EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

Comments on the

European data Protection Board's Guidelines 01/2021

on Examples regarding Data Breach Notification

European Federation of Data Protection Officers

March 2021

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

EFDPOs Position

Following the European Data Protection Board's (EDPB) request for public consultation on Guidelines 01/2021 on Examples regarding Data Breach Notification ("Guidelines"), the European Federation of Data Protection Officers (EFDPO) takes this opportunity to contribute to the ongoing discussion with the following comments.

Our approach to the issues raised by this public consultation is that of a European umbrella association of data protection and privacy officers. The objectives are to create a European network of national associations where information, experience and methods can be exchanged. We will establish a continuous dialogue with the political sphere, business representatives and civil society, to facilitate a flow of information from the European to the national level and to proactively monitor, evaluate and shape the implementation of the GDPR and other European legal acts and texts regarding privacy.

The EFDPO welcomes the EDPB's initiative on this complex and important matter. The WP250 has already provided very useful guidance for Data Protection Officers (DPOs) and the recently adopted recommendations issued by the EDPB provide even better orientation. Regarding the current practice on the data breach notification the EFDPO would like to stress the importance of the following topics that have not been mentioned in either the WP250 or the Guidelines:

One Stop Shop on Breach Notification: In a world of global threats, it should be provided for controllers and processors to be able to perform their legal duty by notifying their supervisory authority centrally; Supervisory authorities in the EU could strengthen the collaboration between the member states by establishing a central repository of breaches. The application of an appropriate one-stop-shop mechanism should drive efficacy and improve protection for data subject rights and freedoms across the EU Member States.

Harmonized Data Breach Notification Online Template: Templates provided by the DPAs are differing from authority to authority. Reasons are unclear. In many countries the templates are available in just one language. It would be of great help if they were offered in more than one language, since translations of (mostly) legal statements cause unnecessary and avoidable delay, because of the involvement of legal counsels from various EU Member States for providing and translating breach notifications. It would be preferable if the right to make the notification in English were provided, so that it would be prepared only once, which would lead to more punctual notifications.

General Comments on the Guidelines

Statutory Time: Besides the mere decision whether it is obligatory to notify or not, in practice we believe that the time limitations raise concerns as well. Especially the more complex scenarios have to be seen as a process instead of a simple collection of already existing information, since a detailed time-consuming investigation is required. When such a process of analysis arises, it is rather unclear, when the statutory period

of 72 hours begins. Although the WP250 discusses this question, it still remains quite unclear in practice, whether it is considered proper to notify with incomplete information about the case. Especially in the ransomware (case 2) and data exfiltration (case 3) cases it would be a good idea to give hints at which stage of the process the decision about the notification should be made. A different kind of case can be found in Case 4.1. The company may first become aware of a data breach with a considerable delay, e.g. after a complaint of the customers. It would be of practical help for many incidents to know, when it is clear that the period is running, after the company got aware of the mere technical data breach. To our experience the turning point between having a data security problem that potentially involves personal data, and a data security problem that definitely involves personal data is extremely important and any suggestion on how the exact moment in time when the countdown starts is determined and concretized would be more than appreciated.

Promoting the importance of information security for data protection: In the Guidelines the term “up-to-date" is used quite often, especially when it comes to technical measures. There is a broad discussion on how this term should be interpreted. The statements regarding prevention in the guidelines are relevant here.

We would welcome better references to any trusted and reliable policy maker baseline standards and resources to “state of the art” technical and organizational measures as provided for example by Teletrust, a German IT Security Association in cooperation with ENISA[1].

We are convinced breaches can be prevented by ensuring that appropriate organizational, physical and technological security measures have been taken. A proper patch management and the use of appropriate anti-malware detection system is not sufficient to this end. For this reason, we would appreciate further clarity on this statement made in the Guidelines. It should be clear that cybersecurity threats are exponentially broad. The full scope of a problem will not be resolved by a box on a network or a single-purpose software agent. Any resolution requires contextual awareness and visibility across environments, including within cloud and ephemeral environments.

To reduce organizations privacy concerns regarding the processing of personal data for IT and network security purposes, we would welcome support from the EU Member States supervisory authorities for a legitimate interest and riskless data processing for data protection and cybersecurity purposes, as outlined in Recital 49 of the GDPR. There should not be any conflict between IT-Security and Data Protection/Privacy.

[1] https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Guideline_State_of_the_art_in_IT_security_EN.pdf

Additional Scenarios

Losing Postal consignments: Another open and unclear scenario we have identified from practice is related to postal services, so an addition to section 6 of the Guidelines would be more than welcome. Our members have experienced scenarios where the incident took place within the sphere of a postal service provider: an item gets lost or is delivered to a false recipient. The sender gets notified about the incident from a report of the correct addressee or from the false recipient. The correct delivery is proved by the relevant receipt of the postal commission. Yet, in case of loss of a postal object or a false delivery of a postal object, it is unclear who the addressee of the obligations under Art. 33, 34 GDPR is. The postal service providers claim that a notification cannot be made, since the identity of the data subjects involved and the risks of these is not known with certainty. On the other hand, if the senders are the controllers a notification has to be made without any direct influence on the causes of the incident. There were rumours that some DPAs even waive the requirement of this notification obligation.

Mistakes in Access Rights: In internal processes of larger organisations, DPOs are regularly confronted with non-compliant access rights which do not conform with the “need-to-know” principle. Even by mistake, there might be a big number of the personnel that acquire access to a document. When dealing with a small number of people involved, low risk is presumed, especially as far as known and trusted colleagues are concerned. When the number of the authorized personnel is getting bigger, this argumentation becomes more and more problematic in practice, therefore any suggestions on this situation in the Guidelines would be appreciated.

Infiltrated Networks: Our members would appreciate further clarity to the handling of breaches dealing with infiltrated networks where adversaries have been in a network but where it is not totally clear whether they have stolen any protected data incl. personal data.

That said, overbroad guidance could have adverse implications by exposing individuals or entities to a high volume of extraneous notifications and thereby desensitizing the importance and purpose of such notifications. In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and standards. Data about computer processes, which may include identifiable information, is integral to distinguishing alerts from incidents.

Minor Comments

Paragraph 8 - "Data breaches are problems in and of themselves, but they are also symptoms of a vulnerable, possibly outdated data security regime..."

> The statement seems to be too far reaching. We suggest to rephrase the wording in a less definite way (keeping room for considering the nature of the breach): "may be also possible symptoms" or "they may also indicate a vulnerability...". Cases of breaches typically caused by individuals´ misconduct

or inattentiveness, would not necessarily indicate a vulnerable or outdated system.

Paragraph 10

The remark expresses a threat for penalties in a case where controllers might have made a mistaken decision about the risk. We agree that this can be easily used as an inappropriate excuse. On the other hand, it can lead to a method where controllers and processors perform the notification in cases even with incomplete information when it is not yet clear if it is actually a case that requires notification - just for the purpose of reducing the risk of penalties. A more thorough discussion on the conditions for penalties in this sentence would lead to a more confident decision for the notification.

Paragraph 49 Bulletpoint 8

“All Logs” it is not clear which logs are meant here, maybe an “including access, security, …logs” addition would help. A different approach for the clause could be: “Operating central log server to collect and securely store all relevant log files.”

Paragraph 84 - “forcing users to follow the rules”

A hint on possible “forces” might be helpful. Is the EDPB suggesting to expressly penalise employees?

Description of case 5.2 (before Paragraph 93, top of page 24).

The question arises if it was not possible to evaluate whether other categories of personal data were affected, when a full daily backup was performed. Access to the backup would lead to the stored data. Either the type of the backup should be clarified or the consequence of necessary notifications should become even more apparent in this case.

Section 5.4 (page 25), paragraph 105

The available measures suggested seem to have been inserted by mistake. They should be related to case No. 12 Stolen paper files with sensitive data, which they do not (they relate to "loss or theft of device").

Paragraph 110 and 114

Both paragraphs suggest without further specification that in case of personal data sent by email by mistake, "the introduction of additional control mechanisms need to be considered". In both scenarios the incident was caused by a human error. We expect employees should be regularly trained on how to handle personal data, and among other topics, on how to avoid causing typical types of breaches like sending an email by mistake to a wrong email address. We consider this to be the main mitigating measure. However, introducing "stricter rules for sending such messages" - is not sufficiently clear. What are

possible examples of such rules and what qualifies as "such message" is not quite clear. In case No. 14, the email that was not correctly sent, affected a large number of data subjects - is that the criteria, or is it the type of data, or both?

Moreover, the case is called "sensitive personal data sent by email by mistake", however, the list of data affected does contain data, the sensitivity of which needs an explanation (Only the SSN of an applicant might be considered sensitive depending on the countries).

Section 6.3. Case 15 before paragraph 114 on Page 27:

This case does not seem to be in any way "clear". Again, it is not clear how the term "such message" should be interpreted in the meaning of paragraph 115 of the draft Guidance.

We believe the Guideline should be clearer about how the term "such message" should be interpreted under paragraphs 110 and 114 of the draft Guidance.

Also, there are no recommendations for "stricter rules" on the sending of "such" messages.

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

EFDPO contacts:

EFDPO Press Office, phone +49 30 20 62 14 41, email: office@efdpo.eu,

President: Thomas Spaeing (Germany)

Vice Presidents: Xavier Leclerc (France), Judith Leschanz (Austria), Inês Oliveira (Portugal), Vladan Rámiš (Czech Republic)

About EFDPO

The European Federation of Data Protection Officers (EFDPO) is the European umbrella association of data protection and privacy officers. Its objectives are to create a European network of national associations to exchange information, experience and methods, to establish a continuous dialogue with the political sphere, business representatives and civil society to ensure a flow of information from the European to the national level and to proactively monitor, evaluate and shape the implementation of the GDPR and other European privacy legal acts. In doing so, the EFDPO aims to strengthen data protection as a competitive and locational advantage for Europe. The new association is based in Brussels.

Founding members:

- Austria: Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter privacyofficers.at
- Czech Republic: Spolek pro ochranu osobních údajů
- France: UDPO, Union des Data Protection Officer - DPO
- Germany: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
- Greece: Hellenic Association for Data Protection and Privacy (HADPP)
- Liechtenstein: dsv.li-Datenschutzverein in Liechtenstein
- Portugal: APDPO PORTUGAL Associação dos Profissionais de Proteção e de Segurança de Dados
- Slovakia: Spolok na ochranu osobných údajov