

# DATA PROTECTION POLICY FOR THE HANDLING OF PERSONAL DATA

This Group-wide policy has been prepared by the Director of Economy in collaboration with the Legal Counsel and Privacy Consultant. The Group-wide policy provides guidance for all Balder's subsidiaries, although local deviations may occur. The policy is reviewed annually and adopted by the company's Board of Directors.

## 1. BACKGROUND

This policy is based on the requirements of the EU's General Data Protection Regulation (GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council) ("GDPR") and shall describe how the Fastighets AB Balder Group ("Balder") processes information that can be directly and indirectly attributed to physical individuals ("personal data"). All individuals whose personal data is processed within the framework of Balder's operations shall feel secure about the way this happens. Balder's objective is to always report in a clear and transparent way which personal data is processed in our operations and in what way, and to comply with current data protection legislation in a correct way.

It should be noted that there are other key documents within the framework of Balder's data protection work that are called "policies", which should not be confused with Balder's governance documentation, which includes this Data Protection Policy, and which are to be adopted by the management team and the Board of Directors. These documents are denoted by \* under Section 9 below.

## 2. PURPOSE

The purpose of this policy is to provide guidelines on a general level describing how personal data may be processed, for what purposes and in what way.

This policy shall ensure that Balder:

- complies with current data protection legislation;
- stores and processes personal data in a correct, consistent way;
- communicates clearly and openly about how personal data is handled in its operations;
- can satisfy the rights of employees, customers and other stakeholders;
- protects the company's own operations against threats and thus minimises privacy risks.

## 3. SCOPE

The policy has been prepared by the Data Protection Responsible at Balder and encompasses all processing of personal data that is performed within the Group. The Data Protection Responsible is the Director of Economy, who can delegate roles, duties and/or responsibilities to the Legal

Counsel or Privacy Consultant. The policy shall be supplemented with guidelines and procedures for information security, as well as other specific operational areas. The guidelines shall be followed by management, employees and other persons working on assignment for or under the supervision of Balder, such as consultants or partners.

#### **4. APPLICABLE DATA PROTECTION LEGISLATION**

The handling and protection of personal data is regulated in general terms by the EU's General Data Protection Regulation (GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council) and by supplementary Swedish legislation in the form of the supplementing Swedish Data Protection Act and associated Ordinance (SFS 2018:218 and SFS 2018:219). Additional relevant legislation may be introduced.

Within the framework of Balder's operations, it is primarily the following laws and provisions that apply:

- The EU's General Data Protection Regulation (GDPR)
- The supplementing Swedish Data Protection Act
- The Swedish Discrimination Act
- Occupational health and safety legislation and the Swedish Work Environment Authority's regulations
- The Swedish Annual Leave Act
- The Swedish Parental Leave Act
- The Swedish Sick Pay Act
- The Swedish Employment Protection Act
- The Swedish Act on Co-determination in the Workplace
- The Swedish Unemployment Insurance Act
- The Swedish Enforcement Code
- The Swedish Bookkeeping Act
- The Swedish Marketing Act
- The Swedish Market Abuse Regulation (and supplementary legislation)
- The Swedish Companies Act
- The Swedish Act on the Protection of Persons Reporting Irregularities ("The Whistleblowing Act").

#### **5. IMPORTANT TERMS AND DEFINITIONS**

This policy concerns the handling of personal data. Personal data is any information that can be used to identify an individual person, either directly or indirectly. The term 'personal data' includes (but is not limited to):

- personal data of a general nature, such as name, personal ID number, email address, phone number, address, postal code, photograph or video recording, responses in market research surveys;
- recruitment-related personal data, such as profile on social media, CV, cover letter;

- employment-related personal data, such as form of employment, period of employment, gender, pay and pension information, sick leave, personal data associated with serving of notice or dismissal, bank details, time worked, trade union membership;
- personal data relating to a tenant, stakeholder in a tenant-owner association or project etc., such as object, agreement or apartment number, loan commitment details, income and, if relevant, benefits;
- reference statements and certificates in respect of candidates and tenants;
- personal data relating to the performance of a work assignment, such as GPS details for registration in driving log, employee appraisals and personal goals;
- technical information such as IP address, browsing history, cookies, login details, tags and logs in respect of access control systems, energy meter information;
- shareholder-related information, such as close relatives and children living at home, shareholding and number of votes.

The phrase **processing of personal data** includes everything that is done in which personal data is involved, for example the administration of, communication with and storage of such data for various purposes and in various contexts.

If there is any **sensitive personal data** in Balder's operations, special rules apply for this.

Sensitive personal data is:

- data that reveals race or ethnic origin;
- data that reveals political opinions;
- data that reveals religious or philosophical belief;
- details of trade union membership;
- details of health;
- details of sex life or sexual orientation;
- genetic information, and
- biometric data used to unambiguously identify a physical person.

Please note that data that indirectly reveals sensitive information of this kind is also included. Balder, and primarily Fastighets AB Balder, is the **controller** of most personal data processing activities that take place in its operations. This means that the organisation is the legal entity that is ultimately responsible for the personal data, and that decides on purpose and means. In specific cases, a party other than Balder may be the controller. Roles and the delegation of responsibilities between the organisation and **processors**, if relevant, shall be specified for each processing activity in the record of processing activities.

## 6. PURPOSE OF THE PROCESSING OF PERSONAL DATA

Balder processes personal data about employees or candidates to the extent necessary in order to manage and administer recruitments, and to enable Balder and its employees to fulfil their obligations and exercise their rights in accordance with employment contracts, and to perform their duties and other commitments in connection with the employment arrangement.

Balder processes personal data for the purpose of administering, communicating and making agreements with tenants or stakeholders who have shown an interest in our objects or projects and/or wish to buy or rent an apartment or commercial building, or are already renting an

apartment, commercial building, parking space, garage or store from Balder, either in the capacity of a private individual or as the representative of a business.

In order to have an effective IT system and to be able to perform Balder's business operations in an efficient way, Balder processes personal data, which includes sharing it with IT providers that process personal data on behalf of, and as instructed by, Balder.

Balder processes personal data in order to administer and follow up on participation in competitions, events and market research surveys and evaluations, and to manage, store and use images or film material.

Balder processes personal data in order to administer and perform work to prevent crime and create security, and to manage legal claims in which Balder is involved, or in other legal cases.

Balder processes personal data in order to establish and administer contacts and agreements with suppliers or partners.

Balder processes personal data for the purpose of providing and administering contacts and visits with us via our website or social media channels, or when Balder sends out marketing material.

Balder manages reported whistleblowing cases and meets its obligations arising from this.

## **7. GENERAL GUIDELINES**

### **7.1 Training**

All employees shall be given basic data protection training, in order to ensure an understanding of the importance of handling personal data correctly. The person responsible for ensuring that training is provided is the Data Protection Responsible.

Each department is responsible for ensuring that employees concerned are able to study any instructions and procedures that are relevant to them, and any information that is needed to ensure that everyone can perform their work in line with data protection legislation. This includes, but is not limited to, training new employees.

### **7.2 Record of processing activities**

Detailed information about all kinds of processing of personal data that takes place in processes, IT systems and in different departments within the framework of Balder's operations shall be documented in the organisation's record of processing activities. The record of processing activities shall be kept updated on an ongoing basis and serve as a comprehensive record of all personal data processing activities, in accordance with Article 30 GDPR.

The record of processing activities is administered by the Data Protection Responsible. System and information owners and department managers may be delegated responsibility for specific parts of the record of processing activities in collaboration with the Data Protection Responsible. The record of processing activities may be presented to the supervisory authority on request.

### 7.3 Legal basis

To be legal to handle the personal data, all processing of personal data shall be based on a specified **legal basis**. No personal data may be processed at Balder without an identified, appropriate legal basis. A valid legal basis might be, for example, an agreement that must be fulfilled, a legitimate interest, a legal obligation (e.g. in accordance with the Swedish Bookkeeping Act or the Swedish Discrimination Act) or an actual consent from a data subject. All of the possible legal bases are listed in Article 6 GDPR.

It is not permitted to process sensitive personal data apart from in specific exceptional cases, which shall in such an event be described in the record of processing activities and in supplementary policy documents/procedural descriptions.

### 7.4 Limitation of purpose and data minimisation

Personal data may only be processed for specific purposes, and to the extent required and in accordance with data protection legislation.

Only such personal data that is necessary may be collected and saved. No data may be saved using vague justifications such as that it "might be good to have".

The processing of personal data in new contexts (for new purposes) must always be evaluated and checked in advance with the Data Protection Responsible, in order to ensure that the new processing activity does not risk infringing the privacy of data subjects or in any other way violate data protection legislation.

### 7.5 Limitation of authorisation

The personal data used in business operations shall only be accessible to people who specifically need it in their work. There shall in general be a narrower delegation of authorisation for sensitive personal data than for more harmless data.

### 7.6 Storage minimisation

Personal data that is no longer required (and that there is no longer an obligation to save) shall be deleted on an ongoing basis. Please note that there may be legal requirements to archive and save data, but there shall be deletion procedures for each process and each system where personal data is processed. Everyone who works there is obliged to follow these procedures.

Personal data may not be used in any other way or transferred to and/or processed at any other location (system/storage place/device) than is instructed in current procedures and instructions.

### 7.7 Information to data subjects

Anyone whose personal data is being handled by Balder has the right to information about how their personal data is being handled. This applies to employees, tenants and other groups. The information shall be easily accessible and sufficiently detailed to meet the requirements of data protection legislation. The information shall be provided in a clear, precise manner.

The information is provided primarily via the intranet (for employees) and on the public website in the form of an information page aimed at tenants, condominium stakeholders/buyers and users.

#### 7.8 The rights of data subjects

Balder shall have procedures and instructions in place describing how the organisation is to fulfil its obligations towards data subjects. The rights of data subjects are set out in Chapter 3 GDPR (Articles 12–23), and Balder shall be prepared to satisfy these rights in all situations required. This includes the aforementioned obligation to inform, as well as the right to access (request for extract from the records), rectification, erasure, restriction, data portability and the right to object.

#### 7.9 Storage and information security

All personal data at Balder shall be protected through secure servers and other appropriate technical and organisational security measures in accordance with Article 32 GDPR. Sensitive personal data generally requires a higher level of security than more harmless data. There are further specifications regarding information security within Balder in the separate IT Policy/Information Security Policy.

#### 7.10 Disclosure of personal data to a third party

Balder shares personal data with companies within the Group and with business partners and suppliers in the way described below:

- Balder shares personal data with the company within the Balder Group that leases the apartment, garage, parking space or store in question;
- Balder shares personal data about representatives of an organisation that is a potential, current or former supplier or partner of the company in the Group to which the contact or agreement in question relates;
- Balder shares personal data with companies that Balder engages to perform various service solutions and that process personal data on behalf of and as instructed by Balder, e.g. various IT suppliers, partners for administration and marketing, and companies that manage salaries, other remuneration and staff benefits;
- Balder may disclose personal data to government agencies, e.g. to the Swedish Tax Agency, the Swedish Social Insurance Agency and the Swedish Enforcement Authority, to the Social Services in connection with a report of concern and to the Police in connection with a report to the police;
- in the event of failure to make payment, personal data is given to a debt collection company, which is the independent controller and conducts debt collection activities;
- Balder shares personal data with government agencies and courts in cases where Balder has a legal obligation to do so, or in cases where we have a legal claim;
- Balder shares personal data in social media channels, such as in connection with participation in a competition or if Balder publishes a photo that people are involved in;

- Balder may share personal data with IT and analytical tools, such as Google and Meta, for analysis of the use of Balder's website in order to improve its functionality, and to provide relevant and adapted marketing;
- personal data will be shared with companies with which Balder collaborates and that in certain cases have an independent responsibility as controllers of the personal data they receive, such as insurance companies, banks and audit firms.

The disclosing of data in this way constitutes a processing of personal data. There shall always be a legal basis for such disclosure, and the data subject shall have been informed about that their data is being disclosed outside Balder.

#### 7.11 Processing of personal data outside the EU/EEA

The IT suppliers we use may transfer personal data outside the EU/EEA. This is done if there is support for the transfer in accordance with GDPR. This means that the transfer can be based on, for example, the EU Commission's decision or standard contract clauses with supplementary security measures.

#### 7.12 Data processing agreement

Balder only engages processors that guarantee appropriate technical and organisational measures and in other ways can provide guarantees that the requirements of GDPR are fulfilled also when another actor processes personal data on our behalf. There shall be written data processing agreements with all suppliers and other processors. The Data Protection Responsible is responsible, together with each information owner, for checking that there is a data processing agreement in place and that it reflects the requirements in Article 28 GDPR.

#### 7.13 Reporting data breaches

Anyone who discovers or suspects a breach that could pose a privacy risk shall report this to the Data Protection Responsible. A personal data breach can be anything from someone having lost their mobile phone to a hacker attack in which information about customers and credit cards has been stolen. The Data Protection Responsible is responsible for procedures for the handling of breaches at Balder. More information is available in the separate Procedure for Responding to Personal Data Breaches.

## 8. ROLES AND RESPONSIBILITIES

The following people have special responsibilities for areas of data protection work:

- IT Manager  
Is responsible for the establishment of the required level of security and compliance with the current IT and security policy. The IT Manager is a member of the Personal Data Breach Response Group.
- Director of Economy  
Serves as Data Protection Responsible and is responsible for Balder's regulatory compliance with current data protection legislation. The Director of Economy is a member of the Personal Data Breach Response Group.

- Privacy Consultant

Is responsible, on behalf of the Data Protection Responsible, for guaranteeing the operation's work on data protection and compliance with GDPR. The Privacy Consultant is a member of the Personal Data Breach Response Group.

- The GDPR Network

The members of the GDPR Network shall, on the instruction of and with guidance from the Data Protection Responsible, ensure and enable Balder's employees to have sufficient knowledge of GDPR and Balder's internal governing documents and external policy documents. Members are responsible for their operational area, or the system for which a system owner is responsible, and transfer knowledge to the organisation and serve as the Privacy Consultant's primary contact and link with their respective operations and/or systems.

Each department that processes personal data in its operations must guarantee that the data is processed in accordance with this policy and follows supplementary instructions drawn up.

Everyone who works within the framework of Balder's operations is obliged to follow this policy and to collaborate with individuals responsible when relevant.

## 9. SUPERVISORY AUTHORITY

Balder has made the assessment that the supervisory authority responsible for the business operations is the Swedish Authority for Privacy Protection (IMY).

Individual persons who have complaints regarding Balder's handling of personal data have the right to contact IMY.

## 10. SUPPLEMENTARY POLICIES AND INSTRUCTIONS

Additional guidelines and instructions concerning Balder's processing of personal data are contained in the following documents:

- Procedure for Responding to Personal Data Breaches
- Procedure – Exercising of Rights, GDPR
- IT Policy
- Information Policy
- Whistleblowing Policy
- General Privacy Policy\*
- Privacy Policy for Letting to Private Individuals\*
- Privacy Policy for Commercial Letting\*
- Privacy Policy for New Production\*
- Privacy Policy for Recruitment\*
- Privacy Policy for Employees\*
- Privacy Policy for Relatives\*
- Privacy Policy for Shareholders, Board Members and Persons with Insider Information\*
- Privacy Policy for the Whistleblowing Function\*.



Gothenburg, 9 February 2024

Board of Directors of Fastighets AB Balder