Comment

of the German Insurance Association (GDV)
ID-number 6437280268-55

on the
EDPB draft Guidelines 01/2021
On Examples regarding Data Breach Notification

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Phone: +49 30 2020-5000
Fax: +49 30 2020-6000

Rue du Champs de Mars 23
B - 1050 Brussels
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Contact:
Datenschutz/Grundsatzfragen

E-Mail: **data-protection@gdv.de**

www.gdv.de

Executive summary

The German Insurance Association welcomes the draft guidelines 01/2021 and their focus on more practical guidance for controllers. The guidelines will be crucial to reduce the persisting legal uncertainty regarding data breach notices.

We believe that additional clarifications would further improve their usefulness. These concern

- a list of relevant factors and their impact on the risk assessment,
- inferences from data breaches,
- the time of notification,
- the term “relevant supervisory authority” and sanctions for risks that materialize at a later time,
- speculations on the consequences of a data breach for data subjects and
- the risk assessment in case no. 16: snail mail mistake.

1. Introduction

The German Insurance Association (GDV) welcomes the EDPB's intention to provide controllers with additional guidance on the obligation for data breach notifications. Experience has shown that the general guidance in Working Paper 250 did not resolve the persisting legal uncertainty sufficiently. More practice-oriented guidance is necessary. Against this background, we would like to provide additional input.

2. List of relevant factors and their impact on the risk assessment

As the EDPB rightfully explains, the risk assessment for data breaches has to be performed on a case to case basis. Modifications in the circumstances may or may not lead to different levels of risk. In order to further increase the usefulness of the guidelines we suggest reinforcing them with a more comprehensive section on relevant factors and their general impact within the risk assessment. WP 250 already provides some guidance on factors to consider, but does not go into detail on how to balance the criteria against each other when assessing the risks of a particular case. Meanwhile, the use cases in the guidelines 01/2021 are very specific and can only be used to extrapolate the significance of certain factors in the assessment for other cases.

3. Inferences from data breaches

According to the guidelines, "data breaches are problems in and of themselves, but they are also symptoms of a vulnerable, possibly outdated data security regime, thus indicate system weaknesses to be addressed" (page 6 para. 8).

We believe that this statement requires more differentiation. Not every data breach is indicative of a vulnerable or outdated security regime. As the EDPB mentions on several occasions, certain types of data breaches cannot be fully prevented. Even state of the art security measures will never be able to prevent every data breach.

4. Time of notification

The guidelines further state that "controllers should make the risk assessment at the time they become aware of the breach. They should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified" (page 6 para. 9).

This section should be rephrased as it is potentially misleading. While a risk assessment should be made at the time of becoming aware of a possible data breach, it should be possible for the controller to wait for the results of additional investigations and examinations if a proper risk assessment cannot be performed with the available information. Otherwise, in many situations the notification will be given prematurely as the investigations reveal that there was no data breach.

5. "Relevant supervisory authority" and sanctions for risks that materialize at a later time

The EDPB remarks that *"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"* (page 6 para. 10).

This statement also requires more differentiation. If the result of the controller's self-assessment appears reasonable at the time it is made and the risk only materializes afterwards, sanctions by the data protection supervisory authority do not seem justified.

The EDPB also introduces new terminology. The term "relevant supervisory authorities (SA)" is not clearly defined. The GDPR itself only mentions "lead SA" and "other SA concerned" in order to determine the competences in cross-border cases. In past guidelines, the EDPB also used the terms "competent SA" and "concerned SA". If the EDPB means "concerned SA" when it speaks of "the relevant SA" in para. 10 of the guidelines, it would create additional competences in cross-border cases, as according to the GDPR only the lead SA may use corrective powers outside of the consistency mechanism. We, therefore, suggest bringing the terminology in line with the GDPR and previous publications.

6. Speculations on consequences of a data breach for data subjects

On several occasions the guidelines mention that the controller has to take into consideration the consequences and difficulties that may be caused to the data subject by the data breach (e. g. page 10 para. 34). While it cannot be argued that the impact of the data breach is not an important factor to consider, it should be specified to what extent the controller has to consider it when assessing the risks. If the controller does not have knowledge of any likely to occur negative ramifications for the data subject, he should not be required to take into account consequences for the data subject which may only be considered possible because they cannot be ruled out completely. Otherwise, the controller would have to enter the realm of speculations. This is the case when a data breach may cause delays for the data

subject which in turn may have additional effects the controller can only speculate on.

7. Risk assessment in case no. 16: Snail mail mistake

Case no. 16 (page 28 para. 118 – page 29 para. 121) concerns the accidental disclosure of certain insurance contract information to another policyholder (name, address, vehicle registration number, insurance rates of the current and next insurance year, approximate annual mileage and date of birth). According to the EDPB, the insurer must notify the SA because it considers the risks for the data subject to be medium. The reasons for that risk assessment are:

- The information concerned is not publicly available.
- If the insurance rate increases, a not insignificant claim, which could also have been an accident, was disclosed to the unauthorized recipient.
- In individual cases it cannot be completely ruled out that the letter will be posted in social networks or that the policyholder will be contacted.

For the risk assessment, the guidelines strongly focus on the disclosure of information on car accidents. We believe that further differentiation is necessary in this regard. If the incorrectly delivered letter does not state the reasons for the increase in the premium or if non-accident-related reasons are stated, no information about accidents is disclosed. Thus, no "sensitive" information is revealed to the recipient. The situation would be different if the letter obviously indicated that the policyholder was downgraded. If, however, other reasons for the increase in the premium can come into consideration, the mere fact that the premiums will be increased as such cannot have a risk-increasing effect for the assessment. In this respect, the misuse of the data no longer constitutes a medium risk.

We would further argue that even if the letter contained the information that the increase of the insurance rates resulted from a car accident, disclosure of that information would not lead to more than a low risk for the rights and freedoms of the data subject. The circumstance that a car accident occurred is as a matter of fact inevitably known to a greater and often indeterminable group of third parties, for example witnesses to the accident, other customers of the car workshop and else. Furthermore, the mere fact that a car accident happened does not reveal anything on who was involved, whether there were any injuries or how big the claims were.

Overall, the risk in case 16 should be considered low, since

- it concerns an individual case and is not indicative of systemic problems
- the premium increase cannot be attributed to a specific reason due to the lack of further information
- misuse of the information is extremely unlikely.

At most, if the behavior of the recipient gives cause for contrary assumptions, a risk could be assumed. It should not be insinuated that recipients of misdelivered letters may publish the information if there is no cause to believe that. In our experience, it is quite often the opposite. Accidental recipients often inform companies about instances of misdelivery on their own and may even make reference to data protection issues. In other cases, the recipients return or destroy the misdelivered letters and promise and assure that they did not take detailed notice of the contents. In these and similar cases of trustworthy recipients there is no reason to believe that the risks for the data subject are anything but low. It would be particularly helpful if the final guidelines properly reflected that.

Berlin, 2 March 2021