

Template for data breach notifications

III. COMPLEMENTARY INFORMATION

To be completed and shared with the Data Protection Authority within maximum four weeks after having been made aware of the data breach.

III.1 Date/time effects of attack ended

III.2 How many personal datasets were exploited / affected / stolen?

III.3 Have data subjects been notified of the data breach?

Yes No

III.4 How many data subjects have been notified?

III.5 Estimated financial losses

Cost of notification

Financial damage (if available)

III.6 What has been done or planned to mitigate this exploit being done again?

- enhancement of data security measures and in particular:
 - Audit and redesign of data collection procedure
 - Audit and redesign of data processing procedure
 - Audit and re-evaluate the "Data processor" (if applicable)
 - Encryption of data at rest
- no data security measures were taken
- other

Although all the information used in this template was taken carefully from reliable sources, Insurance Europe does not accept any responsibility (including, without limitation, any liability arising from fault or negligence) for the accuracy or the comprehensiveness of the information given. The information provided does not constitute financial, legal or tax advice.

Recipients of this template should consider the appropriateness of the information given having regard to their own objectives, financial and tax situation and needs, and seek financial, legal and tax advice as relevant to their jurisdiction. In no event shall Insurance Europe be liable for any loss or damage (including, without limitation, costs, expenses, tax exposure or loss of business or loss of profits) arising from the use of or reliance on this template, or otherwise in connection with this publication or its contents.

III.7 Are you aware of the cause of the breach?:

- malicious attack
 - internal
 - external
- accident (system failure)
- negligence (human error)
- other

III.8 If known, what was the motivation behind the breach, in case of a malicious attack?

III.9 If known, what exploit software was used in case of a malicious attack?

- Man-in-the-middle attack
- Malware
- Ransomware
- SQL Injection Attack
- Cross-site scripting (XSS)
- Denial of Service (DoS)
- Session hijacking
- Credential reuse
- Other