Privacy Policy – contexxt.ai Technologies GmbH (Sesame Platform)

Version: August 7, 2025

1. Data Controller

contexxt.ai Technologies GmbH
Campus, Building A1.1
66123 Saarbrücken, Germany
Email: datenschutz@contexxt.ai
Phone: +49 681 93784033

2. General Information on Data Processing

We process your personal data in accordance with the EU General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG).

Personal data includes all information that relates to an identified or identifiable natural person, such as name, email address, or IP address.

3. Purposes and Legal Bases of Processing

Purpose of Processing	**Legal Basis**
Operation and security of the website	Art. 6 Abs. 1 lit. f DSGVO
Contact and support requests	Art. 6 Abs. 1 lit. b oder f DSGVO
Contract performance via “Sesame”	Art. 6 Abs. 1 lit. b DSGVO
Payment processing with Stripe	Art. 6 Abs. 1 lit. b DSGVO
Error logging & system analysis	Art. 6 Abs. 1 lit. f DSGVO
Consent-based services (e.g., cookies, newsletter)	Art. 6 Abs. 1 lit. a DSGVO

4. Data Processing via Stripe

We use Stripe (Stripe Payments Europe Ltd., Ireland) for payment processing. Personal data such as name, email, address, payment data, and IP address are processed.

More information: https://stripe.com/privacy
Data Processing Agreement with Stripe: https://stripe.com/legal/dpa

5. Data Processing in the “Sesame” SaaS Platform

User-entered content (e.g., documents, text) is processed on servers located in France, Germany, or Finland (OVH Cloud Germany or GROQ).

Purpose: analysis, search, and storage. No processing takes place outside the EU.

A GDPR-compliant Data Processing Agreement (DPA) is available to business customers upon request.

6. Cookies and Tracking

We use technically necessary cookies. Tracking and analytics cookies (e.g., via HubSpot) are used only with your explicit consent.

7. Your Data Protection Rights

You have the right to access, rectification, erasure, restriction, objection, and data portability.

Contact: datenschutz@contexxt.ai
Supervisory authority in Saarland: https://www.datenschutz.saarland.de/

8. Recipients and Data Transfers to Third Countries

Data is only shared where legally permitted or based on your consent. Transfers to third countries occur only with appropriate safeguards.

Marketing tools used:
- HubSpot (USA, SCCs & DPA signed): https://legal.hubspot.com/privacy-policy
- HeyReach (Estonia): https://www.heyreach.com/privacy-policy

9. Data Retention

Data is stored only as long as necessary or legally required (e.g., 10 years for invoice data).

Marketing data: up to 24 months of inactivity.

10. Technical and Organizational Measures (TOMs)

We implement appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of your data – in particular in accordance with Art. 32 GDPR.

Some of these measures are provided by our infrastructure partners. These include:

• Hosting Infrastructure by OVHcloud

We use OVH Cloud Germany, with servers located exclusively in France, Germany, and Finland. According to its data protection commitments, OVH ensures that data remains within the EU, is not processed for purposes other than the contractual agreement, and is processed within the scope of a Data Processing Agreement (DPA). OVH also provides extensive certifications and security information in accordance with Art. 32 GDPR.
Source: https://us.ovhcloud.com/legal/data-processing-agreement

• OVH Data Protection Guarantees:

- OVH processes customer data strictly on customer instructions and does not use it otherwise.
- They provide data reversibility (export/portability) and transparent documentation of security practices.
- A Data Processing Agreement (DPA) covering Art. 28 GDPR is available on request.
- Hosting infrastructure includes widely recognized standards – CVE patching, ISO 27001, PCI DSS, SOC 1 & 2 – and strict EU data residency.

Further technical and organizational measures are implemented by us within the SaaS platform Sesame:

1. Physical Access Control

Responsible: OVHcloud

- Access to data centers only for authorized personnel
- 24/7 surveillance, access logging and controlled entry systems
- Infrastructure is located exclusively within the EU
  (See more on OVH's data center security:
  https://www.ovhcloud.com/de/personal-data-protection/)

2. Logical / IT Access Control

Responsible: contexxt.ai / Sesame

- User accounts with individual login credentials
- Password policies (minimum length, expiration, complexity)
- Two-Factor Authentication (2FA)
- Encrypted access to administrative interfaces (HTTPS, VPN)

3. Access Control (Data & System Level)

Responsible: contexxt.ai / Sesame

- Role-based access with minimum privileges ("need-to-know" principle)
- Granular permission system for data and system access
- Logging of all administrative actions

4. Transfer Control (Data Transmission)

Responsible: contexxt.ai / Sesame

- TLS/HTTPS encryption for all external communication
- API access secured via token-based authentication (e.g., OAuth2)
- Encrypted email transmission via TLS

5. Input Control

Responsible: contexxt.ai / Sesame / OVHcloud

- Logging of relevant user actions (e.g., login, upload)
- Version history and audit trails
- Tamper-proof logs to prevent manipulation

6. Processor Control

Responsible: contexxt.ai / Sesame

- Data Processing Agreements with all subprocessors (e.g., OVHcloud, Stripe, HubSpot)
- Documentation and risk assessment of all external vendors
- Regular review of legal and data protection compliance

7. Availability Control

Responsible: OVHcloud, contexxt.ai / Sesame

- Redundant infrastructure and uninterruptible power supply
- Daily encrypted backups
- Disaster recovery plans and 24/7 system monitoring

8. Separation Control

Responsible: contexxt.ai / Sesame

- Logical separation of all tenants (Tenant ID, namespace)
- Dedicated database segments or isolated instances
- No unauthorized cross-access between customer environments

9. Data Protection by Design & by Default

Responsible: contexxt.ai / Sesame

- Principles of data minimization and purpose limitation
- Configurable data retention and auto-deletion options
- No default logging of user inputs containing personal data

10. Auditing & Internal Compliance Measures

- Documented IT security and data protection concepts
- Regular penetration testing and vulnerability scans
- Mandatory data protection training for staff
- Internal review process for all TOMs and vendor controls

11. Changes to this Privacy Policy

This privacy policy is regularly updated. The current version can be found at:
https://contexxt.ai/privacy-policy-en

An English translation is available for informational purposes. In the event of discrepancies, the German version is legally binding.