BUROHELP DATA PROCESSING AGREEMENT (DPA)

Between:
Stichting Burohelp, a Dutch public-benefit foundation (ANBI)
(hereinafter: the **"Controller"**)

and

Processing Partner

Controller and Processors are collectively referred to as the **"Parties"** and individually as a **"Party."**

This Data Processing Agreement forms an integral part of the main service agreement between the Parties.

1. Definitions

- **"GDPR"** means the General Data Protection Regulation (EU 2016/679).
- **"Personal Data"** means any information relating to an identified or identifiable natural person.
- **"Processing"** means any operation performed on Personal Data as defined by the GDPR.
- **"Sub-processor"** means any third party engaged by the Processor to process Personal Data on behalf of the Controller.
- **"Services"** means hosting, IT support, development, analytics, or any other service performed by the Processor for the Controller.
- **"Platform"** means the Burohelp Time Bank and related systems.

2. Subject Matter and Duration

2.1 The Processor shall process Personal Data **only** for the purpose of delivering the Services to the Controller.

2.2 This DPA is valid for the duration of the main service agreement and remains in force until all Personal Data has been deleted or returned to the Controller.

3. Nature and Purpose of Processing

3.1 The Processor processes Personal Data for the following purposes:

- hosting and maintaining the Burohelp platform
- data storage and backups
- authentication & access management
- technical support
- platform optimisation
- logging and security monitoring

3.2 The Processor shall **not** process Personal Data for its own purposes.

3.3 The Processor shall only process Personal Data on documented instructions of the Controller.

4. Types of Personal Data and Categories of Data Subjects

4.1 Types of Personal Data

- Name, email, phone number
- Organisational affiliation
- Login credentials (encrypted)
- Usage logs
- Activity & Time Bank data
- IP address, device information
- Uploaded documents and evidence

4.2 Categories of Data Subjects

- Nonprofit users
- Donor users
- Volunteers
- Employees and administrators
- Board members
- Website visitors

5. Obligations of the Processor

The Processor shall:

5.1 Process Personal Data **solely** on documented instructions from the Controller.

5.2 Ensure that persons authorised to process Personal Data:

- are bound by confidentiality,
- have received proper training.

5.3 Implement appropriate technical and organisational security measures as required under Article 32 GDPR.

5.4 Assist the Controller in fulfilling GDPR obligations, including:

- responding to Data Subject requests,
- conducting DPIAs,
- complying with breach notification obligations.

5.5 Notify the Controller **without undue delay** and within **24 hours** of becoming aware of a data breach.

5.6 Not engage any Sub-processors without prior **written authorisation** from the Controller.

5.7 Not transfer Personal Data outside the EEA without:

- Controller approval, and
- appropriate safeguards (e.g., SCCs).

5.8 Maintain a written record of all processing activities.

5.9 Allow for audits and inspections by the Controller or an independent auditor appointed by the Controller.

5.10 Return or delete all Personal Data upon termination of the Services unless retention is required by law.

6. Sub-Processors

6.1 The Processor may only engage Sub-processors with the prior written consent of the Controller.

6.2 Sub-processors must be bound by written agreements ensuring equal or higher protection of Personal Data.

6.3 The Processor remains fully liable for the actions and omissions of its Sub-processors.

7. Security Measures

The Processor commits to implement security measures including, at minimum:

- data encryption in transit (TLS)
- secure storage and encrypted backups
- access control and role-based permissions
- multi-factor authentication for admin access
- regular patching and maintenance
- logging and monitoring
- intrusion detection measures
- regular vulnerability testing
- separation of environments (dev/test/live)

If the Controller requests additional measures due to risk assessments, the Processor shall implement them where reasonable.

8. Data Subject Rights

The Processor shall promptly forward to the Controller any request received from a Data Subject, including:

- access
- rectification
- erasure
- restriction
- objection
- portability

The Processor shall not respond directly unless instructed.

9. Data Breach Notification

9.1 A “Data Breach” means any event resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to Personal Data.

9.2 Upon discovery of a breach, the Processor shall:

a. notify the Controller immediately (within **24 hours**)
b. include all information necessary for the Controller to comply with Article 33 GDPR
c. cooperate fully in mitigating the impact

10. Confidentiality

10.1 All Personal Data processed under this Agreement shall be treated as strictly confidential.

10.2 The obligation of confidentiality continues indefinitely, including after termination.

11. Return or Deletion of Data

Upon termination of the Services, the Processor shall:

1. return all Personal Data to the Controller; or
2. delete such data entirely, including backups;

unless legal obligations require retention.

Certification of deletion may be requested by the Controller.

12. Liability

Liability is governed by the main service agreement.
However:

- The Processor shall be fully liable for any GDPR violations caused by its breach of this DPA.
- The Processor is liable for Sub-processors’ actions.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by Dutch law.
13.2 Any disputes shall be submitted to the **competent court in the Netherlands**.

14. Amendments

Changes to this DPA must be made **in writing** and approved by both Parties.

15. Entry into Force

This DPA is enforceable and updated