Position Paper

Response to EDPB guidelines on examples regarding data breach notifications

Our reference:	COB-DAT-21-026	Date:	2 March 2021
Referring to:	EDPB Guidelines 01/2021		
Contact person:	Danilo Gattullo, Policy Advisor, Conduct of Business	E-mail:	gattullo@insuranceeurope.eu
Pages:	4	Transparency Register ID no.:	33213703459-54

General comments

Insurance Europe welcomes the opportunity to provide input to the European Data Protection Board's (EDPB) consultation on its draft guidelines on examples regarding data breach notifications. Insurance Europe welcomes the guidelines which provide the necessary clarity on how to handle practical cases of data breach notifications and the obligations that must be adhered to. Nevertheless, Insurance Europe invites the EDPB to clarify the issues below to provide legal certainty to insurers.

Detailed comments

- Title of the guidelines

The heading of the guidelines should include the concept of *personal data breach*es, rather than just data breaches. The current heading could raise questions around whether a breach of non-personal data should be handled according to the guidance or not.

Recommendations: For further clarity, the EDPB should consider changing the heading to reflect the scope of the document.

- Comments on the introduction

  - Paragraph 1: The current wording of paragraph 1 suggests that all personal data breaches must be notified to the supervisor authority and that communication to affected individuals is only required in certain cases. However, article 33 of the General Data Protection Regulation (GDPR) says that a notification is not always required: "…the controller shall without undue delay and, where feasible… notify the personal data breach to the supervisory authority competent in accordance with article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural person".

Recommendation: Wording in paragraph 1 should be aligned with article 33 GDPR.

- Paragraph 8: According to this section: "Data breaches are problems in and of themselves, but they are also symptoms of a vulnerable, possibly outdated data security regime, thus indicate system weaknesses to be addressed." However, not every data breach is indicative of a vulnerable or outdated security regime. Even state-of-the-art security measures will never be able to prevent every data breach.

- Paragraph 9: The guidelines state that controllers should make the risk assessment at the time they become aware of the breach. Furthermore, they should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether the data breach is likely to result in a risk and therefore should be notified. This section should be rephrased as it could be misleading. While a risk assessment should be conducted when the controller becomes 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.

- Paragraph 10: The EDPB states that: "If a controller self-assesses the risk to be unlikely, but it turns out that the risk materializes, the relevant supervisory authority can use its corrective powers and may resolve to sanctions." However, this sentence does not seem to consider circumstantial factors concerning the risk assessment. 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.

- "Relevant supervisory authorities": The EDPB also introduces new terminology in paragraph 10. The term "relevant supervisory authorities" is not clearly defined. The GDPR itself only mentions "lead supervisory authorities" and "other supervisory authorities concerned" to determine the competences in cross-border cases. In past guidelines, the EDPB also used the terms "competent supervisory authorities" and "concerned supervisory authorities". If the EDPB means "concerned supervisory authorities" when it mentions "the relevant supervisory authorities" in paragraph 10 of the guidelines, it would create additional competences in cross-border cases, as according to the GDPR, as only the lead supervisory authorities may use corrective powers outside of the consistency mechanism.

Recommendations: The EDPB should rephrase paragraphs 8, 9 and 10 to better reflect the risk-based approach to data breaches as envisaged by the GDPR. The EDPB should also clarify the term "relevant supervisory authority" in paragraph 10 or align the terminology with the GDPR text.

Case studies

- Case number. 16: Snail mail mistake

In this case, which explicitly mentions the insurance industry, the EDPB has drawn wrongful conclusions on the risks generally associated with an unauthorised disclosure of insurance documents.

Firstly, the EDPB concludes that an increase of the insurance premium of a motor insurance product indicates that a motor vehicle claim has been submitted to the company which, in turn, also indicates that the data subject affected by the breach suffered an accident. This is incorrect. Insurance companies are obliged to carry out risk assessments when providing insurance. Such risk assessments must contain numerous different elements to be accurate and an increase of the rate does not indicate either a claim or an accident. From the insurer perspective, the increased insurance premium does not constitute sensitive data, because with this information it is not possible to:

- Define whether the increased rate is connected to an accident.
- Define whether the potential accident has led to physical injuries or not.
- Identify the subjects involved in the accident (client, driver or third party).
- Identify the scale of the claims that have potentially occurred.

Secondly, the EDPB stresses that birth dates and vehicle registrations numbers are not publicly available. This is also incorrect in the case of most member states, where public authorities that collect and keep records of such categories of personal data (eg tax authorities or transportation agencies) are obligated to disclose them upon request (since it's not covered by secrecy rules). The EDPB should therefore reconsider the recommendation to notify the supervisory authorities in a case like this.

Generally, when a personal data breach affects a very small number of data subjects, encompasses 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. Case number 16 should, for example, be seen as such a breach. If not, an unwanted administrative burden for both controllers and supervisory authorities could be created that would potentially shift the focus of both parties from more severe breaches and other important matters that relate to data protection.

Recommendation: The EDPB should reconsider the risk level presented in this case from medium to low, due to the following reasons:

1. It concerns an individual case and is not indicative of systemic problems.
2. The premium increase cannot be attributed to a specific reason due to the lack of further information.
3. Misuse of the information is extremely unlikely.

- Case number 8: Exfiltration of business data by a former employee

The EDPB is invited to reconsider case number 8 in light of two questions concerning the employer's responsibility. The first question would be if the company in this example should rightfully 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 in time when they copy the business data they are authorised to access during their 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.

In other words, 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 meets the standards of appropriate level of protection according to article 32, the GDPR suggests that the employee, rather than the employer, can be seen as 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 number 8, this outcome would obviously not be satisfactory. The second question would be for how long a former employer can be seen as and held responsible (ie be seen as a controller) for activities relating to personal data carried out by a former employee.

Finally, the EDPB should consider that controllers/employers are, and rightfully should be, limited by the GDPR when overseeing the processing activities carried out by their employees (employees are considered to be a vulnerable group of data subjects) and must to some extent always rely on the element of trust.

In conclusion, this case also suggests that, whenever a misuse cannot be completely ruled out the controller has always to communicate with the data subject. This would not be in line with the risk-based approach established by the GDPR.

Recommendation: The EDPB should review case number 8 in relation to the scope of responsibility of employers towards (ex) employees.

- Case number 12: Stolen paper files with sensitive data

Case number 12 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 scope of the GDPR. In other words, 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 2(1) GDPR).

Recommendation: Case number 12 should be reviewed, clarified or adapted in relation to the material scope of the GDPR.

- Case number 14: Sensitive personal data sent by mail by mistake

Despite the wording of the heading for case number 14, the case does not encompass sensitive personal data. Sensitive personal data must be interpreted as special category data according to article 9.1 (according to national legislation in some member states, special category data is defined as sensitive personal data) and the fact that a group of individuals, identified by names, social security numbers and contact details, is out of employment is not to be seen as special category data.

Recommendation: It is questionable if this case should be seen as an example of a breach that falls under the obligation to communicate according to article 34. At a minimum, the EDPB should review the heading to avoid confusion.

- Potential new cases

The EDPB should consider adding new cases to provide further guidance for businesses. The EDPB could consider including a case 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).

The EDPB could also consider including a case or statement that clarifies if and to what extent a controller can be said to be responsible for notifying the supervisory and/or communicate with a data subject when a breach occurs as a direct result of the data subject providing the controller with incorrect contact details (postal address, phone number or e-mail address).

Finally, while reviewing case number 12 in light of the comments above in relation to the material scope of the GDPR, the EDPB could also consider adding an example of a printed paper with personal data that by mistake is left in a place and read by an unauthorised person.