ACORNS data protection and privacy policy

Policy brief & purpose

Our Data Protection and privacy Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

Scope

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company handles this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Processed by the company within its business and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

Actions to Enhance Data Privacy

To exercise data privacy, we're committed to:

1. Data Minimization – Collect only the data you truly need.
2. Consent Management – Obtain explicit consent before collecting or sharing personal data.
3. Privacy Policies – Publish clear policies telling users how their data will be used.
4. Access Controls by Purpose – Limit access to personal data based on job role and purpose.
5. Data Retention Policies – Keep personal data only as long as needed, then delete securely.
6. User Rights Enablement – Allow people to request access, correction, or deletion of their data
7. Data Sharing Agreements – Put contracts in place when sharing data with third parties.
8. Privacy by Design – Build privacy considerations into new systems and processes from the start.

Actions to Enforce Data Protection (Security)

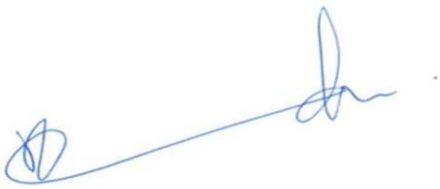
These are technical and operational measures to safeguard data from breaches or misuse:

1. Encryption – Encrypt data at rest (databases, servers) and in transit (emails, HTTPS).
2. Strong Authentication – Use MFA (multi-factor authentication) for system and data access.
3. Firewalls & Intrusion Detection – Block and monitor unauthorized network access.
4. Regular Patching – Keep systems, apps, and devices up-to-date against vulnerabilities.
5. Backup & Disaster Recovery – Maintain secure backups and test recovery processes.
6. Data Masking & Anonymization – Protect sensitive fields when used in reports or testing.
7. Audit Logs & Monitoring – Track who accessed what data and when, and review for anomalies.
8. Training- Train employees in online privacy and security measures

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

Signed



Roselyn Maundu
Founder & CEO