Data protection policy

Contents

Version history

Version	Date	Author	Approved by
1.0	9.4.2018	Maija Pylkkänen, Joonas Mämmelä	Director general
2.0	30.10.2019	Maija Pylkkänen, Joonas Mämmelä	Director general
3.0	10.11.2022	Maija Pylkkänen, Lena Nordqvist	Director general, Board of Business Finland Oy

Introduction

Data protection means the protection of privacy when processing personal data. The importance of data protection has increased in a digital, global world and the EU has responded to this with a Data Protection Regulation, which applies as it stands in all Member States. The Regulation applies to both companies and authorities. The Innovation Funding Agency Business Finland and Business Finland Oy undertake to comply with the EU's General Data Protection Regulation (GDPR).

The data protection policy defines the responsibilities and data protection principles accepted internally by Business Finland for processing the personal data of customers, partners and other stakeholders as well as employees and job seekers. With the data protection policy and function-specific data protection guidelines derived from the policy, we aim to ensure the legal processing of personal data and an appropriate level of data protection.

Our key values are responsibility and maintenance of customer trust.

Responsibilities and organization

ROLE	RESPONSIBILITIES
Mangement (Management group)	• Overall responsibility for data protection for own service area • Allocates resources and assigns responsibility
Data Protection Officer	• Advises, develops and supervises the implementation and application of the regulation • Supervises the preparation and availability of the documentation required by the fulfilment of accountability • Supports the realization of the data subject's rights • Promotes privacy awareness • Acts as a contact point in-house and for external parties (tietosuoja@businessfinland.fi) • Takes care of regular risk mapping • Reports to the senior management
Data protection contact persons (role-based business representatives confirmed by the management team)	• Participate in the activities of the data protection group and mapping of data protection risks • Maintain data protection awareness and coordinate data protection-related issues and documentation in their service area • Respond to information requests regarding personal data in their service area, correct and possibly delete the information
Personnel	• Participates in training activities, comply with the related instructions and uses shared systems • Duty of confidentiality and prohibition of exploitation • Reports any deficiencies in data protection

Principles

Business in Finland applies the following principles in the processing of personal data:

Lawfulness, fairness and transparency

Business Finland complies with the principle of transparency. Data is collected and processed in the manner required by the Data Protection Regulation and other legal acts. Privacy policies have been drawn up for registers, and the legal basis for the processing of personal data is described in the privacy policies.

Purpose limitation and data minimization

Data is only collected on a purpose-limited basis and the amount of data collected is minimized.

Accuracy, limitation, integrity and confidentiality

Personal data is kept up to date and obsolete data is removed or updated. The availability of data within the organization is restricted appropriately. The integrity of data is monitored. The confidentiality of data is ensured by administrative and technical means. The implementation of these principles is monitored, deviations are addressed and implementation can be demonstrated by means of documentation.

Data security and risk management

Data protection work is risk-based. Risks are reviewed regularly and corrective measures are taken based on them. Risks are reported to senior management. Data protection functions as an enabler of the implementation of the principles of data protection. Regular verification, assessment and development constitute the basic framework of the work. The principles of data protection are described in more detail in Business Finland's data protection guidelines.

Data protection by design and by default

The data protection requirements are laid down at the design and procurement stage of a system, application or service. Business Finland implements the requisite technical and administrative changes before introducing the system, in order to secure the rights and privacy of data subjects. Data protection requirements apply to data throughout its life cycle.

Accountability

Business Finland is able to demonstrate measures compliant with its principles and to report regularly on its activities. The data protection organization steers, develops and monitors the units in the fulfilment of accountability.

Procurement

Risks related to personal data are assessed at the planning stage of procurement by the procuring unit. Data protection requirements are identified at the tendering stage. The procuring unit is responsible for data protection when outsourcing the processing of data, and for ensuring that the selected partner complies with the Data Protection Regulation. Acquisitions subject to data protection are reviewed on a regular basis. A written data processing agreement is always drawn up on the outsourcing of personal data processing.

International transfers of personal data

This Privacy Policy covers Business Finland's operations in all of Business Finland's countries of operation.

Due to the international structure of Business Finland's operations, personal data is transferred both within the EU/EEA region and outside the EU/EEA region. It is allowed to transfer personal data from one country to another within the EU/EEA area. When we transfer personal data outside the EU or the EEA, we make sure that an adequate level of data protection is also implemented in the country to which the transfer is made. Depending on the country that is the target of the transfer, a sufficient level of data protection can be guaranteed, for example, by concluding an agreement with the transferee using the EU Commission's model contract clauses. In addition, we conduct international transfers regarding TIA (transfer impact assessment) risk assessments and implement the necessary additional measures.

Obtaining, processing, transfer and disclosure of data

The acquisition and processing of data takes place under the conditions laid down in the Data Protection Regulation. The processing of data is restricted and role-based. Disclosure and transfer of data takes place only in predetermined cases, and this is indicated in the privacy policy. At Business Finland, data may be disclosed within the provisions of the Act on Business Finland (1146/2017). Under the Act on the Customer Data System for Enterprise Services (293/2017), confidential customer data of the Ministry of Economic Affairs and Employment's administrative branch is shared. Disclosure of public information relating to the funding agency and funding activities is based on the Act on the Openness of Government.

Rights of data subjects and provision of information

Business Finland's privacy policies are available on our website, which also provides right of access to personal data forms and rectification request forms. Information on data protection is also provided on a case-by-case basis in connection with communication.

Impact assessment

If the acquired application is considered to cause significant risks to data protection, an impact assessment will be performed on it.

Procedure when data protection is compromised

If the application to be procured is deemed to pose significant risks to data protection, it will be subjected to an impact assessment. Procedure in the event that data protection is undermined: If, on the basis of our monitoring or report, we notice that data protection has been undermined, we will conduct a risk assessment from the perspective of the rights of the individual in question. We will inform the person concerned, the Finnish Communications Regulatory Authority, the data protection authorities and the police of any serious personal data breach.

Sanctions

Business Finland is responsible for the damage caused to the data subject due to the illegal processing of personal data. Illegal processing of personal data can also lead to possible criminal sanctions. In addition, breach of data protection obligations on the part of Business Finland Oy may result in an administrative fine imposed by the supervisory authority. Acts that violate personal data processing regulations, this privacy policy or Business Finland's privacy guidelines are considered activities that endanger data protection, which may result in disciplinary or labor law sanctions for Business Finland's personnel.

Provision of information

This policy is published on Business Finland’s website. Internal and external customers may contact tietosuoja@businessfinland.fi to submit inquiries.