



Vendor security questionnaire, Varhugi's answers

The answers are the same as those published at varhugi.is/oryggi and apply on the day this document is fetched. The latest version is always on that page.

1. What data is stored

Staff name, email, department and role; training progress, quiz results and certificates; sign-in records (time, IP, browser). Nothing else.

The following categories of personal data are processed: staff name, email address, department and role; training progress, quiz results and issued certificates; and technical records of sign-ins and usage (timestamps, IP addresses, browser type). The data subjects are the customer's staff and administrators. The service is not intended for special categories of personal data and the customer must not enter such data into it.

The processing consists of providing security-awareness training: maintaining staff lists, assigning modules, recording quiz results, issuing certificates, and producing statistics and audit reports for the customer. Processing lasts for as long as the customer has an active account, plus the deletion period described in the section on deletion and return of data.

See: Categories of data in the DPA

2. Where it is hosted

Vercel, with the database at Neon in Frankfurt, inside the EEA. Point-in-time database restore and instant rollback of deployments.

The service runs on Vercel and all data is stored in a PostgreSQL database at Neon in Frankfurt, Germany, within the European Economic Area. Email, such as sign-in links and reminders, is sent through Resend.

Some subprocessors are US companies. Where personal data is transferred outside the EEA, the transfer relies on the European Commission's Standard Contractual Clauses (SCC) or the subprocessor's participation in the EU-US Data Privacy Framework.

Components: Varhugi is a single web application running on Vercel. All customer data lives in one PostgreSQL database at Neon in Frankfurt. Upstash Redis holds only short-lived keys for rate limiting and idle checks, never customer data, and Resend delivers email. Varhugi operates no servers of its own.

See: Hosting



3. Authentication

No passwords. Email link or SSO with Microsoft and Google, where your MFA applies. Admin, manager and staff roles. Server-side sessions, admins signed out after four hours idle.

No passwords: Varhugi stores no passwords. Sign-in happens via a verification link sent by email or through your workplace identity provider, so there is no password database that can leak.

SSO with Microsoft and Google: Staff sign in with their workplace Microsoft Entra ID or Google account, so your own MFA and conditional access policies apply at sign-in. Varhugi has no MFA of its own; with the email link, security rests on access to the mailbox. A disabled account can no longer sign in, but the person remains a member in Varhugi until removed under People.

Role-based permissions: Permissions follow roles. Regular staff see only their own training, and administrators see the status of their own company, no one else's.

Tenant isolation: Each company's data is separated from every other's, and all queries are scoped to the signed-in user's company.

Sign-in and sessions: Users sign in with a one-time link sent by email, valid for 24 hours, or with Microsoft or Google SSO. Varhugi stores no passwords. Sessions are kept server-side and end immediately on sign-out. Admin and manager sessions are also terminated after four hours without activity.

See: Sign-in and access control

4. User provisioning

SSO users join automatically and roles sync from Entra app roles. SCIM is not supported yet, so leavers are removed by an admin under People.

Staff sign in with their workplace Microsoft Entra ID or Google account, so your own MFA and conditional access policies apply at sign-in. Varhugi has no MFA of its own; with the email link, security rests on access to the mailbox. A disabled account can no longer sign in, but the person remains a member in Varhugi until removed under People.

See: SSO setup guide

5. Encryption

TLS for all traffic, encryption at rest in the database.

Encryption in transit and at rest: all traffic runs over TLS and database contents are encrypted at rest.

Security headers on every page, including X-Frame-Options: DENY, nosniff, Referrer-Policy and Permissions-Policy.

Rate limiting on sign-in and other sensitive endpoints protects against guessing attempts and abusive traffic.

Security updates to software dependencies are part of the service's regular maintenance.

See: Technical safeguards



6. Who at Varhugi can access your data

A short allowlist of named staff accounts with an operations view. Staff do not sign in to customer workspaces. Customer admin actions are audit-logged.

Staff access and secrets: Varhugi staff do not sign in to customer workspaces. Access to production is limited to a short allowlist of named accounts, held as configuration rather than code, and gives access to an operations view with account and usage figures; that access is not currently written to the customer-facing audit log. Credentials for hosting, database and email providers are kept in the hosting platform's environment configuration, never in source code, and can be rotated without a code change.

Audit trail: Security-relevant admin actions are written to an append-only audit log: sign-ins, role changes, removals, invitations, assignments and changes to SSO settings, each with actor, target, time and IP address. The log is made available to the customer on request.

Separation between customers: Customers share the database, but every record belongs to one organisation. Every read and write in the admin area passes through a single authorisation module that checks the user's membership and role before any data is touched. A department manager can only see and change their own department; only an admin can act across the whole organisation.

See: [Staff access](#)

7. Security testing

Automated dependency audit on every change and weekly. Full code review in July 2026. No independent penetration test yet.

Vulnerability management: Software dependencies are audited automatically on every code change and again every week. A high or critical advisory blocks the release until it is fixed. The whole codebase was reviewed for security in July 2026, as described below.

A thorough security review of the service's entire codebase was carried out in July 2026 and the resulting fixes were shipped. The review is repeated regularly. No independent penetration test has been carried out yet; when one is, the summary will be published here.

If you find a vulnerability in the service, we welcome a report via the [Contact](#) page and will respond quickly.

See: [Security review](#)

8. Incident response

Notification within 24 hours of Varhugi becoming aware of a breach affecting your data, with follow-up as the investigation progresses.

If a breach affecting a customer's data is detected, the customer is notified within 24 hours of Varhugi becoming aware of it, with a description of the nature of the breach, its likely impact and the measures taken, followed by updates as the investigation progresses. This leaves the company time to meet its own 72-hour notification duty to the Icelandic Data Protection Authority where applicable.

If Varhugi becomes aware of a personal data breach affecting the customer's data, it notifies the customer's designated contact without undue delay and no later than 24 hours after becoming aware of it. The notification describes the nature of the breach, which data and individuals may be affected, the likely consequences, and the measures taken, and is followed up as more becomes known. This enables the customer to meet its own obligation to notify the supervisory authority within 72 hours where applicable.

See: [Security incidents](#)



9. GDPR

Data Processing Agreement applies automatically. Five named subprocessors, 30 days' notice of changes. Data deleted or returned within 30 days of contract end.

The Data Processing Agreement applies automatically to every company using the service. Pro customers can request a countersigned copy.

Varhugi uses a small set of well-known subprocessors. Each receives only the data its service requires and is bound by a data processing agreement with Varhugi. Customers are notified of changes to this list 30 days in advance. Vercel (Hosting and running the application), Neon (Database, hosted in Frankfurt), Resend (Sending email), Stripe (Payment processing when a subscription is paid), Upstash (Cache for rate limiting).

At the end of the service, or on request, personal data is deleted within 30 days or returned in a common machine-readable format. Issued certificates are retained so they can be verified on the public verification page, but are deleted on specific request.

Service data is hosted within the European Economic Area as a rule. Some sub-processors are US companies, and any transfer of personal data outside the EEA relies on the European Commission's Standard Contractual Clauses (SCC) or on the sub-processor's participation in the EU-US Data Privacy Framework, under Varhugi's data processing agreement with each party. The list of sub-processors is maintained in the privacy policy.

See: Data Processing Agreement

10. Assurance

No ISO 27001 or SOC 2 for Varhugi itself. Vercel and Neon hold SOC 2 Type 2. No SLA on current plans.

Certifications: Varhugi holds no ISO 27001 or SOC 2 certification and does not claim to. The providers that run the infrastructure, Vercel and Neon, hold SOC 2 Type 2 and publish their reports on their own trust pages. No formal uptime guarantee (SLA) is offered on the current plans.

Backups and recovery: The database provider keeps a continuous history of changes, so the database can be restored to a point in time rather than only to the last nightly copy. The application is deployed from version control and every deployment is kept, so a faulty release can be rolled back within minutes.

See: Certifications

Related documents

Security at Varhugi	https://varhugi.is/en/oryggi
Data Processing Agreement	https://varhugi.is/en/vinnslusamningur
Privacy policy	https://varhugi.is/en/personuvernd
Terms of service	https://varhugi.is/en/skilmalar