

Template for data breach notifications

II. PRINCIPAL INFORMATION ON DATA BREACH

To be completed and shared with the Data Protection Authority within the first 72 hours after having become aware of it.

II.1 Sector of affected party

- Agriculture, forestry and fishing
- Mining and quarrying
- Manufacturing
 - Manufacture of food products, beverages and tobacco products
 - Manufacture of textiles, wearing apparel, leather and related products
 - Manufacture of wood and paper products; printing and reproduction of recorded media
 - Manufacture of coke and refined petroleum products
 - Manufacture of chemicals and chemical products
 - Manufacture of basic pharmaceutical products and pharmaceutical preparations
 - Manufacture of rubber and plastics products, and other non-metallic mineral products
 - Manufacture of basic metals and fabricated metal products, except machinery and equipment
 - Manufacture of computer, electronic and optical products
 - Manufacture of electrical equipment
 - Manufacture of machinery and equipment n.e.c.
 - Manufacture of transport equipment
 - Other manufacturing; repair and installation of machinery and equipment
- Electricity, gas, steam and air conditioning supply
- Water supply; sewerage, waste management and remediation
- Construction
- Wholesale and retail trade; repair of motor vehicles and motorcycles
- Transportation and storage
- Accommodation activities
- Food service activities
- Publishing, audio-visual and broadcasting activities
- Telecommunications
- IT and other information services
- Financial and insurance activities

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.

- Real estate activities
- Legal, accounting, management, architecture, engineering, technical testing and analysis activities
- Scientific research and development
- Other professional, scientific and technical activities
- Administrative and support service activities
- Public administration and defence; compulsory social security
- Education
- Human health activities
- Residential care and social work activities
- Arts, entertainment and recreation
- Other service activities
- Activities of households as employers; undifferentiated goods- and services – producing
- Activities of households for own use
- Activities of extraterritorial organizations and bodies

II.2 Size - number of employees

- 1-9
- 10-49
- 50-249
- 250 - 749
- 750-1000
- > 1000

II.3 Size - turnover

- ≤ € 2 m
- ≤ € 10 m
- ≤ € 50 m
- > € 50 m

II.4 Country where business has its main establishment

II.5 Country where the breach took place

II.6 Date/time of the breach

II.7 Date/time of detection

II.8 Where is data hosted

- Onsite Cloud

II.9 Are you aware of the cause of the breach? (please refer to Q27 in Section 3 if not):

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

II.10 If a result of a malicious attack, what caused the breach:

- Unknown vulnerability
- Known vulnerability:
- Cryptolockers
 - Fire reconnaissance
 - Phishing
 - Distributed denial of service
 - Malware
 - Social engineering
 - Blackmail
- Other

II.11 Which is the likely impact of the breach:

- data publication
- data theft
- identity theft or fraud
- loss of data
- loss of confidentiality of personal data
- property damage
- direct financial loss
- business interruption
- liability issues
- damage to the reputation
- other

II.12 Type of data exploited / affected / stolen?

- personal
 - sensitive (eg health/genetic data, etc.)
 - non-sensitive
- non-personal

II.13 If personal, which is the encryption status of personal data:

- Full
- Partial
- None

II.14 Have the data breached been subject to a Data Protection Impact Assessment (DPIA)?

- Yes
- No

II.15 What type of IT support does the company have?

- internal
- external

II.16 What measures have been taken to mitigate the adverse effects of the breach?

- data recovery
- deletion of negative software
- update system
- replacement of destroyed property
- external testing (eg pen tests, etc)
- enhancement of data security measures
- other

II.17 Does the company have insurance for the type of the incident incurred?

- Yes
- No