the client, if proven as strictly necessary and unavoidable.

Your sincerely,

Maria Raphael
Chair of the EADPP
On behalf of the EADPP Board

Contributors/EADPP members:

1. Maria Raphael, Chair of EADPP and Chair of Cyprus Branch, Cyprus
2. Igor Barlek, EADPP Board Member and the Chair of EADPP Strategy & Policy Committee, Croatia
3. Rob Jones, EADPP member, UK
4. Adriana Neagu, EADPP member, Romania
5. Kristian Kise Haugland, EADPP member, Norway
6. Olga Tsiptse, Chair of Greece Branch, Secretary of EADPP Academic Board and Certification Committee, Greece
7. Patricia del Carmen, EADPP member, France