BUROHELP PRIVACY & DATA PROTECTION POLICY

This Policy explains how the Foundation collects, processes, stores, protects, and uses personal data in accordance with the **General Data Protection Regulation (GDPR / AVG)** and Dutch law.

1. Definitions

For the purposes of this Policy:

- **"Foundation"** means Stichting Burohelp, the data controller.
- **"Platform"** means the Burohelp digital infrastructure, including the Time Bank and related systems.
- **"Personal Data"** means any information relating to an identified or identifiable natural person.
- **"Processing"** means any operation performed on personal data, including storage, collection, use, or deletion.
- **"User"** means any natural or legal person using the Platform, including nonprofits, volunteers, donors, and administrators.
- **"Data Subject"** means any individual whose personal data is processed.
- **"Processor"** means any third party processing data on behalf of the Foundation.
- **"DPA"** means a Data Processing Agreement as required under Article 28 GDPR.
- **"DPIA"** means a Data Protection Impact Assessment.

2. Scope of This Policy

This Policy applies to:

- all personal data collected and processed through the Foundation's website, systems, and The Burohelp Time Bank;
- all users, donors, nonprofit partners, employees, board members, and volunteers whose information is processed;
- all processing activities carried out by or on behalf of the Foundation.

This Policy does not apply to anonymised or aggregated data.

3. The Foundation as Controller

3.1 Stichting Burohelp acts as a data **controller** for all personal data processed within the Platform.

3.2 The Foundation is responsible for ensuring that:

- processing is lawful, fair, and transparent;
- data is collected for legitimate purposes;
- data is accurate and kept up to date;
- data is kept secure;
- data subjects can exercise their GDPR rights.

4. Categories of Personal Data Collected

Depending on the user type, the Foundation may collect the following categories:

4.1 Identification & Contact Data

- Full name
- Email address
- Phone number
- Organisation & position
- Postal address (when relevant)

4.2 Account & Authentication Data

- Username
- Password (encrypted)
- Login timestamps
- Access roles and permissions

4.3 Time Bank Activity Data

- Project registrations
- Activity descriptions
- Verified hours
- Time logs
- Approvals and audit trails
- Uploaded evidence (documents, photos)

4.4 Donor Data

- Name and organisation
- Payment information (processed via secure third parties)
- Donation amounts and purpose
- Reporting and communication records

4.5 Technical & Usage Data

- IP address
- Browser information
- Device information
- Cookie preferences
- Platform interaction logs

4.6 Sensitive Data

The Foundation **does not intentionally collect sensitive personal data**, unless strictly necessary and lawful. If sensitive data is processed, explicit consent or a lawful basis is required.

5. Legal Basis for Processing

The Foundation processes personal data on the following bases:

- **Performance of a contract** (Article 6(1)(b) GDPR):
  For users accessing the Platform, managing accounts, verifying hours, and facilitating donations.
- **Legal obligation** (Article 6(1)(c) GDPR):
  ANBI requirements, financial administration, tax rules, security obligations.
- **Legitimate interest** (Article 6(1)(f) GDPR):
  Platform security, data quality checks, fraud prevention, service improvement.
- **Consent** (Article 6(1)(a) GDPR):
  For newsletters, cookies requiring consent, or optional platform features.

6. Purposes of Processing

Personal data is processed to:

1. Manage user accounts and access rights
2. Operate the Burohelp Time Bank
3. Register and verify volunteer and operational hours
4. Match nonprofits with donors and funding
5. Provide impact insights documentation
6. Comply with ANBI financial and transparency obligations
7. Perform security checks and prevent misuse
8. Improve the Platform and user experience
9. Process payments and donations (via processors)
10. Communicate with users and donors
11. Maintain internal records for governance and audits

7. Data Retention

The Foundation retains data only as long as necessary:

Data Category	Retention Period
Account Data	Until account deletion + 2 years
Time Bank Records	7 years (financial/tax justification)
Financial Administration	7 years (legal requirement)
Technical Logs	12 months
Cookies	In accordance with Cookie Policy
Donor Records	7 years (tax requirement)
Emails & Communications	Up to 5 years or as required for audits

Data may be kept longer only if legally necessary or for the establishment, exercise, or defence of legal claims.

8. Sharing Personal Data

Personal data may be shared with:

- IT service providers and hosting providers
- Payment processors
- External auditors
- Donors (only anonymised or consent-based data)
- Nonprofits (only for operational collaboration)
- Supervisory authorities when legally required

Each third party must sign a **DPA** ensuring GDPR compliance.

The Foundation does **not** sell personal data.

9. International Transfers

If personal data is transferred outside the European Economic Area (EEA):

- adequate safeguards must exist (e.g., EU Standard Contractual Clauses);
- transfers require Board approval;
- data subjects will be informed.

10. Security Measures

The Foundation employs technical and organisational measures including:

- encryption of data in transit and at rest
- access control and authentication
- role-based permissions
- secure hosting in the EU
- regular security updates
- audit logs
- staff confidentiality agreements
- periodic backups
- DPIA where required

11. Rights of Data Subjects

Users have the right to:

1. **Access** their personal data
2. **Rectification** of incorrect data
3. **Erasure** (“Right to be forgotten”)
4. **Restriction** of processing
5. **Objection** to processing
6. **Data portability**
7. **Withdraw consent** at any time
8. **File a complaint** with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens)

Requests can be made at:
info@burohelp.com **or** **privacy@burohelp.com**

The Foundation shall respond within **30 days**.

12. Data Protection Officer (If Applicable)

If legally required, the Foundation shall appoint a **Data Protection Officer (DPO)** and publish contact details.

If not required, a Privacy Lead shall be appointed internally.

13. Data Breach Procedure

In the event of a data breach:

1. Immediate containment and assessment
2. Recording the incident in the internal log
3. Notification to the Board within 24 hours
4. Notification to the Dutch Data Protection Authority within 72 hours if required
5. Notification to affected users if high risk is identified
6. Evaluation and remediation plan

14. Updates to This Policy

This Policy may be updated from time to time.
The most recent version shall always be published on the Foundation’s website.