

APPENDIX 4

Data Processing Instructions

Version 2024-09-24

Definitions used in these Instructions shall have the same meaning as in the Processor Agreement unless the circumstances clearly indicate otherwise.

1. Categories of personal data

The Supplier normally processes the following data in order to be able to perform the service: name, address, IP addresses, email address and telephone number.

2. Special categories of personal data

Sensitive Personal Data is not covered by the Processor Agreement and shall not be processed by the Supplier.

3. Categories of data subjects

Users of the Housing Platform – Registered for the purpose of providing a complete housing experience for the user, including paying rent, booking the laundry room, reporting faults, and more.

The Customer’s staff – Processed as users in the system in order to configure and manage the housing platform.

4. Processing

The Supplier shall primarily process Personal Data on behalf of the Customer for the provision of the Service for the purposes stated below. The Supplier may also, following consent from the end customer, transfer personal data to the partners that are registered on Avy’s platform at any given time.

5. Purpose of each processing operation

The purpose of each Processing operation is to fulfil the Service Agreement, including providing the Service so that the Customer’s users can use it and so that the Customer’s tenants can use the Service by connecting to it, and to ensure that the Service contains correct and up-to-date information.

6. Sub-processors and location of processing of personal data

Company processing personal data	Type of processing	Location of processing
Brevo	Communication	EU
Amazon Web Services	Cloud-based IT solution. Operation and storage of data. Data is protected with encryption and an encryption key to which only the Processor has access.	EU
Google Cloud Platform (GCP)	Cloud-based IT solution. Operation and storage of data. Data is protected with encryption and an encryption key to which only the Processor has access.	EU
Microsoft Azure	Customer service and customer insights supported by Generative AI. No data on Azure is used to train language models.	EU

7. Security measures

7.1 Technical and organisational security measures

The Supplier has an outsourced, cloud-based operating environment. To meet the security requirements, the Supplier takes the following technical and organisational security measures:

7.2 Pseudonymisation

The Supplier does not apply pseudonymisation of personal data as a security measure, as the purpose of the Processing could then not be fulfilled.

7.3 Encryption

The Supplier continuously develops, implements and takes measures to encrypt electronic transmissions of personal data outside the Supplier's network, to prevent the personal data from being read, copied or modified by unauthorised persons or without permission.

7.4 Confidentiality, authorisation and permissions regarding the processing system

The Supplier continuously takes and implements the measures below to manage confidentiality, authorisation and permissions regarding the system for processing personal data:

- separate password authentication to the data processing system;
- a permissions structure that restricts access to data based on functional need; and
- logging of access to the processing system;
- separation of the Processing in the processing system from other processing.

7.5 Resilience of the processing system

The Supplier continuously takes and implements the measures below to manage the resilience of the processing system:

- monitoring of the server components that make up the processing system;
- regular penetration tests of the processing system.

7.6 System owner and system administrators

The Supplier continuously takes and implements organisational measures to ensure control over the use of the processing system and the Personal Data therein. Igor Kovacevic has been appointed as responsible for data protection. He is responsible for the processing system (the "System Owner"). The System Owner leads a working group whose members are appointed as system administrators of the processing system.

7.7 Incident management and notification of security breaches

The Supplier continuously takes and implements organisational measures to be able to handle incidents and security breaches. The System Owner's working group is tasked with receiving information about, evaluating, reporting without undue delay and following up incidents and security breaches. The goal of the incident response is to restore the confidentiality, integrity and availability of the service environment, and to establish underlying causes and corrective actions. The Supplier shall notify the Customer of all incidents that may be of significance for the personal data processed on behalf of the Customer.

8. Storage minimisation

The Supplier continuously implements routines and measures to be able to weed out (delete) Personal Data as follows: The Supplier does not store Personal Data for longer than is required to fulfil the purpose of the Processing. The Supplier is moreover obliged to take into account the storage periods prescribed by law. To the extent Personal Data cannot be deleted in connection with the termination of the Processor Agreement, the Supplier Processes the Personal Data for as long as it has a statutory obligation to Process the Personal Data.

8.1 Deletion

The Supplier shall, on behalf of the Customer, delete customer data that is no longer needed for the performance of agreements with end customers. For certain information, the Supplier may have statutory requirements to retain information on its own account, under applicable law. In such cases, deletion will be completed once the statutory retention period has passed. In addition to the statutory requirements, the Supplier undertakes to promptly activate deletion of all personal data relating to customers that is attributable to the agreement between the Parties as follows:

- a) the housing company notifies that the tenant has moved out;
- b) the housing company manually blocks a user from the service;

- c) the housing company disconnects the property where the user lives from the service;
- d) the housing company terminates the agreement with Avy.

Upon an event/request as above, the following information is archived for one year from the activation of deletion, so that the Supplier can fulfil its service commitment towards the tenants:

- Address
- Contact details (email and telephone)
- Active subscriptions and services signed up for via the housing app.