Position Paper

Insurance Europe's contribution to Article 29 Working Party guidelines on data breach notification

Our reference:	COB-DAT-17-078	Date:	24 November 2017
Referring to:	Article 29 Working Party guidelines on data breach notification		
Contact persons:	Georgia Bakatsia, policy advisor conduct of business Sara MacArthur, policy advisor general insurance	E-mail:	bakatsia@insuranceeurope.eu macarthur@insuranceeurope.eu
Pages:	2	Transparency Register ID no.:	33213703459-54

Introduction

Insurance Europe welcomes the Article 29 Working Party's (WP) draft guidelines on personal data breach notification under the General Data Protection Regulation (GDPR) and the intention to help controllers and processors to meet the new notification and communication requirements.

Overall, Insurance Europe believes that clarifying key notions regarding data breach notification requirements is necessary to provide legal certainty to stakeholders. Therefore, Insurance Europe endorses the clarification of the notion of "being aware of the data breach" and the flexibility provided to stakeholders by establishing, in specific circumstances, an investigation period during which the data subject is not considered to be aware.

The quality of those guidelines is of high importance since they constitute a significant tool for stakeholders when implementing the GDPR provisions. In the context of the public consultation launched by the Article 29 WP, Insurance Europe would like to draw Article 29 WP's attention to the issues outlined below.

Guidelines should respect Level 1 GDPR text

The guidelines would provide insurers with an important tool when implementing the GDPR provisions. However, as agreed by the EU co-legislators, the WP guidelines should not go beyond the Level 1 text of GDPR. This is extremely important: although these guidelines are non-binding, they may be introduced as compulsory requirements at national level.

For instance, on page 22 of the guidelines, the WP recommends that, if in doubt of the existence and level of the risk, "the controller should err on the side of caution and notify".

Following a strict reading of the guidelines, data controllers would have to notify the supervisory authority and the data subject to ensure that they are compliant. As a consequence, the scope of Articles 33 and 34, which requires notification to the supervisory authority and the data subject when specific conditions are met, is significantly broadened.

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

Similarly, on page 23 of the guidelines, the WP recommends that the controller documents its reasoning behind the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented.

However, this recommendation is expanding the scope of Article 33(5) of the GDPR that requires controllers to document the facts relating to the personal data breach, its effects and remedial action taken, without establishing any further obligations to include a reasoning. Thus, the recommendation of documenting a reasoning for not notifying the breach should not be included in the guidelines.

Data gathered as a result of notification requirements: insurance perspective

Insurance Europe also welcomes this opportunity to restate the importance from an insurance perspective of the data that will be collected by the supervisory authorities as a result of the notification requirements in the GDPR.

As recent cyberattacks have demonstrated, cybersecurity is a key issue for businesses across all sectors. This has also been stressed by the European Commission in its recently published Cybersecurity Strategy, which acknowledges that unless we substantially improve our cybersecurity, the risk will increase in line with digital transformation.

Insurance Europe fully shares this assessment and stresses the key role insurance can play in making the EU more resilient to cyber risks. This can happen via insurance products offering protection against a range of cyber risks. Beyond risk transfer, insurers also help their clients implement adequate protection measures and mitigate the effects of a successful cyberattack.

The GDPR will make companies more aware of their cyber risk exposures and of the importance of implementing appropriate cybersecurity measures, and it is therefore likely to lead to a sharp increase in demand for cyber insurance. However, cyber risks are often hard to understand, quantify and underwrite as there is little historical data available due to their ever-evolving nature. This lack of available information and data on cyber risks hampers insurers' ability to offer cyber risk cover and related services.

This could change should insurers be granted access to the (anonymised) data that will be gathered by the national supervisory authorities as a result of the data breach notification requirements in Article 33 of the GDPR. Access to this data would significantly help insurers to increase their ability to underwrite cyber risks, as well as help their clients understand those risks better and how best to prevent and mitigate them.

Insurance Europe therefore calls on the WP to take into account the importance for insurers to be given access to relevant data in a sufficiently granular and anonymised format in its final guidelines on data breach notifications under the GDPR.

To facilitate these discussions, Insurance Europe has developed a template for data breach notifications that could be used by companies across all sectors in case of a data breach. The template provides for an easy mechanism for companies to complete even if still under the effects of a data breach.

The information can be shared with third-parties without having to aggregate or anonymise it beforehand, as the responses are numerical fields or multiple-choice answers. Such a format will help the relevant authorities compare information across companies and sectors, and ensure that the information in both sections remains anonymous and can be safely shared with the insurance sector.

Insurance Europe therefore strongly encourages the WP to make use of this good practice in its final guidelines on data breach notification.