LECS (Layered Encryption & Compartment Storage)

Verschlüsselungsarchitektur, Datenhaltung, Mandantentrennung und Compliance mit der Cloud-Speicherung

1. Übersicht

LECS (Layered Encryption & Compartment Storage) ist das Verschlüsselungssystem von Noxtua, das alle in der Plattform verarbeiteten Daten durch projektbasierte Verschlüsselung mit individuellen kryptographischen Schlüsseln schützt.

Jedes Projekt – beispielsweise jeder Chat – wird kryptographisch isoliert. Ein kompromittierter Schlüssel betrifft ausschließlich ein einzelnes Projekt. Noxtua selbst hat zu keinem Zeitpunkt dauerhaften Zugriff auf Klartextdaten.

Dieses Dokument beschreibt die technische Funktionsweise von LECS und die organisatorischen Rahmenbedingungen zu Datenhaltung, Schlüsselkontrolle und Nachweisführung.

2. Systemarchitektur

LECS besteht aus zwei Teilsystemen, die zusammenwirken:

2.1 Schlüsselmanagement (Key Management)

Das Schlüsselmanagement basiert auf drei Komponenten:

Verschlüsselter Schlüsselbund (Encrypted Keyring): Wird auf dem Noxtua-Backend gespeichert und enthält die projektspezifischen Schlüssel aller Projekte, auf die der Nutzer Zugriff hat. Der Schlüsselbund ist mit dem persönlichen Unlock Key des Nutzers verschlüsselt. Das Backend hat zu keinem Zeitpunkt Zugriff auf den entschlüsselten Schlüsselbund.

Unlock Key: Ein individueller Schlüssel pro Nutzer, der zur Entschlüsselung des Schlüsselbunds dient. Der Unlock Key wird niemals auf dem Noxtua-Backend gespeichert oder dorthin übertragen. Die Entschlüsselung des Schlüsselbunds erfolgt ausschließlich im Browser des Nutzers.

Unlock Key Vault: Ein separater, gehärteter Dienst, dessen einzige Aufgabe die sichere Aufbewahrung und Herausgabe von Unlock Keys ist. Der Zugriff erfordert eine gültige Authentifizierung über den Noxtua-IDP und, sofern zutreffend, den IDP des jeweiligen Mandanten (Dual-IDP-Authentifizierung).

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

2.2 Verschlüsselte Speicherung (Encrypted Storage)

Die verschlüsselte Speicherung basiert auf zwei Komponenten:

Encryption Layer: Sitzt zwischen der Anwendungslogik und dem Objektspeicher. Projektschlüssel werden dem Encryption Layer ausschließlich für die Dauer einer einzelnen Operation bereitgestellt und unmittelbar danach gelöscht (Schlüsselbereitstellung).

Object Storage: Speichert alle Projektinhalte in einer dateisystemähnlichen Struktur, gruppiert nach Projekt. Sämtliche sensiblen Inhalte werden vor der Übergabe an den Speicher verschlüsselt – der Speicher selbst sieht ausschließlich Chiffretexte.

3. Verschlüsselungsdetails

3.1 Kryptographische Parameter

Parameter	Wert
Schlüsseltyp	Symmetrisch
Algorithmus	XChaCha20-Poly1305
Schlüssellänge	256 Bit
Tag-Größe	128 Bit
Nonce-Größe	192 Bit
Schlüsselgenerierung	CSPRNG (kryptographisch sicherer Zufallsgenerator)
Nonce-Generierung	Zufällig pro Verschlüsselungsvorgang (CSPRNG)

3.2 Authenticated Encryption (AEAD)

Jeder verschlüsselte Datensatz ist durch Additional Authenticated Data (AD) an seinen Kontext gebunden. Die AD umfasst:

- Fester Kontextstring
- Protokollversion
- Tenant-ID, User-ID, Project-ID und File-ID

Dadurch wird eingeschränkt, in welchen Kontexten Chiffretexte entschlüsselt werden können, ohne dass die Integritätsprüfung fehlschlägt.

4. Umfang der Verschlüsselung

4.1 Verschlüsselte Daten

Sämtliche sensiblen Inhalte werden verschlüsselt, einschließlich Chat-Nachrichten, hochgeladene Dateien, KI-generierte Antworten und potenziell sensible Metadaten wie Dateinamen.

4.2 Nicht verschlüsselte Metadaten

Folgende technische Metadaten werden im Klartext gespeichert, da sie für den Betrieb des Systems erforderlich sind:

- Zugriffsmuster (welcher Nutzer greift wann auf welche Datei zu)
- Dateigröße und zufällig generierte IDs
- Strukturelle Pfadpräfixe (z. B. /user-uploads)

Diese Metadaten enthalten keine inhaltlichen oder personenbezogenen Daten der Mandantenkommunikation. Sie werden ausschließlich zu Betriebszwecken (Routing, Speicherverwaltung, Abrechnung interner Ressourcen) ausgewertet und unterliegen denselben Mandantengrenzen wie die verschlüsselten Inhalte.

5. Datenhaltung und Auftragsverarbeitung

Die Datenhaltung von Noxtua ist auf die Anforderungen europäischer Kanzleien und Rechtsabteilungen ausgerichtet und bietet vollständige Transparenz über Standort, Verarbeitung und vertragliche Grundlagen.

5.1 Standort der Datenverarbeitung

Sämtliche Mandantendaten – verschlüsselte Inhalte ebenso wie betriebliche Metadaten – werden ausschließlich in Rechenzentren innerhalb der Europäischen Union und der Schweiz verarbeitet und gespeichert. Eine Übermittlung außerhalb der Europäischen Union und der Schweiz findet im Standardbetrieb nicht statt.

5.2 Sub-Prozessoren

Noxtua führt eine vollständige, aktuelle Liste aller eingesetzten Sub-Prozessoren. Die Liste umfasst Anbieter, Verarbeitungszweck und Verarbeitungsort und wird Mandanten auf Anfrage zur Verfügung gestellt. Jeder Sub-Prozessor unterliegt einer vertraglichen Bindung nach Art. 28 DSGVO.
Änderungen am Kreis der Sub-Prozessoren werden den Mandanten mit angemessener Vorlaufzeit angekündigt. Vereinbarte Widerspruchsrechte bleiben unberührt.

5.3 Auftragsverarbeitung

Für die Verarbeitung personenbezogener Daten wird ein Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO bei Partnerprodukten (z. B. Beck-Noxtua, MANZ-Noxtua, Swiss-Noxtua) zwischen dem jeweiligen Verlag und dem Mandanten sowie gesondert zwischen Verlag (als Auftraggeber) und Noxtua (als Auftragsverarbeiter) abgeschlossen. Bei direkten Mandaten schließt Noxtua den AVV unmittelbar mit dem Mandanten ab. Der AVV regelt insbesondere Gegenstand und Dauer der Verarbeitung, Art und Zweck, betroffene Personenkategorien sowie die technischen und organisatorischen Maßnahmen (TOM).

5.4 Aufbewahrungsdauer

Für die Aufbewahrungsdauer der in der Cloud gespeicherten Inhalte stehen zwei Optionen zur Verfügung, die dieselbe Speicher- und Verschlüsselungsarchitektur nutzen und sich ausschließlich in der Aufbewahrungsdauer unterscheiden. Standardmäßig ist die unbegrenzte Aufbewahrung aktiv; die achtstündige Aufbewahrung wird ausschließlich auf ausdrücklichen Wunsch des Mandanten eingerichtet:

Unbegrenzte Aufbewahrung (Standard): Inhalte bleiben gespeichert, bis sie vom Nutzer oder Mandanten gelöscht werden oder das Vertragsverhältnis endet. Diese Option ermöglicht den fortlaufenden Zugriff auf vergangene Inhalte, eine durchgängige Chat-Historie sowie die Nutzung von Funktionen, die auf in der Cloud gespeicherte Daten zugreifen.

Aufbewahrung für acht Stunden (auf Anfrage): Projektinhalte werden acht Stunden nach der letzten Interaktion automatisch kryptographisch gelöscht. Nach Ablauf dieser Frist ist ein Zugriff auf die betreffenden Inhalte nicht mehr möglich. Diese Option eignet sich für Mandanten mit restriktiven Anforderungen an die Datenaufbewahrung.

In beiden Optionen werden die Inhalte pro Projekt mit XChaCha20-Poly1305 (256 Bit) verschlüsselt; der Grundsatz der Datenminimierung bleibt gewahrt. Einzelne Projekte können unabhängig von der gewählten Aufbewahrungsdauer jederzeit durch den Nutzer gelöscht werden.

6. Mandantentrennung

LECS implementiert eine zweistufige Mandantentrennung:

Organisatorische Trennung: Projekte sind Nutzern zugeordnet, die wiederum Mandanten (Tenants) zugeordnet sind. Diese Hierarchie spiegelt sich in der Speicherstruktur wider.

Kryptographische Trennung: Jedes Projekt hat einen eigenen Verschlüsselungsschlüssel. Selbst bei einem Softwarefehler oder böswilligem Zugriff auf den Speicher können Daten anderer Projekte nicht entschlüsselt werden.

6.1 Blast Radius bei Schlüsselkompromittierung

Der maximale Wirkungsbereich (Blast Radius) eines kompromittierten Projektschlüssels beschränkt sich auf genau ein Projekt. Da jeder Projektschlüssel unabhängig generiert wird und nur über den nutzerspezifischen Schlüsselbund zugänglich ist, ergibt sich folgende Eindämmung:

- Ein kompromittierter Projektschlüssel betrifft ausschließlich die Daten dieses einen Projekts – nicht den Mandanten, nicht den Nutzer und nicht andere Projekte.
- Ein kompromittierter Unlock Key betrifft maximal die Projekte eines einzelnen Nutzers, da andere Nutzer eigene Unlock Keys verwenden.
- Ein Eingriff in den Objektspeicher allein – ohne Zugriff auf die zugehörigen Schlüssel – führt zu keinerlei Klartextoffenlegung.

7. Schlüsselkontrolle und Zugriffsmodell

Die kryptographische und operative Architektur von LECS ist so gestaltet, dass ein Klartext-Zugriff durch Noxtua ausschließlich dann erfolgen kann, wenn der Kunde eine Verarbeitung veranlasst. Außerhalb dieser Verarbeitungsvorgänge – im Ruhezustand (at-rest) und dauerhaft – verhindern die technischen und operativen Maßnahmen einen Klartext-Zugriff mit einem dem Marktstandard entsprechenden hohen Schutzniveau, sodass ein Zugriff sowohl durch unbefugte Dritte als auch durch den Anbieter selbst nur unter außergewöhnlich erschwerten Bedingungen möglich ist. Dieses Kapitel beschreibt die organisatorischen und rechtlichen Konsequenzen dieser Architektur.

7.1 Schlüsselhalter

Die effektive Kontrolle über die Schlüssel liegt beim Nutzer und damit beim Mandanten:

- Unlock Key: Niemals auf dem Noxtua-Backend gespeichert. Die Entschlüsselung des Schlüsselbunds erfolgt ausschließlich im Browser des Nutzers.
- Schlüsselbund: Nur in mit Unlock Key verschlüsselter Form auf dem Backend abgelegt.
- Projektschlüssel: Dem Encryption Layer ausschließlich für die Dauer einer einzelnen Operation bereitgestellt und unmittelbar danach gelöscht.

7.2 Zugriff auf Klartextdaten

Die LECS Speicherarchitektur gewährleistet, dass Noxtua zu keinem Zeitpunkt dauerhaften Zugriff auf Klartextdaten hat. Klartexte existieren ausschließlich:

- im Browser des authentifizierten Nutzers, und
- flüchtig im Speicher des Backend-Agents während der Bearbeitung einer einzelnen Anfrage.

Administrative Rollen bei Noxtua verfügen über keinen technischen Pfad, projektbezogene Klartextdaten ohne aktive Nutzer-Authentifizierung einzusehen. Dies wird durch die Dual-IDP-Authentifizierung und die strikte Trennung zwischen Unlock Key Vault und Anwendungsbackend abgesichert.

7.3 Löschung bei Vertragsende

Bei Beendigung des Vertragsverhältnisses werden alle Mandantendaten in einem definierten Verfahren gelöscht:

- Kryptographische Löschung: Die projektspezifischen Schlüssel werden unwiederbringlich vernichtet. Die zugehörigen Chiffretexte sind damit auch bei späterem Zugriff auf den Speicher nicht mehr entschlüsselbar.
- Physische Löschung: Im Anschluss werden die verschlüsselten Inhalte sowie die zugehörigen Metadaten aus den produktiven Systemen entfernt.
- Backups: Restbestände in Backups werden im Rahmen der vertraglich vereinbarten Backup-Aufbewahrungsfrist überschrieben bzw. vernichtet.
- Bestätigung: Mandanten erhalten auf Anfrage eine Löschbestätigung.

Eine Datenrückgabe vor Vertragsende kann in einem von Noxtua bereitgestellten, lesbaren Format vereinbart werden.

8. Datenzugriffsdauer

Komponente	Schlüssel- und Datenlebensdauer
Browser (Client)	Verwirft Inhalte, Schlüssel und Token bei Logout oder Projektlöschung
Backend (Agent)	Verwirft alle Schlüssel und Inhalte sofort nach Abschluss der jeweiligen Anfrage
LECS-Service	Agiert ausschließlich als Durchleitungsdienst; persistiert keine Schlüssel

9. Nachweise, Zertifizierungen und Audit-Logs

Die in LECS implementierten Maßnahmen werden durch externe Zertifizierungen und interne Nachweisprozesse abgesichert.

9.1 Zertifizierungen und Standards

Noxtua orientiert seinen Informationssicherheits- und Compliance-Rahmen an folgenden Standards und Gesetzen:

- ISO/IEC 27001: Informationssicherheits-Managementsystem (ISMS) – Zertifizierung bzw. Zertifizierungsverfahren nach aktuellem Stand. Der jeweilige Status wird Mandanten auf Anfrage durch das Sicherheitsteam bestätigt.
- BSI C5: Ausrichtung der Cloud-spezifischen Kontrollen am Cloud Computing Compliance Criteria Catalogue des Bundesamts für Sicherheit in der Informationstechnik. Testate werden Mandanten unter NDA zur Verfügung gestellt, sobald verfügbar.
- SOC 2: Berichterstattung zu den Trust Services Criteria Security, Availability und Confidentiality – aktueller Status auf Anfrage.
- DSGVO / BDSG: Verarbeitung im Einklang mit Art. 28 DSGVO; Abbildung der Anforderungen aus § 203 StGB und § 43e BRAO im Mandanten-Onboarding.

Aktuelle Zertifikatskopien, SOC-Berichte und C5-Testate werden auf Anfrage bereitgestellt.

9.2 Audit-Logs

Alle sicherheitsrelevanten Vorgänge werden in manipulationsgeschützten Audit-Logs erfasst. Erfasst werden insbesondere:

- Authentifizierungs- und Autorisierungsereignisse (inkl. Dual-IDP-Vorgänge)
- Zugriffe auf den Unlock Key Vault
- Anlage, Änderung und Löschung von Projekten und Schlüsseln
- Administrative Zugriffe auf Systeme im Verarbeitungsumfeld

Audit-Logs werden für einen definierten Zeitraum revisionssicher aufbewahrt und im Rahmen interner sowie externer Audits ausgewertet. Mandanten erhalten auf Anfrage Auszüge der sie betreffenden Ereignisse.

9.3 Klartext-Metadaten und ihre Behandlung

Wie in Abschnitt 4.2 beschrieben, verbleibt eine eng begrenzte Menge betrieblicher Metadaten im Klartext. Diese Metadaten:

- enthalten keine Mandanteninhalte und keine personenbezogenen Daten aus den Projekten,
- unterliegen denselben Mandantengrenzen und Zugriffskontrollen wie verschlüsselte Inhalte,
- werden über die Audit-Log-Mechanismen mit überwacht.

Damit ist sichergestellt, dass auch nicht verschlüsselte technische Metadaten nicht für eine inhaltliche Profilbildung über Mandantenkommunikation genutzt werden können.