versie 1.1
datum: 11-04-2025

Data Processing Agreement

1. Your organisation as the client of the Leviy Platform, hereinafter referred to as the "***Data Controller"***

   and,

2. **Leviy B.V.,** a private limited liability company under Dutch law, with its office located at Databankweg 12 H, (3821 AL) Amersfoort, the Netherlands, registered in the Trade Register of the Chamber of Commerce under number 66628547, legally represented here by Michiel Hillebrand, Managing Director, hereinafter referred to as the **"Processor,"**

Collectively hereinafter also referred to as the "**Parties**,"

Considering that:

- The Data Controller is engaged in, among other things, facility management services;
- The Processor is a software company operating within the facility management industry and, in this capacity, processes (special) personal data on behalf of the Data Controller;
- The Data Controller and the Processor have entered into an agreement regarding the provision of services by the Processor to the Data Controller, of which this Data Processing Agreement forms a part;
- The Data Controller is to be considered a data controller within the meaning of Article 4, heading and subsection 7, of the General Data Protection Regulation ("GDPR") with regard to the processing of personal data;
- The Processor is to be considered a data processor within the meaning of Article 4, heading and subsection 8, GDPR, with regard to the storage and processing of personal data on behalf of the Data Controller;
- The Parties, partly to fulfil the requirements of Article 28(3) GDPR, wish to establish in this agreement a number of conditions applicable to their relationship in connection with the processing of personal data in the context of the aforementioned activities for and on behalf of the Data Controller.

Declare that they have agreed as follows:

Article 1 – Definitions

1.1 In this Data Processing Agreement, the following terms, always written with a capital letter, have the following meanings, regardless of whether they are used in the singular or plural:

a. *General Terms and Conditions:* the Processor's general terms and conditions, which form an inseparable part of the Agreement (see website https://www.leviy.com/terms-conditions/?lang=en);

b. *Annex*: an appendix to the Data Processing Agreement, which forms an inseparable part of the Data Processing Agreement;

c. *Data Processing Agreement:* this present agreement, which forms part of the Agreement;

d. *Agreement:* the agreement(s) entered into between the Data Controller and the Processor, to which the Leviy General Terms and Conditions are inseparably linked;

e. *Personal Data:* all data that can be traced directly or indirectly to a natural person, as defined in Article 4, heading and subsection 1, GDPR;

f. *Processing:* the processing of Personal Data, as defined in Article 4, heading and subsection 2, GDPR.

1.2 The provisions of the Agreement shall apply in full to this Data Processing Agreement. Insofar as the Agreement contains provisions regarding the processing of personal data, the provisions of this Data Processing Agreement shall prevail.

Article 2 – Data Controller and Processor of the data

2.1 The Processor undertakes, in the context of this Data Processing Agreement, to process Personal Data on behalf of the Data Controller. The Data Controller and the Processor have entered into this Data Processing Agreement concerning the performance of the Agreement. A summary of the types of Personal Data, the categories of data subjects, and the purposes for which the Personal Data is processed are included in **Annex 1.**

2.2 The Data Controller guarantees that the instruction to process such Personal Data is in accordance with all applicable laws and regulations. The Data Controller indemnifies the Processor against any claims from third parties resulting in any way from non-compliance with this guarantee.

2.3 The Processor undertakes to process Personal Data solely for the activities mentioned in this Data Processing Agreement and/or the Agreement. The Processor guarantees that, without the explicit and written consent of the Data Controller, it will not use the Personal Data processed under this Data Processing Agreement and/or the Agreement in any way, unless a legal provision applicable to the Processor requires it to do so. In such a case, the Processor shall inform the Data Controller of this legal requirement prior to the processing, unless such legislation prohibits this notification for reasons of public interest.

Article 3 – Technical and organisational measures

3.1 The Processor shall implement (or cause to be implemented) appropriate technical and organisational measures to secure Personal Data against loss or any form of unlawful processing and thus ensure a level of security appropriate to the risk. These measures will, taking into account the state of the art and the costs of implementation, guarantee a level of security appropriate to the risks posed by the processing and the nature of the data to be protected. The Processor shall, in any case, take measures to protect Personal Data against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access, and any other form of unlawful processing.

3.2 The technical and organisational measures taken by the Processor are described in **Annex 2**. The Data Controller acknowledges that they are aware of these measures and, by signing this Data Processing Agreement, agrees to the measures taken by the Processor.

Category: Personnel Information

Description	The Processor stores personnel information
Examples	List of names and positions of the Controller's personnel
Purposes	● To carry out activities such as DKS inspections, checklist checks, and work planning, where an activity is linked to staff member(s); ● To log staff members in activities, allowing for analyses at the employee level and enabling employee-focused follow-up.

Category: Personnel Attendance Registration

This consent only applies if the Controller uses the 'Time & Attendance Registration' module from the Processor.

Description	The Processor records the presence and absence of the Controller's employees.
Examples	Location, times, leave, sickness
Purposes	● To enable analyses related to employee attendance; ● To collect information (time) for the Processor's hours registration

Category: Employment Contract Information

This consent only applies if the Controller uses the 'In Service' module from the Processor.

Description	The Processor stores information regarding the Controller's staff employment contracts
Examples	Personal details, bank account information, working hours, references, experiences, evaluations
Purposes	● To enable staff onboarding for the Controller on-site and digitally; ● To allow (new) employees to download employment contracts 3.3 The Processor shall, taking into account the nature of the Processing and as far as reasonably possible, assist the Controller in complying with their obligation under the GDPR to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Article 4 Confidentiality

4.1 The Processor will require all employees involved in executing the Agreement to sign a confidentiality agreement – either incorporated into their employment contract or separately – stating that they must observe confidentiality regarding Personal Data. The Processor will take measures, such as employee screening and securing data carriers, to ensure compliance with this confidentiality obligation.

Article 5 Data Processing Outside the Netherlands

5.1 Transferring Personal Data by the Processor outside the European Economic Area is only permitted in compliance with applicable legal obligations and/or with prior written consent from the Controller.

Article 6 Third Parties and Subcontractors

6.1 The Processor is permitted to use third parties and/or subcontractors ("Sub-processors") in the context of this Data Processing Agreement and the Agreement, as listed in Annex 3. If the Processor wishes to engage other Sub-processors, it will inform the Controller of the intended changes and allow the Controller to object.

6.2 The Processor contractually obliges each Sub-processor to comply with the confidentiality obligations, notification requirements, and security measures related to the Processing of Personal Data, which must meet at least the standards set out in this Data Processing Agreement.

Article 7 Liability

7.1 The Processor indemnifies the Controller only against third-party claims, including fines from the regulator, resulting from the Processor's failure to comply with the security measures laid down in this Data Processing Agreement, unless this non-compliance is not attributable to the Processor.

7.2 If and insofar as the imposition of a fine by the supervisory authority is also attributable to the Controller (for example, because the fine is imposed due to previous privacy breaches by the Controller in which the Processor was not involved and which were taken into account by the supervisory authority when imposing the fine on the Controller), the Processor shall be liable as follows: only for the proportion of the fine amount that corresponds to the part(s) of the fine-causing event(s) that can be attributed to the Processor, provided that the Controller involves or has involved the Processor in relevant contacts and communication with the supervisory authority in such situations.

7.3 The Processor's liability under the Data Processing Agreement, including the indemnification obligations, will be subject to the limitation of liability provisions as stipulated in Article 8 of the General Terms and Conditions of Leviy.

7.4 Notwithstanding Article 7.1 of this Data Processing Agreement, the Processor is only liable for damage caused by Processing if the Processor has failed to comply with obligations specifically directed at it under the GDPR, or has acted outside or contrary to the lawful instructions of the Controller.

Article 8 Security Breach

8.1 If the Processor becomes aware of a breach concerning Personal Data, as defined in the GDPR, or any other security incident, it will:
i) Notify the Controller without undue delay; and
ii) Take all reasonable measures to prevent and/or limit further violations of the GDPR.

8.2 The Processor will reasonably cooperate with the Controller and support the Controller in fulfilling its legal obligations regarding the identified incident.

8.3 The Processor will support the Controller in its obligation to report to the Data Protection Authority and/or the data subject, as set out in Articles 33(3) and 34(1) of the GDPR. The Processor is never required to independently notify the Data Protection Authority and/or the data subject of a breach concerning Personal Data.

8.4 The Processor is never liable for the (correct and/or timely execution of) the Controller's obligation to report breaches as stipulated in Articles 33 and 34 of the GDPR.

Article 9 Assistance to the Controller

9.1 The Processor will assist the Controller, as far as reasonably possible, in fulfilling its obligation under the GDPR to respond to requests for the exercise of a data subject's rights, in particular the right of access (Article 15 GDPR), rectification (Article 16 GDPR), erasure (Article 17 GDPR), restriction (Article 18 GDPR), portability (Article 20 GDPR), and the right to object (Articles 21 and 22 GDPR). The Processor will forward any complaint or request from a data subject regarding the Processing of Personal Data to the Controller as soon as possible, who is responsible for handling the request. The parties will reasonably discuss the allocation of any costs involved.

9.2. The Processor will assist the Controller, as far as reasonably possible, in complying with its obligation under the GDPR to conduct a data protection impact assessment (Articles 35 and 36 GDPR).

9.3. The Processor will provide the Controller with all information necessary to demonstrate that the Processor complies with its obligations under the GDPR. The Processor will also, at the Controller's request, allow audits or inspections by the Controller or an authorised auditor. The Processor is entitled to charge the Controller for any associated costs.

Article 10 Termination & Miscellaneous

10.1 Regarding the termination and/or dissolution of this Data Processing Agreement, the specific provisions of the Agreement apply. Notwithstanding these provisions, the Processor will, upon request from the Controller, delete all Personal Data or return them to the Controller and remove any existing copies, unless the Processor is legally required to retain the Personal Data. The timeline for deletion and removal of copies will be mutually agreed. The costs of returning Personal Data will be borne by the Controller and will be reasonably determined.

10.2 The Controller will adequately inform the Processor about the (legal) retention periods that apply to the Processing of Personal Data. The Processor will not Process Personal Data for longer than these retention periods allow.

10.3 The obligations of this Data Processing Agreement that are intended to survive termination will remain in force even after the termination of this Data Processing Agreement.

10.4 The choice of law and competent court correspond to those stipulated in the Agreement.

Annex 1: Overview of Personal Data Processing

The Controller authorises and instructs the Processor to process the following personal data:

Conditions:

1. The Controller can maintain and set up personal data independently;
2. The Controller will inform individuals for whom a user account is created about the processing of their personal data;
3. The Controller will ensure that users only place personal data in the designated positions in the Leviy application and act in accordance with the instructions given to the Processor;
4. The Controller will ensure that users are instructed on how to place information and (personal) data in the Leviy application and how to handle personal data.
5. Software developers, system administrators, customer managers from the Processor, or subcontractors engaged by the Processor, may have occasional access, strictly on a "need-to-know" basis, to support the technical operation, hosting, (if necessary) development of the application, and service activities.

Category: Contact List

Description	The Processor processes data for the purpose of verifying authorised contacts on behalf of the Controller.
Examples	Email addresses, names, job titles, dates of birth
Purposes	● To verify contacts who communicate with Leviy on behalf of the Controller for data access and/or giving instructions.

Category: Account Data

Description	The Processor processes account data for the creation and management of user accounts in the application, for users at the Controller. To avoid misunderstandings: The Parties agree that the mentioned processing of personal data by the Processor occurs in the capacity of the Controller. The Processor's privacy statement applies to this processing, and the Processor will make the statement available to users within the application itself. The statement can be found here: https://www.leviy.com/privacy-policy/?lang=en
Examples	Email addresses, names, job titles, user groups, and roles
Purposes	● To grant users access and identify them within Leviy; ● To log user activities so they can be analysed; ● The purpose of the job title is to allow the Controller to register the type of users; ● The purpose of user groups is to grant users rights to access information stored within the Leviy application; ● The purpose of roles is to enable users to access specific functionalities within Leviy; ● To send (automated) push notifications to users via an (external) push notification service; ● To send (automated) emails to users via an (external)

	email service.
Category: Device Registration	
Description	The Processor logs which devices users are working within Leviy
Examples	Mobile phones, tablets
Purposes	● To provide insight into the times users logged into the Leviy application with their mobile devices; ● To verify which devices users have logged in on; ● To view the versions of the Leviy application being used; ● To take action in case of issues, such as in the event of a device being lost, allowing for remote logout.
Category: Log Data	
Description	The Processor logs user activities using an external logging service
Examples	When entering, modifying, and deleting information.
Purposes	● To analyse user activities; ● To analyse the causes of bugs; ● To reverse actions that have been performed.
Category: General Purposes	
Description	Processor performs activities for the Controller (upon request).
Description	At the request of employees of the Controller, employees of the Processor may export information from the Leviy application to another format (e.g., PDF or Excel) for alternative use by the Controller.
Purposes	● Supporting the Controller in making information from Leviy available.
● Enabling the digital recording of experiences and evaluations with employees.	

Annex 2 Security Specifications

The security measures taken by the Processor:

- The Processor implements a certified information security management system according to NEN-EN-ISO 27001;
- The Processor has implemented the following measures to raise awareness of information security among all employees:
  a) Establishing a house policy on information security, including:
     i. Policies on the secure handling of customer information;
     ii. Policies on secure workplace and remote working practices;
     iii. Policies on encrypted storage, transportation, or transmission of confidential information;
     iv. Policies to prevent and report information and equipment theft;
     v. Policies on the secure handling of logins and passwords.
  b) Including a confidentiality agreement in employee employment contracts;
  c) Raising awareness of information security when giving presentations, demos, instructions, and distributing manuals to end-users.
  d) Processor actively ensures that employees comply with the information security regulations and provides appropriate consequences in cases of non-compliance.
- Processor has implemented the following measures for physical security:
  a) Data is stored in a secure data centre, certified according to NEN-EN-ISO 27001;
  b) Leviy's server infrastructure is set up as a layered system to secure data;
  c) Processor's computers are cryptographically secured;
  d) An authorisation matrix is in place to regulate employees' access rights within the Processor's organisation;
- Processor follows an information security incident policy, where incidents are logged, and a fixed procedure is followed for reporting;
- Processor has drawn up a privacy statement for users of the Leviy system, which is easily accessible to users.
- To test the information security management system, the Processor conducts both internal and external audits. Internal security audits are conducted annually by specialists. External audits are carried out annually by an accredited organisation (according to the Dutch Accreditation Council).

Annex 3 OVERVIEW OF SUB-PROCESSORS

Processor uses the following sub-processors:

For data hosting:

- True, Keienbergweg 100, 1101 GH Amsterdam.