LECS Encryption System (Live Encrypted Cloud Storage)

Overview of the encryption architecture, data storage, tenant separation, and compliance in connection with the new cloud storage

1. Overview

LECS (Live Encrypted Cloud Storage) is Noxtua's encryption system, which protects all data processed on the platform through project-based encryption using individual cryptographic keys.
Each project, for example each chat, is cryptographically isolated. In the unlikely event that an access key is compromised, any unauthorized access can affect at most a single project (e.g. an individual chat).
This document describes how LECS works technically and the organizational framework for data storage, key control, and record-keeping.

2. System Architecture

LECS consists of two interacting subsystems:

2.1 Key Management

Key management is based on three components:

Encrypted Keyring: Stored on the Noxtua backend, the keyring contains the project-specific keys for all projects to which the user has access. The keyring is encrypted with the user's personal unlock key. At no point does the backend have access to the decrypted keyring.

Unlock Key: An individual key for each user used to decrypt the keyring. The unlock key is never stored on or transmitted to the Noxtua backend. The keyring is decrypted exclusively in the user's browser.

Unlock Key Vault: A separate, hardened service whose sole task is the secure storage and release of unlock keys. Access requires valid authentication via the Noxtua IDP and, where applicable, the IDP of the respective tenant (dual-IDP authentication).

2.2 Encrypted Storage

Encrypted storage is based on two components:

Encryption Layer: Sits between the application logic and the object storage. Project keys are provided to the encryption layer solely for the duration of a single operation and are deleted immediately afterwards (key provisioning).

hello@noxtua.com
www.noxtua.com
linkedin.com/company/noxtua
+49 162 2577678

Noxtua AG
Grosse Hamburger
Strasse 17
10115 Berlin, Germany

Berlin, Germany
Amtsgericht Charlottenburg
HRB 202784 B
USt-ID: DE311 315 441

Sitz der Gesellschaft: Berlin
Vorstand: Dr. Leif-Nissen Lundbæk
(Vorsitzender)
Aufsichtsratsvorsitzender: Dr. Roland Klaes

Object Storage: Stores all project content in a file-system-like structure, grouped by project. All sensitive content is encrypted before being handed over to storage; the storage itself sees only ciphertext.

3. Encryption Details

3.1 Cryptographic Parameters

Parameter	Value
Key type	Symmetric
Algorithm	XChaCha20-Poly1305
Key length	256-bit
Tag size	128 Bit
Nonce size	192 Bit
Key generation	CSPRNG (cryptographically secure random number generator)
Nonce generation	Random per encryption operation (CSPRNG)

3.2 Authenticated Encryption (AEAD)

Each encrypted record is bound to its context by Additional Authenticated Data (AD).
The AD comprises:

- A fixed context string
- Protocol version
- Tenant ID, user ID, project ID, and file ID

As a result, a ciphertext can only be decrypted successfully in the exact context in which it was created; any mismatch causes the integrity check to fail.

4. Scope of Encryption

4.1 Encrypted Data

All sensitive content is encrypted, including chat messages, uploaded files, AI-generated responses, and potentially sensitive metadata such as file names.

4.2 Unencrypted Metadata

The following technical metadata is stored in plaintext because it is required for the operation of the system:

- Access patterns (which user accesses which file and when)
- File size and randomly generated IDs
- Structural path prefixes (e.g. /user-uploads)

This metadata contains no content-related or personal data and no information about the customer's clients. It is evaluated exclusively for operational purposes (routing, storage management, internal resource accounting) and is subject to the same limits as the encrypted content.

5. Data Storage and Data Processing

Noxtua's data storage is designed to meet the requirements of European law firms and legal departments and provides full transparency regarding location, processing, and contractual basis.

5.1 Location of Data Processing and Storage

All customer data, whether encrypted content or operational metadata, is processed and stored exclusively in data centers within Germany and Switzerland. No transfer outside Germany and Switzerland takes place.

5.2 Sub-Processors

Noxtua maintains a complete, up-to-date list of all sub-processors used. The list includes the provider, the purpose of processing, and the place of processing, and is made available to customers on request. Each sub-processor is contractually bound in accordance with Article 28 GDPR.

Changes to the group of sub-processors are announced to customers with reasonable advance notice. This does not affect any agreed rights of objection.

5.3 Processing on Behalf of the Controller

For the processing of personal data, a data processing agreement (DPA) pursuant to Article 28 GDPR is concluded. In the case of partner products (e.g. Beck-Noxtua, MANZ-Noxtua, Swiss-Noxtua), it is entered into between the respective publisher and the customer, and separately between the publisher (as controller) and Noxtua (as processor). For direct customers, Noxtua concludes the DPA directly with the customer. In particular, the DPA governs the subject matter and duration of the processing, its nature and purpose, the categories of data subjects concerned, and the technical and organizational measures (TOMs).

5.4 Retention Period

Two options are available for the retention period of content stored in the cloud. They use the same storage and encryption architecture and differ solely in the retention period. By default, an unlimited retention period is active; an eight-hour retention period is set up only at the customer's express request.

Unlimited retention (default): Chats are stored permanently. This option enables continuous access to past content, an uninterrupted chat history, and the use of features that access data stored in the cloud. In addition, chats can be manually deleted by the user at any time. At the end of the contract, all data is automatically and irretrievably deleted.

hello@noxtua.com
www.noxtua.com
linkedin.com/company/noxtua
+49 162 2577678

Noxtua AG
Grosse Hamburger
Strasse 17
10115 Berlin, Germany

Berlin, Germany
Amtsgericht Charlottenburg
HRB 202784 B
USt-ID: DE311 315 441

Sitz der Gesellschaft: Berlin
Vorstand: Dr. Leif-Nissen Lundbæk
(Vorsitzender)
Aufsichtsratsvorsitzender: Dr. Roland Klaes

Eight-hour retention (on request): Chats are automatically deleted cryptographically eight hours after the last interaction. Once this period has elapsed, the content concerned can no longer be accessed. This option is suitable for customers with restrictive data retention requirements. Please note, however, that due to the shorter retention period, future features within the Noxtua application will be unavailable or only available to a limited extent.

In both options, content is encrypted per project with XChaCha20-Poly1305 (256-bit); the principle of data minimization is maintained. Individual chats can be deleted by users at any time, regardless of the chosen retention period.

6. Tenant Separation

LECS implements a two-level separation of tenants:

Organizational separation: Projects are assigned to users, who in turn are assigned to tenants. This hierarchy is reflected in the storage structure.

Cryptographic separation: Each project has its own encryption key. Even in the event of a software error or malicious access to the storage, data belonging to other projects cannot be decrypted.

6.1 Blast Radius in the Event of Key Compromise

The maximum area of impact (blast radius) of a compromised project key is limited to exactly one project. Because each project key is generated independently and is accessible only via the user-specific keyring, the following containment results:

- A compromised project key affects only the data of a single project (such as an individual chat) and not the tenant, not the user, and not other projects.
- A compromised unlock key affects at most the projects of a single user, since other users use their own unlock keys.
- Interference with the object storage alone, without access to the associated keys, results in no disclosure of plaintext whatsoever.

7. Key Control and Access Model

The cryptographic and operational architecture of LECS is designed so that Noxtua itself has no permanent access to plaintext data.

This section describes the organizational and legal consequences of this architecture.

7.1 Key Holders

Effective control over the keys lies with the user and therefore with the customer:

- Unlock Key: Never stored on the Noxtua backend. The keyring is decrypted exclusively in the user's browser.
- Keyring: Stored on the backend only in a form encrypted with the unlock key.
- Project keys: Provided to the encryption layer solely for the duration of a single operation and deleted immediately afterwards.

hello@noxtua.com
www.noxtua.com
linkedin.com/company/noxtua
+49 162 2577678

Noxtua AG
Grosse Hamburger
Strasse 17
10115 Berlin, Germany

Berlin, Germany
Amtsgericht Charlottenburg
HRB 202784 B
USt-ID: DE311 315 441

Sitz der Gesellschaft: Berlin
Vorstand: Dr. Leif-Nissen Lundbæk
(Vorsitzender)
Aufsichtsratsvorsitzender: Dr. Roland Klaes

7.2 Access to Plaintext Data

The LECS storage architecture ensures that Noxtua never has permanent access to plaintext data. Plaintext exists exclusively:

- in the browser of the authenticated user, and
- transiently in the memory of the backend agent while a single request is being processed.

Administrative roles at Noxtua have no technical path by which to view project-related plaintext data without active user authentication. This is safeguarded by dual-IDP authentication and the strict separation between the Unlock Key Vault and the application backend.

7.3 Deletion at End of Contract

Upon termination of the contractual relationship, all customer data is deleted through a defined procedure:

- Cryptographic deletion: The project-specific keys are irretrievably destroyed. As a result, the associated ciphertexts can no longer be decrypted, even if the storage is accessed at a later time.
- Physical deletion: Subsequently, the encrypted content and the associated metadata are removed from the production systems.
- Backups: Any residual data in backups is overwritten or destroyed within the contractually agreed backup retention period.
- Confirmation: Customers receive confirmation of deletion on request.

It can be agreed that data will be returned before the end of the contract in a readable format provided by Noxtua.

8. Data Access Lifetime

Component	Key and data lifetime
Browser (client)	Discards content, keys, and tokens on logout or project deletion
Backend (agent)	Discards all keys and content immediately after completing the respective request
LECS service	Acts solely as a pass-through service; does not persist any keys

9. Evidence, Certifications, and Audit Logs

The measures implemented in LECS are backed by external certifications and internal evidence processes.

9.1 Certifications and Standards

Noxtua aligns its information security and compliance framework with the following standards and laws:

- ISO/IEC 27001: Information Security Management System (ISMS); certified or certification in progress, depending on current status. The security team confirms the relevant status to customers on request.

- BSI C5: Alignment of the cloud-specific controls with the Cloud Computing Compliance Criteria Catalogue of the German Federal Office for Information Security (BSI). Attestations are made available to customers under NDA as soon as they are available.
- SOC 2: Reporting on the Trust Services Criteria of Security, Availability, and Confidentiality; current status on request.
- GDPR / BDSG: Processing in accordance with Article 28 GDPR; implementation of the requirements of Section 203 of the German Criminal Code (StGB) and Section 43e of the Federal Lawyers' Act (BRAO) during customer onboarding.

Current certificate copies, SOC reports, and C5 attestations are provided on request.

9.2 Audit Logs

All security-relevant events are recorded in tamper-protected audit logs. In particular, the following are recorded:

- Authentication and authorization events (including dual-IDP operations)
- Access to the Unlock Key Vault
- Creation, modification, and deletion of projects and keys
- Administrative access to systems in the processing environment

Audit logs are retained in a tamper-protected manner for a defined period and are evaluated in the course of internal and external audits. Customers receive extracts of the events concerning them on request.

9.3 Plaintext Metadata and Its Handling

As described in Section 4.2, a strictly limited amount of operational metadata remains in plaintext. This metadata:

- contains no personal data and no information about the customer's clients,
- is subject to the same limits and access controls as encrypted content,
- is also monitored via the audit-log mechanisms.

This ensures that encrypted technical metadata cannot be used for content-based profiling of the communication between a person bound by professional confidentiality and their clients.

hello@noxtua.com
www.noxtua.com
linkedin.com/company/noxtua
+49 162 2577678

Noxtua AG
Grosse Hamburger
Strasse 17
10115 Berlin, Germany

Berlin, Germany
Amtsgericht Charlottenburg
HRB 202784 B
USt-ID: DE311 315 441

Sitz der Gesellschaft: Berlin
Vorstand: Dr. Leif-Nissen Lundbæk
(Vorsitzender)
Aufsichtsratsvorsitzender: Dr. Roland Klaes