INFORMATION ON PROCESSING OF PERSONAL DATA WHISTLEBLOWING FUNCTION

The following information describes the processing of personal data that takes place in connection with our handling of whistleblowing cases, as well as your rights as a data subject.

CONTROLLER

The Controller in relation to the processing of personal data is:

Fastighets AB Balder, corp. ID no. 556525-6905

Box 53121, 400 15 Gothenburg

Contact: info@balder.se / Phone: +46 (0)774 49 49 49

Data Protection Officer:

dataskydd@balder.se

For additional information about our processing of personal data, please refer to the current version of our Privacy Policy.

PURPOSE AND LAWFULNESS OF THE PROCESSING

The purpose of the processing is to enable compliance with the statutory requirements imposed on the organisation with regard to the provision of a whistleblowing service, and to perform the investigations required in relation to whistleblowing cases. The purpose is also to process personal data where necessary in connection with the following up of whistleblowing cases. This means that we may need to process personal data in order to:

- Handle reported whistleblowing cases,
- Safeguard the rights and obligations of the organisation based on the instances of misconduct or impropriety detected in the whistleblowing cases, or
- Comply with the statutory requirements imposed on the organisation.

As a starting point, the lawful basis for the processing of personal data in connection with whistleblowing cases is the legal obligation pursuant to chapter 5, section 2 of the Swedish Act on the Protection of Persons Reporting Irregularities.

The lawful basis for the processing of personal data in connection with the following up of whistleblowing cases and other measures taken in relation to a reported case, is compliance with a legal obligation or the organisation's legitimate interest in safeguarding its rights based on suspected or confirmed instances of misconduct or impropriety.

CATEGORIES OF DATA SUBJECT

In connection with the handling of whistleblowing cases, processing of personal data may take place in relation to the following categories of data subject:

- The person who reports a case, if he or she does not choose to remain anonymous,
- The person or persons included in a report, or
- The person who has an administrative role in relation to the processing and investigation of reported cases.

DISCLOSURE OF PERSONAL DATA AND PROCESSORS

Personal data may be disclosed to competent authorities (e.g. the Swedish Police if a whistleblowing case leads to the filing of a police report). Personal data may also be disclosed to other parts of the business or other companies within the group in connection with the investigation and following up of whistleblowing cases and actions taken in relation to such cases.

Personal data is also processed by Processors in connection with whistleblowing cases. These Processors may only act in accordance with our instructions, which are specifically regulated in a data processing agreement.

TRANSFERS TO THIRD COUNTRIES

We strive to ensure that personal data is not transferred to a country or company located outside the EU/EEA and that all storage of personal data relating to the content of whistleblowing cases takes place within the EU/EEA on servers that are owned by companies in Sweden.

The login administration takes place via an active directory, Microsoft Azure. The storage of personal data takes place within the EU/EEA. However, the service provider is American, which means that there is a risk that login-related personal data may be made available to American authorities, which could entail a negative impact on privacy protection due to the fact that American authorities are not obligated to comply with GDPR. If personal data is transferred to a third country, standard contractual data protection clauses are used as a safeguard. Please contact us if you would like more information about how we protect your personal data.

STORAGE AND CULLING

Personal data processed in connection with a whistleblowing case will be saved for two years following completion of the case.

Personal data processed in order to manage administration and permissions will be saved for as long as the relevant permissions are valid.

All personal data is culled at the end of the storage period.

If a case requires continued investigation internally, we will continue to process your personal data for as long as necessary in relation to the case.

YOUR RIGHTS AS A DATA SUBJECT

When we collect and process your personal data, you have certain rights as a data subject. You have the right to:

- Request a register excerpt with details of the personal data processed by the company and the way in which such data is processed;
- Request rectification of any inaccurate personal data;
- Request erasure of personal data. However, this can only be done if the company does not have the right to retain the personal data pursuant to some other lawful basis;
- Request that the processing be restricted in certain circumstances, e.g. for the period of time during which an investigation is conducted into the issue of whether or not the personal data is accurate;
- Exercise the right to data portability;
- Object to profiling. This only applies to data that you have provided to the company, in circumstances where the data is subject to automated processing and is processed on the basis of a contract or consent; and
- Contact an authorised supervisory authority (in Sweden the relevant authority is IMY – the Swedish Authority for Privacy Protection) if you wish to lodge a complaint about how we process your personal data.

Please note that your rights as described above may be affected by the duty of confidentiality that applies to whistleblowing-related data, as well as in cases where disclosure makes the investigation more difficult. The possibility to exercise your rights will be assessed on the basis of, among other things, the purpose and lawful basis of the processing in question.

If you have questions regarding the processing of your personal data, please contact us via the contact details provided in the first section of this document.

SECURITY

The company implements appropriate technical and organisational information security measures to prevent and limit risks associated with the provision of personal data, such as unauthorised access, disclosure, misuse, modification and destruction. Only a small number of authorised persons, all of whom are bound by a duty of confidentiality, have access to identifiable personal data.