Lexabit

Trust Center

Security, data protection and compliance documentation for the Lexabit platform.

Version	v0.4.15
Generated	2026-08-24
Source	docs.lexabit.com/docs/trust
Contact	security@lexabit.com

CONTENTS

1. Trust Center
2. Security Overview
3. Architecture Overview
4. Security Controls
5. Data Protection & GDPR
6. Sub-processors & Service Providers
7. Banking & Data Providers
8. Security FAQ
9. Compliance Roadmap

This document is a point-in-time export of the Lexabit Trust Center, generated automatically from the same release that is published on the web. The web version is authoritative and may have been updated since this PDF was generated — check the version above against the live site before relying on it.

Trust Center

Last updated: 2026-08-17

Lexabit is a platform for working with transaction data — compliance and financial intelligence for law firms, financial institutions, and other organisations that analyse financial activity. This Trust Center documents our security posture as it is today, including what is still on our roadmap — we would rather give a straight answer than a polished one.

The web application and the API share the same backend and the same access-control path, so everything described here applies to both unless a page states otherwise.

At a glance

- **Hosting**: EU — DigitalOcean, Amsterdam
- **GDPR**: the customer is the data controller; Lexabit is the data processor (contracting entity: Lexabit AB (SE), or its Danish entity Lexabit ApS where the customer contracts with it)
- **Certifications**: see the Compliance Roadmap for current status
- **Banking access**: via regulated open-banking providers, supervised by their national financial supervisory authorities
- **Security contact**: security@lexabit.com

Explore the Trust Center

- **Security Overview** — architecture, access control, and encryption, as they operate today.
- **Architecture Overview** — components, integrations, infrastructure, and key technical dependencies.
- **Security Controls** — the full control register, with an honest status for each control.
- **Data Protection & GDPR** — what data we process, where it lives, and data-subject rights.
- **Sub-processors & Service Providers** — sub-processors, operational service providers, and banking/data partners.
- **Banking & Data Providers** — the open-banking and company-data providers we connect to.
- **Security FAQ** — answers to common questions from IT and security reviewers.
- **Compliance Roadmap** — current certification status and what's planned.

Security Overview

Last updated: 2026-08-17

Lexabit is a platform for working with transaction data — compliance and financial intelligence for law firms, financial institutions, and other organisations. This page describes the security architecture as it operates today. Where a control is on our roadmap rather than live, it is labelled **Planned** — we do not present planned controls as current.

Platform architecture

Lexabit's backend is a Laravel 11 API; the customer portal and administration panel are React single-page applications that consume it over HTTPS. The platform is hosted by DigitalOcean in Amsterdam, keeping infrastructure and data within the EU.

The application database is MySQL, with a self-hosted MongoDB instance on the same server used only for public business-registry data — company information and registered-role information from national registries — it does not contain the customer's own client, case, or user data. Background work — transaction auditing, bank-account synchronisation, and health monitoring — runs through Laravel's database-backed queue system. Production runs on its own dedicated infrastructure, fully separated from all non-production environments; development and staging are separate deployments, each with its own configuration and data, hosted on shared non-production infrastructure.

Tenant isolation

Lexabit runs on a single shared application database — it does not use a separate database per customer. Isolation is enforced in the application layer by the entity-permissions system on every request: each request carries an `X-Scope` header identifying the entity context (tenant, group, project, client, or case); middleware resolves that header and verifies the authenticated actor can access the requested scope through structural relationship chains and explicit visibility assignments. This follows a four-layer model — Authentication, Visibility, Entitlement, and Action — and scope and permission checks are enforced across the v1 API. Generated reports and documents are access-controlled behind the same permission and scope checks.

Access control

Access to data and actions is governed by a role-based, fine-grained entity-permissions system covering every application entity — tenants, clients, cases, groups, and projects. Every request is evaluated against the authenticated actor's specific role assignments and explicit visibility grants for the requested scope: results are filtered to what the actor can see, and each action is separately permission-gated, rather than access being implied by authentication alone. These checks are enforced across the v1 API.

Authentication

User passwords are hashed with Argon2id before storage. API and single-page-application sessions are authenticated using Laravel Sanctum, and application-to-application access uses Sanctum-issued API keys and OAuth2 client-credentials tokens. Sign-in via Google and Microsoft is supported using OAuth with PKCE, where enabled for a tenant. Session cookies are set with the `Secure`, `HttpOnly`, and `SameSite=Lax` attributes in all deployed environments. Login attempts are rate-limited (6 per minute per IP) and password-reset requests are rate-limited separately (5 per 15 minutes); a credential is locked for 15 minutes after 5 consecutive failed login attempts.

Two-factor authentication (2FA) is **Planned** and not yet available.

Encryption

All traffic to Lexabit is served over HTTPS (TLS, via Let's Encrypt certificates) with HSTS enabled.

Integration credentials — the secrets Lexabit uses to connect to external providers — are encrypted at rest using AES-256 via the application's encryption layer. Client national identity numbers are also column-encrypted. Column-level encryption at rest is currently limited to these two categories; other application data (including transaction records) is protected by the access controls described above and by infrastructure-level controls rather than field-level encryption.

Banking data & PSD2

Lexabit retrieves banking data through regulated third-party open-banking (AISP) providers, each supervised by its national financial supervisory authority. The currently active provider is **Enable Banking**; the platform has integration support for additional providers (such as Neonomics), which are only presented as active when they actually are. Customers authenticate directly with their bank during the connection flow; Lexabit never receives or stores bank login credentials. Connected accounts are covered by individual consents, each with its own status and lifecycle; consents expire and must be renewed, and expired or revoked consents are enforced automatically.

Provider credentials Lexabit uses to authenticate with our banking providers are encrypted at rest; per-connection session data is held server-side.

Access granted to a connected banking application is fail-closed: an app's permitted actions are hard-capped to an explicit allowed set at connection time, and an unrecognised app is denied by default rather than implicitly trusted. Transaction data retrieved from connected accounts is subject to the same entity-permission and scope checks as the rest of the platform.

Monitoring & availability

Lexabit publishes a public `/health` endpoint reporting overall platform status, a token-gated endpoint with detailed diagnostics, and a per-service health check for each core service. The public endpoint is monitored externally by an uptime-monitoring service (UptimeRobot) to alert on availability issues. Background and asynchronous work — including transaction auditing, bank-account synchronisation, and health monitoring itself — runs through dedicated, database-backed job queues rather than inline in the request cycle.

Security contact

Report vulnerabilities or security questions to **security@lexabit.com**.

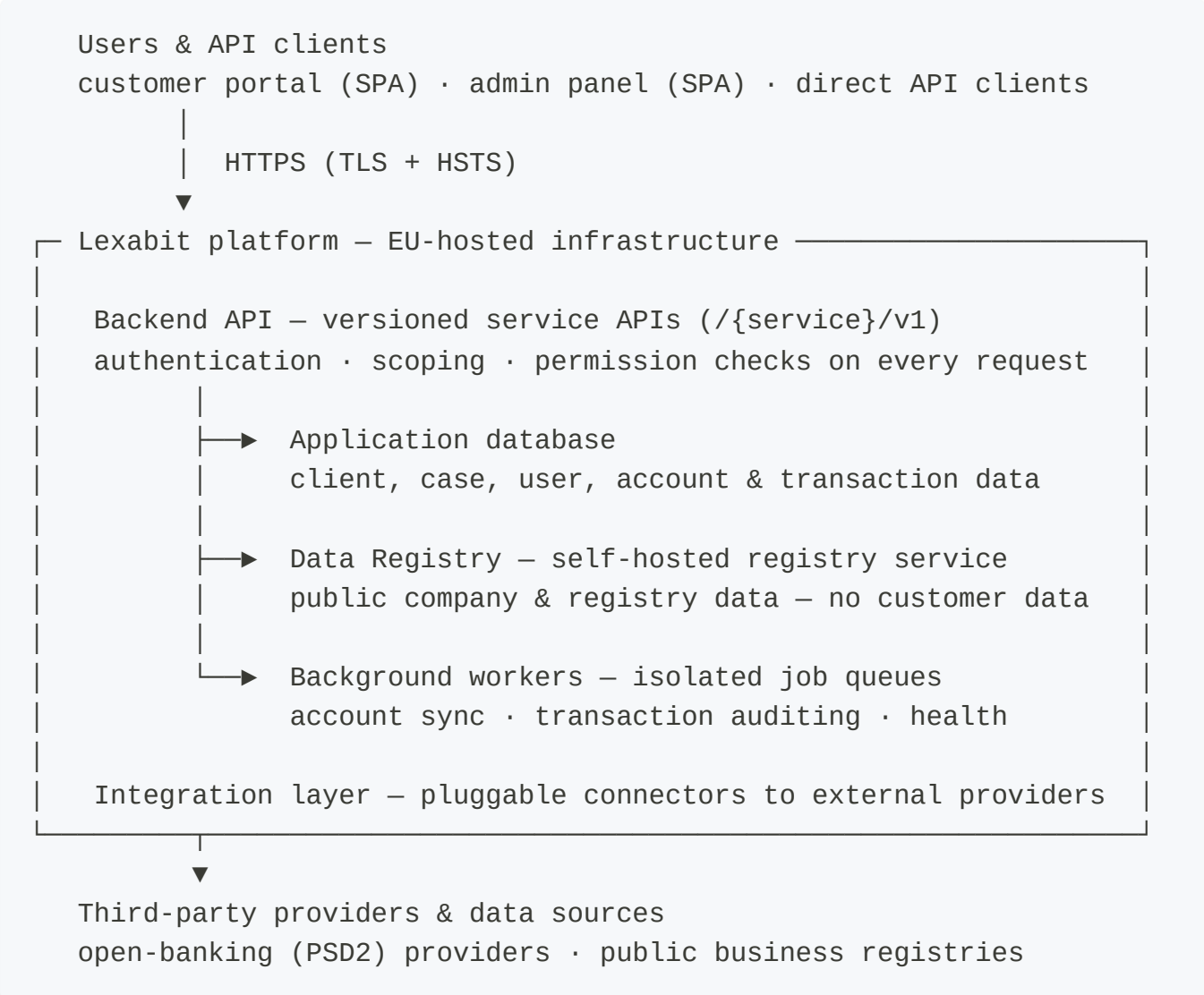
Architecture Overview

Last updated: 2026-08-17

This page describes how the platform actually fits together: the components, how a request travels through them, where data lives, and what the platform depends on. It is written for technical and security reviewers; the security properties of each part are covered in depth in the Security Overview.

The system at a glance

Everything inside the boundary below runs within Lexabit's own hosted infrastructure in the EU.



- The **backend** is a single API exposing versioned service APIs (`/{service}/v1/...`). The **customer portal** and **administration panel** are single-page applications with no

backend of their own — every capability goes through the same API, so the access-control path below applies to all surfaces equally.

- There is **one shared application database** — isolation between customers is enforced in the application layer on every request, not by separate databases per customer.
- The **Data Registry** is a separate, self-hosted registry service deployed inside the same infrastructure. It is deliberately segregated by content: it holds only public business-registry data (companies, registered role holders, beneficial owners) and never the customer's own client, case, or user data.
- The **integration layer** connects the platform to external providers through a common integration framework — providers are pluggable behind it and engaged per provider. Which providers are active, and on what basis, is documented on Banking & Data Providers rather than hard-wired into the architecture.

What happens on a request

Every API request passes through the same pipeline before any data is returned:

```
request ──▶ TLS (HTTPS + HSTS)                          transport
encryption   ENC-5
        ──▶ Authentication (session / API token)        who is the
actor?      AUTH-2
        ──▶ Scope resolution (X-Scope header)           which entity
context?
        ──▶ Visibility check                            may the actor
SEE it?
        ──▶ Entitlement & action check                  may the actor DO
this?
        ──▶ Filtered response                           only what the
actor may see
```

The scope, visibility, and entitlement stages are the entity-permissions system's four-layer model (Authentication → Visibility → Entitlement → Action), enforced across the v1 API — including generated reports and documents. The Security Overview describes the mechanism in full.

Where data lives

Data	Store	Notes
Client, case, user, and account/transaction data	Application database (MySQL)	Single shared database; application-layer isolation per request

Data	Store	Notes
Public company & registry data	Data Registry — self-hosted registry service (MongoDB)	Public-registry content only, fed by national business registries; no customer data
Uploaded files & generated documents	DO object storage (AMS3)	Generated reports/documents are permission-gated; signed-URL storage for uploaded profile media is **Planned**
Bank login credentials	**Nowhere**	End users authenticate at their bank; Lexabit never receives them
Integration/provider credentials	MySQL, encrypted	AES-256 via the credential-management layer

The full data map, by category and source, is on Data Protection & GDPR.

Data flows in and out

- **Banking data (in)** — retrieved through regulated open-banking providers under a PSD2 consent authorized in the bank's own flow, by the account holder or another party entitled to access the accounts. Consents have individual lifecycles and expiry is enforced automatically. The currently active provider is listed on Banking & Data Providers.
- **Registry data (in)** — public national business registries feed the self-hosted Data Registry.
- **Email (out)** — transactional notifications via Mailtrap (Railsware).
- **Monitoring (out)** — a public `/health` endpoint is polled externally by UptimeRobot; per-service health checks run internally.

Background work — bank-account synchronisation, transaction auditing, and health monitoring — runs on isolated, database-backed queues rather than inline in the request cycle.

Environments & deployment

Production runs on its own dedicated infrastructure, fully separated from all non-production environments. Development and staging are separate deployments — each with its own configuration and data — hosted on shared non-production infrastructure. Production releases are tag-based and deployed through a controlled pipeline with environment-scoped secrets and approvals — no ad-hoc production changes.

Key technical dependencies

Dependency	Role
DigitalOcean (Amsterdam, EU)	Hosting: application server, databases, object storage, CDN
Laravel 11 / PHP	Backend framework — parameterized queries, CSRF protection, output escaping by default
React	Customer portal and administration panel SPAs
MySQL / MongoDB (self-hosted)	Application database / Data Registry storage
Laravel Sanctum	API and session authentication
Enable Banking	Open-banking (PSD2) account and transaction access
Let's Encrypt	TLS certificates; HTTPS with HSTS on all traffic
Mailtrap (Railsware)	Outbound transactional email
Google Workspace	Internal business email and support correspondence
UptimeRobot	External availability monitoring

Third parties that process customer personal data, with data categories and regions, are listed on the Sub-processors & Service Providers page.

Questions

Architecture questions from security reviews: **security@lexabit.com**.

Security Controls

Last updated: 2026-08-17

This page lists Lexabit's security controls with an honest status for each. **Planned** means the control is on our roadmap, not live today — nothing planned is presented as current. Every status below traces to an internal evidence inventory reviewed against the current codebase and infrastructure.

Data Security

Control	Statement	Status
Encryption in transit	All traffic served over HTTPS (TLS, via Let's Encrypt certificates) with HSTS enabled	In place
Credential encryption	Integration credentials encrypted with AES-256 via the application's encryption layer	In place
Sensitive-field encryption	Client national identity numbers are column-encrypted	In place
Credential key management	Credential encryption supports key versioning and rotation; keys are application-managed	In place
Database encryption at rest	Arrives with the planned move to a managed database service	Planned
Backups	No backup regime today; planned together with the managed-database move	Planned
Recovery objectives (RPO/RTO)	To be defined and published with the backup regime and recovery testing	Planned

Infrastructure Security

Control	Statement	Status
EU data residency	All hosting in DigitalOcean Amsterdam — droplet, database, object storage, and CDN	In place

Control	Statement	Status
Environment separation	Production on dedicated infrastructure, fully separate from non-production; dev and staging as distinct deployments with their own configuration and data	In place
Availability monitoring	Public health endpoint, per-service health checks, and external uptime monitoring	In place
Background processing	Sync, transaction auditing, and health monitoring run on isolated, database-backed queues	In place
Managed database	Migration to a managed database service, within the same provider project	Planned

Access Control & Product Security

Control	Statement	Status
Tenant isolation	Entity-scoped access control enforced across the v1 API (four-layer model)	In place
Fine-grained permissions	Role-based and per-entity permission checks on individual actions	In place
Password hashing	Argon2id	In place
Account lockout	5 consecutive failed login attempts trigger a 15-minute lockout	In place
Login rate limiting	Per-IP throttling on login and password-reset endpoints	In place
Secure session cookies	Secure, HttpOnly, and SameSite attributes set	In place
API authentication	Token-based (Laravel Sanctum) for SPA sessions and application API keys	In place
OAuth sign-in	Google and Microsoft sign-in, where enabled	In place
Two-factor authentication	Not yet available	Planned

Control	Statement	Status
Enterprise SSO (SAML/OIDC federation)	Not yet available	● Planned
User deprovisioning	Tenant administrators can deactivate or remove users directly in the product	● In place
Token & key revocation	Personal access tokens, application API keys, and OAuth consents are customer-revocable	● In place
Connected-app constraints	App permission grants hard-capped to a connector-defined allowed set, fail-closed	● In place
Report & document access control	Generated reports and documents are permission- and scope-gated	● In place
Private media storage	Signed-URL storage for uploaded profile media	● Planned

Banking Data & PSD2

Control	Statement	Status
Consent-based account access	Bank access via authorized open-banking providers; authorization happens at the bank, by the account holder or an entitled party — Lexabit never sees online-banking credentials	● In place
Individual consent lifecycle	Individual consents, each with its own status and lifecycle	● In place
Consent expiry & renewal	Consents expire and are renewed through dedicated flows	● In place
Provider credential encryption	Lexabit's own provider credentials are encrypted at rest	● In place
Scoped banking data	Bank account and transaction data are behind the same entity-permission scoping as the rest of the platform	● In place

Security Operations

Control	Statement	Status
Application audit logs	Integration activity and login metadata recorded	In place
Controlled deployments	Tag-based production deploys through a pipeline with environment-scoped secrets and approvals	In place
Dependency & code security checks	Dependency security audit and static analysis in the development quality gate	In place
Privileged-access audit logging	Formal logging of administrative access to production infrastructure	Planned
Central security monitoring & alerting	SIEM-style monitoring and automated alerting on suspicious activity	Planned
Scheduled vulnerability scanning	Recurring scanning of application, APIs, and infrastructure	Planned

Privacy & Assurance

Control	Statement	Status
GDPR roles	Customer is data controller; Lexabit (Lexabit AB / Lexabit ApS per contract) is data processor	In place
Data-map transparency	Processed data categories are published, including registry-sourced data	In place
Data subject requests	Handled via security@lexabit.com	In place
Data Processing Agreement	Standard DPA template — today, data-processing terms are agreed directly with each customer during onboarding	Planned
Privacy policy	Not yet published	Planned
External penetration test	Not yet conducted	Planned

Control	Statement	Status
Certifications (ISO 27001 direction)	See the Compliance Roadmap for current status and direction	● Planned

For narrative detail on how these controls work together, see the Security Overview. For committed direction and target dates as they're set, see the Compliance Roadmap.

Data Protection & GDPR

Last updated: 2026-08-18

Roles under GDPR

For customer data processed in the platform, the customer is the data controller and Lexabit is the data processor. The contracting Lexabit entity is Lexabit AB (Sweden) or its Danish entity Lexabit ApS, depending on which entity the customer's agreement is with; the processing described in this Trust Center is the same in either case. A Data Processing Agreement is **Planned**: bilateral data-processing terms are currently handled directly with each customer during onboarding, rather than through a standard published template.

Data we process

Category	Examples	Source
Account & user data	Login credentials, session and authentication metadata	Created at sign-up / sign-in
Client & case records	Client and case records the customer creates in the platform	Entered by the customer
Bank account & transaction data	Account and transaction data from connected bank accounts	Retrieved under an authorized PSD2 consent through regulated open-banking providers (currently Enable Banking)
Company & registry data	Public company information plus registered role holders (directors, board members — name, date of birth, address) and beneficial owners	Public national business registries via Lexabit's self-hosted data registry
Audit logs	Integration activity and login metadata	Recorded by the platform's logging infrastructure

Data residency

Lexabit is hosted entirely on DigitalOcean in Amsterdam — the application server, database, and CDN all run in the Amsterdam region, with object storage in the DO Spaces AMS3 region. All customer data therefore resides within the EU (Netherlands). Both MySQL and MongoDB are self-hosted on the same server. The self-hosted MongoDB registry — on the same Amsterdam

infrastructure — holds this public-registry dataset; it does not contain the customer's own client, case, or user data.

Retention & deletion

Data is retained for as long as the customer's account remains active and used to deliver the platform's features. A formalized retention schedule is **Planned**. Requests for data deletion or erasure are handled operationally by contacting the security contact below.

Data-subject rights

Data subjects can access and correct their personal data through the application's normal features (for example, account and profile settings). Requests for data export or erasure beyond what the application supports are handled by contacting **security@lexabit.com**.

Sub-processors

Lexabit uses a small number of sub-processors to deliver the platform, including hosting and outbound email , and lists operational service providers where customer personal data may incidentally appear. Open-banking and company-data providers are used under a different model — see Sub-processors & Service Providers and Banking & Data Providers for details.

Sub-processors & Service Providers

Last updated: 2026-08-19

This page lists the third parties involved in delivering Lexabit, in three categories that reflect how each one actually touches data. We list deliberately inclusively — where there is any realistic path for customer personal data to reach a vendor, we would rather disclose it than argue it away.

Sub-processors

Sub-processors are third parties that process customer personal data on Lexabit's behalf, engaged under GDPR Article 28, as part of delivering or supporting the service. Each processes data only to the extent needed for its stated function.

Provider	Purpose	Data categories	Region	Status
DigitalOcean, LLC	Cloud infrastructure hosting (servers, database, object storage, CDN)	All platform data	Amsterdam, Netherlands (EU)	● Active
Railsware Products Studio LLC	Mailtrap — outbound transactional email delivery	Email addresses and notification content	EU/US (provider-operated)	● Active
Google Cloud EMEA Limited	Google Workspace — internal business email and customer support correspondence (Google Cloud EMEA Limited is Google's EMEA contracting entity for Workspace)	Correspondence with customer staff	EU/US (provider-operated)	● Active
Functional Software, Inc. (Sentry)	Error tracking and debugging — reserved for future integration; will receive error/diagnostic data if introduced	None today — not integrated	EU/US (provider-operated)	● Planned

A **Planned** row means the provider is named in our Data Processing Agreement's approved list ahead of use — part of future-proofing the approved list — but is not integrated and receives no data today. It will move to Active here before any data flows to it.

Service providers

Operational tools we use to run the company. They are **not** engaged to process customer data, and no customer data is shared with them by design — but day-to-day work (support coordination, issue tracking) means customer personal data may **incidentally** appear in them, for example in a support ticket that quotes a customer email. We list them for exactly that reason.

Provider	Purpose	Exposure	Region
Slack Technologies, LLC (Salesforce)	Internal team communication	Incidental — customer context may be referenced in internal discussion	EU/US (provider-operated)
Linear Orbit, Inc.	Issue tracking and development planning	Incidental — tickets may reference customer context	EU/US (provider-operated)

Slack also appears in the Data Processing Agreement's approved sub-processor list — it is included there for completeness under the same over-inclusive principle as this page; the actual engagement is as described here.

Banking & data partners

Regulated parties we retrieve data **from**. They act under their own regulatory obligations and the end user's consent — Lexabit does not share customer data with them or instruct them to process data on Lexabit's behalf, so they are not sub-processors in the Article 28 sense. For safety, the full roster named in our agreements is listed here with each provider's honest current status (mirroring Banking & Data Providers).

Provider	Purpose	Basis	Region	Status
Enable Banking Oy	Open-banking (PSD2) account and transaction retrieval	Authorized TPP, supervised by its national FSA; access authorized by the end user at their bank	EEA	• Active

Provider	Purpose	Basis	Region	Status
Neonomics AS	Open-banking (PSD2) account and transaction retrieval	Authorized TPP; no data flows today	EEA	● Integration built — not active
Tink AB	Open-banking (PSD2) — named in the Master Agreement ahead of use	Authorized TPP; not integrated, no data flows	EEA	● Not yet integrated
Aiia A/S (a Mastercard company)	Open-banking (PSD2) — named in the Master Agreement ahead of use	Authorized TPP; not integrated, no data flows	EEA	● Not yet integrated

Enable Banking also appears in the Data Processing Agreement's approved sub-processor list — included there for completeness; the engagement model is as described here and on Banking & Data Providers, and Lexabit does not instruct it to process customer data on our behalf.

Public national business registries feed the self-hosted Data Registry; how each source is engaged is described on Banking & Data Providers.

MongoDB is self-hosted on Lexabit's own DigitalOcean infrastructure and is not a third-party sub-processor.

Changes to this list are announced to customers in advance. A downloadable export lives on the Downloads page. Questions: **security@lexabit.com**.

Banking & Data Providers

Last updated: 2026-08-19

Lexabit connects to a small number of external providers to retrieve banking and company data. These providers are not engaged as sub-processors of customer data in the classic sense described on the Sub-processors & Service Providers page — they either act under their own regulatory obligations and the end user's direct consent, or receive no customer personal data at all. This page explains how each is used.

Open-banking providers

Lexabit retrieves banking data through regulated third-party open-banking providers (TPPs), each authorized and supervised by its national financial supervisory authority. The currently active provider is  **Enable Banking** (Enable Banking Oy), operating under its own regulatory obligations within the EEA. Account and transaction data is retrieved under the end user's explicit consent, given directly in the provider's or bank's own consent flow, not to Lexabit.

To future-proof our contractual documents, additional providers are named in the Master Agreement ahead of use. Their honest current status:

Provider	Status
Enable Banking Oy	● **Active**
Neonomics AS	● **Integration built — not active**
Tink AB	● **Not yet integrated**
Aiia A/S	● **Not yet integrated**

A provider is only presented as active when it actually is, and this page is updated before any additional provider is put into use.

Company data sources

Company information in Lexabit is served from our own self-hosted data registry, fed by public national business registries in the countries where our customers operate. The registry includes public-registry information about companies and their registered role holders —

directors and board members (name, date of birth, address) — and beneficial owners. See Data Protection & GDPR for the full data map.

The platform includes integration support for commercial company-data providers; none is currently active, and this page will be updated before any is put into use.

Data source catalogue

To future-proof our contractual documents, the Master Agreement names data sources ahead of use. This catalogue mirrors that list with each source's honest current status: **Active** means data actually flows today; **Not yet in use** means the source is pre-approved contractually but no integration exists and no data is retrieved. A source moves to Active here before it is put into use.

Business registers

Source	Contributes	Basis	Status
Brønnøysundregistrene (NO)	Companies, registered role holders, beneficial owners	Public national register	• Active
CVR / Erhvervsstyrelsen (DK)	Companies, participants/role holders, production units, registration history, financial statements	Public national register	• Not yet in use
Bolagsverket (SE)	Companies and registered roles	Public national register	• Not yet in use
Skat.dk / Danish Tax Agency (SKAT)	VAT registration status	Public lookup	• Not yet in use
Statstidende (DK)	Official gazette notices	Public register	• Not yet in use

Property, address & geo

Source	Contributes	Basis	Status
BBR (DK)	Building and dwelling data	Public register	• Not yet in use

Source	Contributes	Basis	Status
Tinglysning.dk (DK)	Property registration	Public register	• Not yet in use
Address Register (SDFI) / DAWA (DK)	Address data	Public open data	• Not yet in use
DinGeo (DK)	Geo and property context	Public open data	• Not yet in use
Opendata.dk	Open public datasets	Public open data	• Not yet in use

Sanctions, PEP & adverse media

Source	Contributes	Basis	Status
EU sanctions lists	Sanctions screening	Public official lists	• Not yet in use
OFAC sanctions lists	Sanctions screening	Public official lists	• Not yet in use
PEP lists	Politically-exposed-person screening	Provider will be named here before use	• Not yet in use
Media searches	Adverse-media screening	Source/engine will be named here before use	• Not yet in use

Licences, authorisations & supervisory registers

Source	Contributes	Basis	Status
Finanstilsynet (DK)	Financial supervisory register	Public register	• Not yet in use
FSR auditors register (DK)	Authorised auditors	Public register	• Not yet in use
Advokatnøglen (DK)	Lawyers directory	Public directory	• Not yet in use

Source	Contributes	Basis	Status
Indsamlingsnævnet (DK)	Fundraising permits	Public register	● Not yet in use
Haulage permits (DK)	Transport licences	Public register	● Not yet in use
Spillemyndigheden (DK)	Gaming licences	Public register	● Not yet in use
Findsmiley.dk + inspection metadata (DK)	Food-inspection results	Public register	● Not yet in use

Commercial query services

Unlike the public registers above, these are commercial third parties that would **receive a query** (an address or company name) when used — so they get their own disclosure with basis and region before any use:

Source	Contributes	Basis	Status
Google Street View	Visual address context	Commercial service — receives the queried address	● Not yet in use
Google My Business	Business-listing context	Commercial service — receives the queried company name	● Not yet in use

A downloadable export of this catalogue is on the Downloads page.

Security FAQ

Last updated: 2026-08-17

Where is our data hosted?

Lexabit is hosted by DigitalOcean in Amsterdam, the Netherlands — the application server, database, and CDN all run in that region, keeping data within the EU.

Is data encrypted in transit and at rest?

All traffic to Lexabit is served over HTTPS (TLS, via Let's Encrypt certificates) with HSTS enabled. At rest, integration credentials are encrypted using AES-256 via the application's encryption layer, and client national identity numbers are column-encrypted. Column-level encryption at rest is currently limited to those two categories; other application data (including transaction records) is protected by access controls and infrastructure-level controls rather than field-level encryption. Encryption keys are application-managed on the production environment; the credential-encryption layer supports key versioning and rotation. There are currently no backups to encrypt — see How are backups handled?

How is our data isolated from other tenants?

Lexabit runs on a single shared application database — it does not use a separate database per customer. Isolation is enforced in the application layer: every request carries an `X-Scope` header identifying the entity context (tenant, group, project, client, or case), and middleware verifies the authenticated actor can access that scope through structural relationship chains and explicit visibility assignments before any data is returned. See the Security Overview for the full mechanism.

Do you support Single Sign-On (SSO)?

Sign-in via Google and Microsoft is supported using OAuth with PKCE, where enabled. Enterprise SSO federation (SAML or OIDC) is **Planned** and not yet available.

Do you support two-factor authentication (2FA)?

Two-factor authentication is **Planned** and not yet available. Today, account security relies on Argon2id password hashing and an automatic lockout after 5 consecutive failed login attempts.

Who at Lexabit can access our data?

Lexabit is a small team; access to customer data in production systems is limited to operations personnel who need it to run and support the platform. Production infrastructure access is key-

based and restricted to that same small group, and production deploys run through a controlled pipeline with environment-scoped secrets and approvals. Formal audit logging of privileged (administrative) access to production infrastructure is **Planned** — it is not yet in place, and we say so rather than imply otherwise.

How are tokens, credentials, and other secrets handled?

Secrets fall into three groups, handled differently:

- **Customer bank credentials** — never seen or stored by Lexabit; authentication happens at the bank (see below).
- **Integration and provider credentials** — stored encrypted (AES-256) through a dedicated credential-management layer that supports key versioning and rotation, and logs credential operations to an audit trail.
- **API tokens and keys** — user sessions and API access use Laravel Sanctum tokens; personal access tokens, application API keys, and OAuth consents can each be revoked by the customer directly in the product, taking effect immediately.

Can we remove a user and their access ourselves?

Yes. Tenant administrators can deactivate or remove users in the product; a removed or deactivated user loses platform access, and their role assignments no longer grant access to customer data. Personal access tokens and application keys created under the tenant can likewise be revoked by the customer without contacting Lexabit.

Is the isolation between customers and cases tested?

Tenant and case isolation is enforced by the entity-permissions system on every request (see how isolation works), and that system is covered by an automated test suite exercising role, permission, visibility, and scope checks, run as part of the development workflow. An external penetration test, which would provide independent validation, is **Planned**.

Do you have central security logging, monitoring, and alerting?

Partially — and we distinguish honestly between the pieces:

- **Application audit logs** are **In place**: integration activity and login metadata are recorded.
- **Availability monitoring** is **In place**: a public health endpoint plus per-service health checks, monitored externally, with a public status view at status.lexabit.com.
- **Centralized security monitoring and automated alerting on suspicious activity** (SIEM-style) is **Planned** — not yet implemented.

Have you defined RPO and RTO?

Not yet. Lexabit does not run backups today, so publishing recovery objectives would be meaningless — we would rather state that plainly. RPO and RTO will be defined and published together with the planned backup regime and managed-database move, along with the status of recovery testing.

How do you handle vulnerabilities, patching, and security testing?

Today: dependency security auditing and static analysis run as part of the development quality gate before changes ship, and framework/dependency updates are applied through the normal development cycle. Scheduled vulnerability scanning of the running application and infrastructure, formalized patch-management cadence, and an external penetration test are **Planned** and tracked on the Compliance Roadmap.

How do you handle bank credentials?

Lexabit connects to bank accounts through regulated open-banking providers — currently Enable Banking. Customers authenticate directly with their bank during the connection flow — Lexabit never receives or stores bank login credentials. Bank connections are covered by individual consents, each with its own lifecycle, and expired or revoked consents are enforced automatically. The credentials Lexabit uses to authenticate with our banking providers are encrypted at rest.

Are you ISO 27001 or SOC 2 certified?

Not yet. Lexabit does not hold ISO 27001 or SOC 2 certification directly; our infrastructure provider, DigitalOcean, is independently certified to both. See the Compliance Roadmap for current status and direction.

Have you had a third-party penetration test?

Not yet — an external penetration test is **Planned**. See the Compliance Roadmap for details.

How are backups handled?

Honestly: Lexabit does not run backups today. A formal backup regime, alongside a planned move to a managed database service, is **Planned**.

What is your incident-response process?

Lexabit publishes a public `/health` endpoint and a per-service health check for each core service, monitored externally by an uptime-monitoring service to alert on availability issues. As

a data processor, Lexabit is committed to notifying affected customers without undue delay, consistent with our GDPR obligations.

How do you develop software securely?

Production runs on its own dedicated infrastructure, fully separated from the non-production environments. Development and staging are separate deployments — each with its own configuration and data — on shared non-production infrastructure. The underlying framework (Laravel) provides parameterized database queries, CSRF protection, and output escaping by default.

Can we get our data out?

Audit-log export for integration activity is available in-product. The platform also generates on-demand reports and documents, which are access-controlled behind the same permission and scope checks as the rest of the platform. For other data export or erasure requests, contact **security@lexabit.com**.

How do we report a vulnerability?

Email **security@lexabit.com**.

Compliance Roadmap

Last updated: 2026-08-18

Lexabit is an early-stage platform. We believe security reviews deserve straight answers, so this page states exactly where we are.

Today

- No third-party certifications (ISO 27001, SOC 2) yet.
- No completed external penetration test yet.
- Security controls that ARE live are documented in the Security Overview and labelled **In place**.

Inherited assurances

- **DigitalOcean** (infrastructure): independently certified to ISO/IEC 27001 and SOC 2 Type II, and offers a GDPR Data Processing Agreement. See DigitalOcean's trust page for their current certifications.
- **Enable Banking** (open banking): an authorized open-banking provider, supervised by its national financial supervisory authority.

Planned

- External penetration test.
- A standard Data Processing Agreement (DPA) template.
- A published privacy policy.
- Two-factor authentication (2FA).
- An automated backup regime, alongside a move to a managed database service.
- Private, signed-URL document storage for files currently served by unguessable public URL.
- Scheduled vulnerability scanning of the running application and infrastructure, and a formalized patch-management cadence. (Dependency security auditing and static analysis already run in the development quality gate.)
- Central security monitoring and alerting for suspicious activity (SIEM-style).
- Audit logging of privileged administrative access to production infrastructure.
- Defined and published RPO and RTO, together with the backup regime and recovery testing.
- Movement toward ISO 27001 as our customer base grows.

Planned items describe direction only — they are **not part of any current subscription or price**. None have committed dates yet; this page will be updated as that changes.

Questions

Contact **security@lexabit.com**.