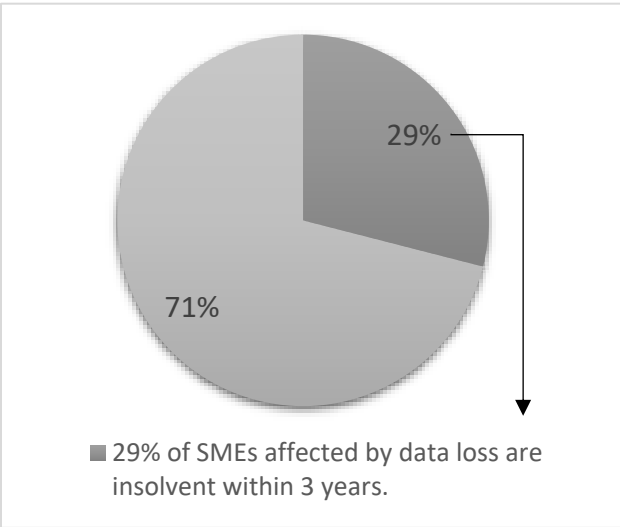
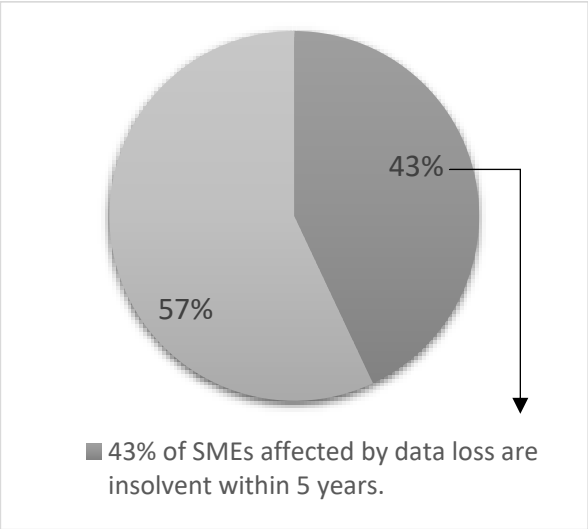
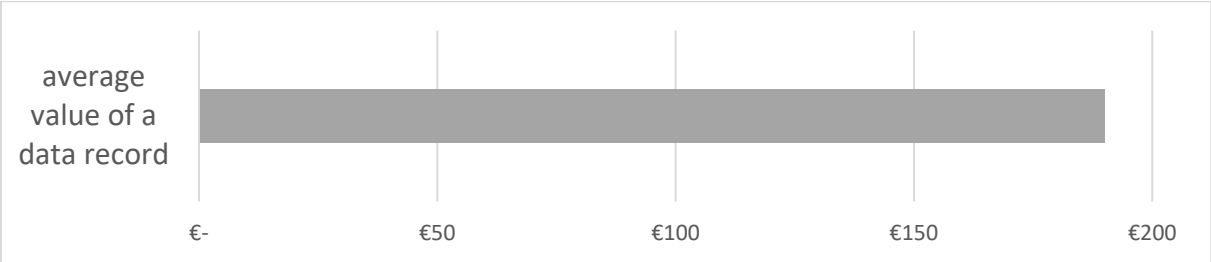
Data Security-Policy







General

People may trust that personal and business data and thus all business-critical information will be kept secret. As for personal data, this is also stipulated as a fundamental right by law.

However, trust also means responsibility for the actions, work, systems and data of customers, employees and suppliers and partners. That is why it is especially important to deal responsibly with this data.

The General Data Protection Regulation (GDPR) unifies the substantive data protection law within the EU as far as possible. The provisions of the GDPR are valid from 25th May 2018. Until then, all data applications must be adapted to the new legal situation. Any company that processes personal data in some way (for example, keeps a customer file, issues invoices, stores supplier data) is affected.

Punishment

Supervisory authorities have extensive investigative and remedial powers. These include, for example house searches, warnings, instructions,... In addition, the supervisory authority also has criminal powers. Therefore, depending on the type of data breach, fines of up to EUR 20,000,000 or up to 4% of the total worldwide annual turnover can be imposed.

Data Processing

Any process or series of operations performed with or without the support of automated processes, in connection with personal data, such as collection, collection, organization, ordering, storage, adaptation, modification, read-out, retrieval, use, disclosure by transmission, dissemination or other

form of provision, reconciliation or association, restriction, erasure or destruction. Data processing is always allowed only for a specific purpose. The purpose must be determined in advance and be clear and legitimate.

Objective scope

The GDPR applies to the fully or partially automated and also manual processing of personal data. Personal data is any information that relates to an identified or identifiable natural person.

Spatial scope

- **Branches within the EU**: The GDPR applies to the processing of personal data for activities of a branch in the European Union. It is applicable even if the processing of data for the establishment does not take place in the EU at all.
    - **Example**: The customer data of an Austrian trading company are stored by the parent company in the USA.
- **Branches outside the EU:** The GDPR also deals with the processing of personal data of persons who are outside the EU and cannot be assigned to an establishment in the EU, but are related to the provision of goods or services to natural persons in the EU.
    - **Example**: A US company offers books in Austria via the Internet.

Rights of Persons Affected

Right to Information

The right to information is one of the rights of the persons affected. Affected persons have a comprehensive right of access to personal data concerning them. The processing of the personal data of data subjects should become transparent. In addition, persons affected can verify the legality of the processing of their personal data. The data subject has a right to know if his personal data is being processed. As far as this is the case, the data subject has further the right to information about the circumstances of the data processing. The right to information extends to the particular data, the purposes of the processing, the categories of personal data being processed and the recipients to whom the data is or has been transferred. In addition, the data subject has the right to information about the planned duration of storage, the origin of the data, insofar as these were not collected from the data subjects themselves and the existence of automated decision-making (especially profiling). This information must always be given free of charge. The answer must be given without undue delay, but no later than within one month. The request for information should, if possible, be answered electronically if it was provided electronically.

Right to Rectification

If a controller processes incorrect personal data, the persons affected can request their immediate correction or, if applicable, the completion of incomplete personal data, as far as this is appropriate in view of the respective processing purposes.

Right to Delete

A person affected may require their deletion by a controller who processes their personal data. If one of the reasons for cancellation set out in Art. 17 GDPR exists, the person responsible must immediately delete the personal data affected.

Grounds for cancellation:

- The personal data are no longer necessary for the purposes for which they were collected or otherwise processed.
- The data subject has revoked their consent to processing (and there is no other legal basis).
- The data subject has objected to processing (and there are no legitimate grounds for processing).
- The personal data were processed unlawfully.
- The deletion of personal data is required to fulfill a legal obligation under Union or national law.

If the controller has made the personal data publicly available, Controller must take appropriate measures to inform other persons responsible that an affected person has requested the deletion (including links, copies and replications). In spite of the applicability of one of the above mentioned points, there is not always a duty to delete, e.g. if the data continues to be required to fulfill legal obligations or assert legal claims.

Right to Restriction of Processing

The person affected is entitled to demand that its data processing is restricted. This is the case if the accuracy of the personal data is disputed by the data subject or if there is a dispute over the authorization of the person responsible for further processing. For example, a restriction can be made by blocking users, removing them from the site,...

Right to Data Portability

Affected individuals may now request that the controller provide the data provided to them in a structured, common and machine-readable format. Concerned persons can also demand that the person responsible transfer their data directly to another controller.

Right of Withdrawal

Affected persons may object to the processing of their data with the exception of a few defined exceptions.

Exceptions are:

- The affected person can prove compelling reasons for the processing, which outweigh the interests, rights and freedoms of the person affected.
- The processing serves the assertion, exercise or defense of legal claims.
- Processing is for scientific, historical or statistical purposes and is required to fulfill a public interest task.

In addition to this "general" right of objection, the GDPR also introduces a separate express right to object to the processing of personal data for the purpose of direct mail.

Right of Appeal

Data subjects are granted the right to complain to the supervisory authority (in Austria: Data Protection Authority, Wickenburggasse 8-10, 1080 Vienna, e-mail: dsb@dsb.gv.at) if they consider that the processing of their personal data violates the GDPR.

Data Breach Notification Duty

If it becomes known that personal data have been "systematically and seriously unlawfully used and threatened with harm to those affected", those affected must be informed immediately. The misuse of data may occur due to the following events:

- Unauthorized access to data, e.g. by external perpetrators (hacking attack) or unauthorized employees
- Theft of IT components and data carriers (PCs, notebooks, USB sticks, paper documents, printouts,...)
- Loss of IT components and data carriers (notebooks, USB sticks, smartphones,...)

It should be noted that the damage does not have to have already occurred; future damage (financially, in terms of reputation or physical threat to those affected) is enough. However, this must also be serious, a likely minor damage does not lead to the emergence of a duty to inform.

The information of those concerned has to be done within 72 hours and can basically be done in every possible form. Apart from direct forms of communication, e.g. by letter or e-mail, the publication in daily newspapers is conceivable. However, account must be taken of the verifiability of the notification (which is given in the case of a registered letter, but not in the case of an e-mail) and the possible negative effects on the reputation of the company, e.g. could appear in a broad publication in the newspaper.

For further questions please contact our data protection coordinator Alexander Gisy (alexander.gisy@innofly.at or 0660 6233407).