SENSEVEN

Data Processing, Data Protection and Security

1. Controller Information and Contact Details

The controller within the meaning of Art. 4(7) of the General Data Protection Regulation (GDPR) for the data processing activities described in this Privacy Notice is:

Senseven GmbH
Montleartstraße 1b/7/14
1140 Vienna
Austria
Email: office@senseven.ai

This Privacy Notice applies to the use of the Senseven Software, including:

- The mobile application installed on the smartphone (the “Senseven App”)
- The cloud-hosted platform for data storage, processing, and reporting (the “Senseven Backoffice”)
- Associated cloud services, APIs, and support systems

If you have any questions regarding this Privacy Notice or the processing of personal data, you may contact Senseven at the address provided above.

2. Roles of the Parties (Controller and Processor)

The Senseven Software is designed for use by companies and organizations (“Customers”) in the course of their business activities.

Depending on the context of the processing activity, Senseven may act either as a data processor or as an independent controller under the GDPR.

2.1. Processing on behalf of Customers (Senseven as Processor)

When Customers upload, store, manage, or analyze data within the Senseven Software, the Customer acts as the controller within the meaning of Art. 4(7) GDPR.

Senseven processes such data solely on behalf of the Customer in order to provide and operate the Senseven Software.

This includes, for example:

- inspection records and measurement data
- uploaded documents, photographs, and reports
- notes and other operational information entered by users

Customer Responsibility for Uploaded Data
The Customer is responsible for ensuring that any personal data uploaded or entered into the Senseven

Software has been collected and processed in accordance with applicable data protection laws. The Customer shall ensure that no unnecessary or unlawful personal data is included in inspection records, reports, notes, or uploaded content.

The details of this processing relationship are governed by a Data Processing Agreement (DPA) in accordance with Art. 28 GDPR.

2.2. Processing for Senseven's Own Purposes (Senseven as Controller)

Senseven also processes certain personal data as an independent controller where this is necessary to operate the service and manage the contractual relationship with Customers.

This may include processing related to:

- creation and management of user accounts
- customer communication and support
- system security and fraud prevention
- billing and contractual administration
- compliance with legal obligations

Such processing is carried out on the applicable legal bases under Art. 6 GDPR.

3. Categories of Data Subjects

Depending on how the Senseven Software is used, the processing of personal data may relate to the following categories of data subjects:

Authorized Users
Individuals who are authorized by a Customer to access and use the Senseven Software. This may include employees, inspectors, technicians, administrators, or contractors who use the Senseven mobile application or the Backoffice platform as part of their professional activities.

Customer Representatives
Individuals acting as contact persons for the Customer in connection with the contractual relationship with Senseven. This may include administrative contacts, technical contacts, or billing contacts involved in the management of the service.

Support Contacts
Individuals who communicate with Senseven in connection with support requests, technical assistance, or service inquiries.

Individuals Referenced in Customer-Generated Content
In limited cases, information uploaded by Customers (such as inspection notes, reports, or attachments) may contain references to individuals. The Customer remains responsible for ensuring the lawful collection and processing of such information.

4. Categories of Personal Data Processed

Depending on how the Senseven Software is used, the following categories of personal data may be processed.

Senseven primarily processes technical inspection data uploaded by Customers during industrial inspections. Such data generally relates to industrial equipment and typically does not constitute

personal data unless it is combined with information identifying an individual. Personal data processed by Senseven is therefore generally limited to account information required to operate the service and related system data.

Account and Identity Data
Information required to create and manage user accounts for the Senseven Software and Backoffice platform. This may include the user's name, business email address, company or organizational affiliation, user role, and password.

Contact and Communication Data
Information related to communication between Customers and Senseven, such as contact details of customer representatives, email correspondence, and information contained in support requests or service inquiries.

Usage and Log Data
Technical information generated during the use of the Senseven Software, including login timestamps, user actions within the system, system event logs, IP addresses. This information is processed primarily for system security, troubleshooting, and maintaining reliable operation of the service.

Device and Technical Information
Information relating to the inspection devices used to access the Senseven Software, such as device identifiers (e.g., IMEI or serial number), Senseven App version and system information (Android version) and network-related information. This data is used to ensure compatibility, security, and proper functioning of the software.

Media and Uploaded Content
Content uploaded by users through the software during inspections or reporting activities, including photographs. The Customer is responsible for ensuring that such uploads comply with applicable data protection laws.

Billing and Contractual Data
Information required to manage the contractual relationship between Senseven and the Customer, such as company name, billing address, tax identification numbers, and invoicing or payment information.

5. Requirement to provide Personal data

Certain personal data such as name, email address, and company is required to create and manage user accounts and to provide access to the Senseven Software. If such information is not provided, the use of the software may not be possible.

6. Purposes of processing and legal basis

Senseven processes personal data only to the extent necessary to provide and operate the Senseven Software and related services. The processing activities and their legal bases under the GDPR are summarized below:

Purpose of Processing	Description	Categories of Data	Legal Basis
Provision of the Senseven Software	Operation of the mobile app, Backoffice platform, and related cloud services, including user account management and system access	Account data, usage data, device data	Art. 6(1)(b) GDPR – performance of a contract
Management of user accounts	Creation, administration, and maintenance of user accounts and roles within the system	Account data, contact data	Art. 6(1)(b) GDPR – performance of a contract
Inspection and operational functionality	Processing of inspection records, sensor data, uploaded content, and reports generated by users	Inspection data, media uploads, metadata	Art. 6(1)(b) GDPR – performance of a contract
Synchronization and system functionality	Synchronization of data between mobile devices, cloud infrastructure, and the Backoffice platform	Usage data, device data, inspection data	Art. 6(1)(b) GDPR – performance of a contract
Customer communication and support	Responding to support requests, troubleshooting technical issues, and communicating with customer representatives	Contact data, communication data, log data	Art. 6(1)(b) GDPR – performance of a contract
System security and abuse prevention	Monitoring system activity, detecting security incidents, preventing unauthorized access, and maintaining platform integrity	Log data, IP addresses, device data	Art. 6(1)(f) GDPR – legitimate interest in ensuring system security
Troubleshooting and service improvement	Analysis of system errors, debugging, and maintaining reliable operation of the platform	Log data, device data, usage data	Art. 6(1)(f) GDPR – legitimate interest in maintaining reliable services
Contract management and billing	Managing contractual relationships, invoicing, payment processing, and accounting	Billing data, contact data	Art. 6(1)(b) GDPR – performance of a contract
Compliance with legal obligations	Compliance with statutory obligations such as tax laws, accounting requirements, or regulatory reporting	Billing data, contractual data	Art. 6(1)(c) GDPR – legal obligation

7. Recipients of Personal Data

Senseven may disclose or make personal data accessible to certain recipients where necessary for the operation of the Senseven Software and the provision of related services.

Recipients may include the following categories:

Recipient Category	Purpose
Cloud infrastructure providers	Hosting of the Senseven platform, databases, and application infrastructure
IT and infrastructure service providers	Provision of system monitoring, logging, and operational support services
Communication service providers	Delivery of email notifications, system alerts, and support communications
Payment and billing service providers	Processing of invoices and payments where applicable
Professional advisors	Legal, tax, or accounting advisors where necessary for compliance with legal obligations

All recipients are contractually required to process personal data in accordance with applicable data protection laws.

Where recipients act as data processors, they process personal data solely on behalf of Senseven and under appropriate contractual safeguards.

8. Subprocessors

In order to operate the Senseven Software, Senseven may engage third-party service providers acting as subprocessors who process personal data on behalf of Senseven.

The Senseven subprocessors are:

Subprocessor	Service	Location*
Amazon Web Services (AWS)	Cloud hosting and managed infrastructure services	Europe (Frankfurt)
Cloudflare	Network infrastructure and DDoS protection	Global
Sentry (Functional Software Inc.)	Application monitoring and error tracking	Europe
Mixpanel Inc.	Product analytics and usage insights	Europe
SOTI Inc.	Mobile device management (SOTI MobiControl Cloud)	Europe (Frankfurt)

*For customer specific projects, these locations can change on customer request

Senseven ensures that all subprocessors are bound by data processing agreements in accordance with Article 28 GDPR and are required to implement appropriate technical and organizational security measures. Senseven may update the list of subprocessors from time to time. Customers will be informed of material changes where required by applicable agreements.

SENSEVEN

9. International Data Transfers

Personal data processed in connection with the Senseven Software is generally stored and processed within the European Economic Area (EEA).

All customer data is stored and processed within the EEA. Only Cloudflare, as a global network provider, may route encrypted traffic through locations outside the EEA. In such cases, Senseven ensures that appropriate safeguards are implemented to protect personal data in accordance with Chapter V of the General Data Protection Regulation (GDPR).

Such safeguards may include:

- the use of Standard Contractual Clauses (SCCs) approved by the European Commission
- reliance on an adequacy decision issued by the European Commission
- additional contractual, technical, or organizational safeguards where appropriate

These measures are intended to ensure that personal data transferred outside the EEA remains protected at a level consistent with the requirements of the GDPR.

10. Data Retention and Deletion

Senseven retains personal data only for as long as necessary to fulfill the purposes described in this Privacy Notice, to provide the Senseven Software, and to comply with applicable legal obligations.

Retention periods may vary depending on the category of data and the context in which it was collected. The general retention periods applied by Senseven are summarized below:

Data Category	Retention Period
User account data	Retained for the duration of the customer relationship and deleted or anonymized after account termination unless legal obligations require longer retention
Inspection and operational data	Retained for the duration of the customer contract and controlled by the Customer as the data controller
Usage and system logs	Typically retained for a limited period necessary for security monitoring and troubleshooting
Support communications	Retained for the duration necessary to resolve support requests and maintain service records
Billing and contractual data	Retained for the duration required by applicable accounting and tax laws
Backup data	Stored in secure backup systems with a rolling retention period of 30 days

Upon termination of the contractual relationship, Customers may request the export or deletion of their data in accordance with the applicable contractual agreements.

Senseven implements appropriate procedures to ensure that personal data is securely deleted or anonymized once the applicable retention period has expired, unless further retention is required by law.

11. Technical and Organizational Security Measures

Senseven implements appropriate technical and organizational measures to protect personal data against unauthorized access, loss, alteration, or disclosure in accordance with Art. 32 GDPR.

These measures are designed to ensure the confidentiality, integrity, availability, and resilience of the systems used to process personal data.

Security measures implemented by Senseven include, among others:

- Encryption of data in transit using industry-standard security protocols (https, TLS)
- Access control mechanisms ensuring that only authorized personnel can access systems containing personal data
- Role-based access management and authentication procedures
- Access to systems is restricted through unique user identifiers and authentication mechanisms to detect and prevent unauthorized access or misuse
- Servers have individual user IDs
- Data backup and disaster recovery procedures to ensure system availability and resilience
- Encryption of data at rest in the cloud (AWS S3, RDS)
- Multi factor authentication for all administrative accounts
- Central device management with remote wipe (SOTI MobiControl)
- Continuous monitoring of availability and traffic, and automated scanning of code dependencies for vulnerabilities

Access to personal data is restricted to authorized personnel who require such access to perform their duties and who are bound by appropriate confidentiality obligations.

Senseven regularly reviews and updates its security measures to address evolving security risks and technological developments.

12. Rights of Data Subjects

Individuals whose personal data is processed in connection with the Senseven Software may have certain rights under applicable data protection laws, including the General Data Protection Regulation (GDPR). These rights may include:

- **Right of access:** to obtain confirmation as to whether personal data concerning them is being processed and to access such data
- **Right to rectification:** to request the correction of inaccurate or incomplete personal data
- **Right to erasure:** to request the deletion of personal data under certain conditions
- **Right to restriction of processing:** to request that the processing of personal data be limited under certain circumstances

- **Right to data portability:** to receive personal data in a structured, commonly used, and machine-readable format where applicable
- **Right to object:** to object to the processing of personal data where processing is based on legitimate interests
- **Right to lodge a complaint:** to file a complaint with a competent data protection supervisory authority Individuals also have the right to lodge a complaint with a data protection supervisory authority, in particular in the Member State of their habitual residence, place of work, or the place of the alleged infringement, if they believe that the processing of their personal data violates applicable data protection laws.

Where Senseven processes personal data on behalf of a Customer acting as the controller, requests relating to the exercise of data subject rights should generally be directed to the respective Customer. Senseven will assist Customers in responding to such requests where required under applicable data protection laws or contractual agreements.

Where Senseven acts as the controller of personal data, individuals may contact Senseven using the contact details provided in Section 1 to exercise their rights.

Senseven may take appropriate steps to verify the identity of the requesting individual before responding to such requests.

13 . Automated Decision-Making and Profiling

The Senseven Software does not involve automated decision-making or profiling within the meaning of Art. 22 GDPR.

14. Changes to this notice

Senseven may update this Privacy Notice from time to time. The latest version will be made available through the Senseven Software or the company website.