

# Data protection policy

## Contents

Introduction .....	3
Responsibilities and organisation.....	3
Principles .....	4
Lawfulness, fairness and transparency .....	4
Purpose limitation and data minimisation.....	4
Accuracy, limitation, integrity and confidentiality .....	4
Data security and risk management.....	4
Data protection by design and by default .....	4
Accountability .....	4
Procurement .....	5
Obtaining, processing, transfer and disclosure of data .....	5
Rights of data subjects and provision of information.....	5
Impact assessment.....	5
Procedure in the event that data protection is undermined.....	5
Provision of information.....	5

## Version history

Version	Date	Author	Approved by	Changes
1.0	9 April 2018	Maija Pykkänen, Joonas Mämmelä	Board of Directors	First version
2.0	1 December 2019	Maija Pykkänen	General Director	Governance model change

## 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).

Our key values are maintenance of customer trust, and responsibility.

## Responsibilities and organisation

The overall responsibility for data protection at Business Finland lies with senior management (the Management Team).

The directors act as the owners of data for their service areas, appointing data protection contact persons for these areas who promote data protection awareness and the processing of personal data in accordance with the Regulation, as well as the fulfilment of accountability. They are responsible for information requests with respect to data in their service area.

Each employee at Business Finland must be familiar with the basic principles of data protection, comply with the related instructions, participate in training activities, use shared systems, and report any deficiencies in data protection.

As part of the consolidation of the governance model, Business Finland has appointed the data protection officer who provides guidance and advice on implementing and applying the Data Protection Regulation. The data protection officer monitors the implementation of the Regulation's requirements and ensures that documentation pursuant to accountability in the Regulation has been drawn up and is available. The data protection officer ensures that risk assessments are conducted on a regular basis, and reports to the organisation's senior management. The data protection officer acts as a contact point within the organisation and for external bodies ([tietosuoja@businessfinland.fi](mailto:tietosuoja@businessfinland.fi)). The competence of the data protection officer is enhanced continuously.

A data protection team consisting of data protection contact persons supports the work of the data protection officer. The team meets regularly and whenever necessary to discuss data protection issues. For their part, the units are responsible for allocating the requisite resources. The function of the data protection organisation is to ensure that accountability is fulfilled, to coordinate the personnel's training, and to oversee the implementation of data protection as a whole.

## 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 minimisation

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

### 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 organisation 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 on their basis. 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 guideline.

### 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 lifecycle.

### Accountability

Business Finland is able to demonstrate measures compliant with its principles and to report regularly on its activities. The data protection organisation 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.

### 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 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.

### Provision of information

This policy is published on Business Finland's website. Internal and external customers [tietosuoja@businessfinland.fi](mailto:tietosuoja@businessfinland.fi).

This data security policy comes into effect on 1 December 2019 and replaces the previous version. The data protection officer reviews the document annually.

Nina Kopola  
Director General