Position Paper

Insurance Europe comments on data breach notification

Our reference:	GEN-CYB-17-017	Date:	01 June 2017
Referring to:	Follow up to the Fab Lab discussions on data breach notification		
Contact person:	Sara MacArthur, Policy Advisor, General Insurance Lamprini Gyftokosta, Policy Advisor, Conduct of Business	E-mail:	MacArthur@insuranceeurope.eu Gyftokosta@insuranceeurope.eu
Pages:	3	Transparency Register ID no.:	33213703459-54

Introduction

Insurance Europe participated in the profiling session of the Fab Lab workshop organised by Article 29 Working Party (WP) in April 2017 and had the opportunity to exchange views on implementation concerns with the WP, as well as with the European Commission (EC) and other stakeholders.

The WP must improve the current dialogue with stakeholders, through the organisation of proper public consultations on its draft guidelines, in line with the European Commission Better Regulation agenda. In order to strengthen the transparency and efficiency of the process, the WP should implement immediately the following improvements:

- The WP should **systematically make all the questions on all topics available to all stakeholders** to be discussed at the workshops **at least two weeks ahead of each workshop**. This would enable stakeholders to get appropriately prepared for the discussions and provide qualitative input on the sector specific implementation issues.

- The WP should **allow stakeholders to participate in several or all sessions of the workshop** as all topics featuring the agendas may be relevant to their sectors. For example, the topics of profiling, consent and breach notification are all key to insurance and an extensive exchange of views on all these topics at the workshop in April would have been mutually beneficial for the WP and the industry. This cannot be achieved only through participation in the plenary session that follows the break.

Insurance is a highly-regulated sector, and the General Data Protection Regulation (GDPR) is one of the many new pieces of EU legislation that insurers will have to comply with by 2018. For example, insurance consumer protection rules will change significantly as a result of the Packaged Retail and Insurance-based Investment

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

Products Regulation (PRIIPs) and the Insurance Distribution Directive (IDD), which are both to be completed by additional Level 2 and Level 3 measures in the coming months.

For the new regulatory framework to be successful, it is crucial to ensure that stakeholders have sufficient time to provide input and that the industry has sufficient time to prepare for implementation. The technical work for new consumer protection rules mentioned above always goes through and appropriate consultation process as part of a dialogue with stakeholders and the European Insurance and Occupational Pensions Authority (EIOPA).

Insurance Europe invites urgently the WP to adopt a similar process when developing the GDPR Level 3 measures. This includes:

- making the consultation schedule publicly available sufficiently in advance;
- consulting stakeholders systematically and at least once on initiatives before they are final, including draft guidelines and conduct an impact assessment;
- ensuring an appropriate consultation period of at least 12 weeks;
- publishing the input of stakeholders, where authorised by the concerned stakeholders;
- providing reasoned feedback on the input received; and
- differentiating clearly drafts from final, adopted documents

In the context of discussions on the Article 29 WP and EC's work on guidelines regarding data breach notification requirements, Insurance Europe welcomes this opportunity to address the issues outlined below.

Insurance Europe position on data breach notification

- Cybersecurity is a key issue for businesses across all sectors.
- Insurance Europe is confident that the GDPR will be instrumental in making companies more aware of their cyber risk exposures and of the importance of implementing appropriate cybersecurity measures.
- Insurance can contribute to making businesses more resilient to cyber risks. This can happen via insurance products offering protection against a range of cyber risks. Beyond risk transfer, insurers typically also help their clients implement adequate protection measures and mitigate the effects of a successful cyberattack.
- The current lack of available information and data on cyber risks hampers insurers' ability to offer cyber risk cover and related services.
- Insurance Europe is of the opinion that the data gathered by the national Data Protection Authorities as a result of the data breach notification requirements could significantly help insurers to increase their ability to underwrite those risks more effectively, as well as help their clients understand their cyber risks better and how best to prevent them.

Insurance Europe therefore calls on the European Commission and the Article 29 Working Party to take into account during the discussions on the GDPR the importance for insurers to be given access to relevant data in a sufficiently granular and anonymised format.

In order to facilitate these discussions, Insurance Europe has compiled a list of data sets/categories that would be useful for insurers underwriting cyber risks. Any guidelines on notification templates should also take into account that standardised formats with checkboxes and/or multiple choice answers will facilitate the creation of useful databases.

Data sets that should be included in data breach notification templates:

- Sector of affected party
- Size - number of employees
- Size - turnover
- Date/time of the incident
- Was the attack a result of a malicious attack, system failure or human error?
    - If a result of a malicious attack, who was the actor?
- Impact of the incident (e.g. data theft, data publication, trojans, encryption, CEO-fraud, blackmailing, property damage, business interruption, liability issues…?)
- Type of data exploited / affected / stolen?
    - Was it personal or corporate (non-personal) data?
    - If personal, how many personal details were stolen?
- If the system was down, how long was the outage?
- What exploit software was used for the attack?
- How long did the attack last before detected?
- How long did it take to end the exploit?
- What damage was done by the attack?
    - Was the damage to the systems or was it physical damage?
- Does the company have any insurance cover? If so, what does it cover?
- What was the motivation, if known, behind the attack?
- What have been the recovery efforts with or without external support like IT security experts (data recovery, deletion of negative software, ransom, replacement of destroyed property, etc)?
- Is there an in-house IT department or is it outsourced? In case it is outsourced, does the external provider hold an approved IT security certification?
- Estimated financial damage
- What has been done to mitigate this exploit being done again (eg staff training, improved security measures, etc)