Insurance
& Pension
Denmark

The European Data Protection Board

02.03.2021

Insurance & Pension Denmark
Philip Heymans Allé 1
DK-2900 Hellerup
Phone: +45 41 91 91 91
fp@forsikringogpension.dk
www.forsikringogpension.dk

Karen Gjølbo
Senior Consultant. LL.M
Dir. +45 41 91 90 45
kgj@fogp.dk

Case No. GES-2017-00303
DocID 420132

Insurance and Pension Denmark's response to the draft guidelines on data-breaches

Insurance and Pension Denmark would like to thank the European Data Protection Board for the initiative of a more practical guidance in handling data-breaches and for giving this opportunity to provide comments.

We are very positive of this quite comprehensive and practical approach towards a rather complex part of data protection. The insurance companies are of course very focused on security of data and the confidence of their customers, who entrusts them with a significant amount of personal data. Still, they find it sometimes difficult to navigate as the obligations are not always clear and depends on further evaluations.

Regarding the rules on data breach notifications, we find it most important to ensure the clarity of the obligations, in order to keep the rules efficient. If not, an unwanted administrative burden for both controllers and SA's could be created and shift the focus of both parties from more severe breaches and other important matters that relate to data protection.

Please find below our specific comments for the draft guidelines. If there is a need for further elaboration, we will of course be available.

Yours Sincerely,

Karen Gjølbo

General comments

- *Clarification of the scope*

The draft guidelines are presented as guidelines on "examples regarding data breach notifications". We find the heading misleading since it only says, "data breaches", which indicates a broader scope of the guidelines and of the data controllers obligations than what is in the GDPR. Obviously, breaches of non-personal data (for example unauthorized disclosure of information covered by secrecy, but not encompassing information relating to identified or identifiable natural persons) could produce negative effects for individuals (for example financial loss) but these breaches are out of scope of the GDPR.

➢ ***Hence, the heading of the guidelines should be amended for clarification to ensure, that these guidelines are focused only on "personal data breaches".***

Further, for clarification, we find that paragraph 1 should be rewritten. Currently it states that all personal data breaches must be notified to the NSA's, which is misleading, as the GDPR does not ask for notification where the breach is unlikely to result in the a risk to the rights and freedoms of natural persons, ref. Article 33.

➢ ***Paragraph 1 should be rewritten according to the wording of Articles 33***

- *Streamlining of concepts/definitions*

In several cases there is a reference to national identification number, though different designations are used (Case 4 (identity card numbers), Case 17 (fiscal number) og Case 14 (social security number)).

➢ ***We suggest for the use of the designation of "national identifications numbers" as stated in article 87 of the GDPR.***

There is an inconsistency within the guidelines as to the tables on actions necessary based on the identified risks. The first tables (until paragraph 40) are divided into "No Risk, Risk and High Risk", whereas the following tables mentions "Internal documentation, Notification to SA and Communication to Data Subject".

➢ ***We find that the tables should be aligned within the document.***

Comments on the specific examples/cases

- *Need for more examples or elaboration of the examples already presented*

Insurance & Pension Denmark finds it challenging that the examples given comes with a lot of prerequisites, making it difficult to have a conclusion in situations, that varies just a little bit from what is described. We find that there is a need for more examples or elaborations of the examples already presented in order to make the guidelines less rigid and more useful. This is particularly relevant when it comes to the examples of human risk source and where the data breach does not occur due to malicious behavior.

➢ ***We suggest an elaboration of both the risk scenarios and the security measures taken, with alternative examples of both. (Suggestions are included in the following comments on cases no. 9 + no. 13).***

- *Need for clarification on the evaluation of the risk*

Several times (ie in case 9, 11 and 14) the EDPB highlights the number of data subjects impacted by the data breach, as an indicator of the severity of the breach. Insurance & Pensions Denmark finds this strange, as the focus should be on the risk of the individual data subjects rights, and specific conditions related to him or her, which could increase that risk. The fact that other data subjects are harmed should not affect the risk of the individual data subject. The amount of data could of course increase the risk for a breach, as it makes it more interesting for hackers to enter a data system, but this should then be clarified in the text.

➢ ***References to the number of datasubjects as an indicator of the severity of a databreach should be deleted in the guidelines.***

- *Comments for the specific cases/examples*

<u>Case no. 5</u> on exfiltration of job application data from a website – In this case, the EDPB concludes that there is a high risk, hence an obligation for both a notification for the NSA and communication to the subject. We find that there is a need for further elaboration of the specific factors to be taken into account here, since there is no indication of sensitive data or special conditions of the data subject.

<u>Case no. 8</u> on exfiltration of business data by a former employee – Insurance & Pension Denmark finds that this case should be reconsidered. At a minimum, EDPB should consider two questions that arise due to this case.

The first question would be if the company in this example rightfully should be seen as a controller for the activities carried out by the employee (and later the *former* employee). From a general point of view, it can be assumed that the employee in this case deliberately, and not just out of negligence or carelessness, violates the instructions and policies issued by the controller at the point of time where he copies the business data he is authorised to access during his period of notice and (presumably) stores this data on a "private" storage media. This would not be a processing activity covered by the purposes and means determined by the controller according to Article 4(7). Furthermore, the activity is not carried out under the authority of the controller. Put differently, it can be assumed that the employee has not processed the data on instructions from the controller according to Article 29. A person acting under the authority of the controller who has access to personal data should normally not be regarded as a controller, not even when he or she is making mistakes. But when a person deliberately and clearly violates instructions and policies issued by the employer in a manner that has no connection to the employment contract, and the employer meet the standards of appropriate level of protection according to Article 32, the GDPR suggests that the employee, rather than the employer, can be seen a controller with obligations under Article 33 and 34. This would also be true for a processor (and persons under the supervision of a processor) according to Article 28(10). Given the risks that can arise for affected data subjects as a result of events similar to that in case no. 8, this outcome would obviously not be satisfactory. Nevertheless, it would probably be the outcome given the systematics of the GDPR.

The second question would be for how long a former employer can be seen as datacontroller and held responsible for activities carried out on personal data by a former employee. Finally, the EDPB should keep in mind that controllers/employers are, and rightfully should be, limited by the GDPR when overseeing the processing activities carried out by their employees and must to some extent always rely on the element of trust.

Case no. 9 on accidental transmission of data to a trusted third party. A number of factors are listed in support of the conclusion that there is no obligation for notification to the NSA, nor for communication to the data subject. It would be useful to change the prerequisites and have an answer to the situation where:

- Special categories of data are submitted in the transmission?
- Data are sent to several trusted 3rd parties and/or if the confidentiality – by accident or by lack of control - are compromised?
- Significantly more data subjects are affected by the data breach in relation to mitigating measures?

Case no. 10 on stolen material storing encrypted personal data. For this case, we would like the EDPB to describe a scenario taking into account the use of VPN and two-factor approval as specific security measures.

Case no. 11 on stolen material storing non-encrypted personal data. It follows from paragraph 96 that in this case the risk is considered high, i.e due to the risk of identity fraud. There was a leak of name, address and birthday, but no further identity information. We find that the conclusion should be altered, as is it not possible to commit identity fraud with only access to the given information.

Case no. 12 on stolen paper files with sensitive data is based on the example where personal data is documented and saved in physical documents. Such a processing activity is not always covered by the material scope of the GDPR.

Simplified, if personal data is documented and saved solely on paper, without any automated means, the processing would be out of the scope of the GDPR as long as the personal data do not from part of a filing system or is intended to form part of a filing system (Article 3(1) GDPR). Case no. 12 should be reviewed, clarified or adapted in relation to the material scope of the GDPR.

Case no. 13 on snail mail mistakes. For this case, it could be useful to have further conclusions as to whether notification of the NSA and Communication to the data subject would be requested if:

- The mail contained Social Security Number
- The mail contained other sensitive data
- Where the customer himself would draw attention to the data breach

Case no. 14 on sensitive personal data sent by mail by mistake. In this example it is stated that Social Security Number is to be considered sensitive data, even though it is not covered by Article 9.1 on special categories of data. Even though some member states have special regulation on Social Security Number, we think this data should not be categorized as sensitive personal data. Therefore, it is questionable if this case should be seen as an example of a breach that falls under the obligation to communicate to the data subject according to Article 34. This should be considered by the EDPB. At a minimum, the heading should be reviewed.

Case no. 15 on personal data sent by mail by mistake. In this case on personal data sent by mail by mistake, the EDPB highlights for the evaluation of the risk, that there is no-one among the recipients with a protected identity. This has not been taken into consideration in other examples. Further in this example it is stated that "food preferences" is to be seen as sensitive data, which is confusing, as it is not covered by article 9, 1. This should be further clarified.

Case no. 16 on snail mail mistake in connection with adjustments of insurance policies. The EDPB states in paragraph 119 that information on the increase of an insurance rate in a following year indicates a motor vehicle claim submitted to the insurance company and could be sensitive to the data-subject, as it might also be linked to an accident. We find the example questionable, as it is highly speculative whether one could make these assumptions from an adjustment of an insurance police. The EDPB should therefore reconsider the recommendation to notify the SA's in a case like this. Generally, when a personal data breach affects a very small number of data subjects, encompass a limited number of non-sensitive categories of personal data and when there are no seemingly aggravating circumstances that suggest that the breach will result in a notable risk for the affected individuals, documentation according to Article 33(5) must be seen as sufficient. As for the technical measures for preventing/mitigating risks in paragraph 123, we suggest adding an extra example on "instructions for counting the actual letters and compare with the number of requested prints".

Case no. 17 on identity fraud. It follows from note 124, that there is a high risk in revealing name, Social Security Number and address, as it can be (mis)used for changing contact information and hence get access to even more personal information. We agree that contact information should not be changed without control, but all the prerequisites of this case could be challenged, as the intention of fraud is not always clear, but should be based on specific circumstances.

Suggestions for further examples

The EDPB should consider including further examples on how to assess:

- formal responsibility for the presumably common instances of unauthorised disclosures of personal data where correctly addressed postal letters containing personal data are delivered and opened by wrongful recipients. Such events can occur due to errors when delivering post and/or when individuals open post explicitly addressed to someone else (which in some member states could constitute a criminal offence).

- a breach that occur as a direct result of the data subject providing the controller with incorrect contact details (postal address, phone number or e-mail address)

- a snail mail with personal data that has disappeared

- more cases on accidental publication of personal data

- not secured transmission

- different levels – or lack of access control