Company: Senbee A/S

Version: 1.0

Effective date: 2026-02-17

Owner: Management (CEO)

Operational responsible: Security / Compliance Lead (or delegated role)

Review frequency: At least annually, and upon material changes to products, processing activities, or applicable requirements.

1. Purpose and goals

Senbee is committed to responsible and transparent use of data. The goals of this policy are to ensure that:

- data is processed fairly, lawfully, and in a way that respects individuals,
- only necessary data is collected and used for clear purposes,
- customers and users can understand how data is used,
- statistics and insights are used responsibly and in a way that avoids harm,
- accountability is maintained through defined roles, implementation measures, and management oversight.

2. Scope

This policy applies to:

- all Senbee employees, contractors, and temporary staff,
- all Senbee products, services, systems, and processes,
- all data handled by Senbee, including personal data and customer-related operational data.

This policy supplements (and does not replace) Senbee's Privacy Policy, Data Processing Agreement, and Information Security Management System.

3. Core principles

Senbee's data ethics principles are:

1. **Purpose limitation and clarity**
   Data is collected and used for defined, legitimate purposes related to delivering and improving the service (e.g. account administration, authentication, communication, security, support, and service-related analytics).

2. **Data minimisation**
   Senbee collects and retains the minimum amount of data required for the stated purposes.
3. **Transparency**
   Senbee aims to explain in clear terms what data is processed, why, and how it is protected.
4. **Fairness and avoidance of harm**
   Senbee avoids using data in ways that could lead to unjustified discrimination, manipulation, or harm to individuals. Where statistics are used, Senbee prioritises aggregated insights and avoids unnecessary individual-level profiling.
5. **Customer control and confidentiality**
   Customer data is treated as confidential and is not sold. Senbee uses customer data only as required to provide the service and fulfil contractual obligations.
6. **Security by design**
   Data is protected through appropriate technical and organisational measures, aligned with Senbee's security policies and management system.
7. **Retention and deletion discipline**
   Data is not kept "just in case." Retention is defined and data is deleted or anonymised when no longer needed, subject to contractual and legal requirements.

4. Roles and responsibilities

- **Management (CEO)** is accountable for this policy, approves it, and ensures adequate resources and prioritisation.
- **Security / Compliance Lead (or equivalent role)** is responsible for maintaining the policy, supporting implementation, and reporting status to management.
- **Product and Engineering** are responsible for implementing the policy through product design, system configuration, access controls, logging, and secure development practices.
- **All employees and contractors** must follow this policy and complete relevant training/briefings.

5. Implementation (how the policy is put into practice)

Senbee implements this policy through the following measures:

- maintaining a high-level mapping of personal data processed (categories, purposes, systems, recipients, retention),
- performing risk assessments for new features and changes that impact data use (including security and privacy considerations),
- applying access control and least privilege to systems containing personal data,
- documenting and approving sub-processors and third-party services that may process data,

- using statistics primarily in aggregated form and limiting individual-level analysis to what is necessary for service delivery, security, and support,
- maintaining customer-facing documentation (e.g. Trust Center materials) that supports transparency.

6. Follow-up, measurement, and continuous improvement

Senbee monitors adherence to this policy through:

- periodic internal reviews (at least annually),
- reviews triggered by major product or processing changes,
- handling and lessons learned from incidents, complaints, or audit findings,
- review of sub-processor changes and related risk assessments.

7. Reporting to management

The Security / Compliance Lead reports to management at least annually (and as needed) on:

- status of the personal data mapping and notable changes,
- data ethics and privacy-related risks identified in product changes,
- notable incidents or suspected violations relating to personal data use,
- third-party/sub-processor changes relevant to data handling,
- recommended actions and improvements.

Management reviews the report, prioritises actions, and documents decisions and follow-up as appropriate.

8. Exceptions and violations

Any exception to this policy must be justified, documented, and approved by management. Suspected violations must be reported internally and will be handled according to Senbee's internal processes.

9. Contact

Questions about this policy can be directed to Senbee management or the responsible security/compliance function.