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; reports of suspicious messages and policy attestations submitted by staff; sign-in records (time, IP, browser). Nothing else.

marketing.vinnslusamningur.sections.data_body

marketing.vinnslusamningur.sections.scope_body

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. Data is stored in a database at Neon in Frankfurt, Germany, and issued certificates in Vercel file storage, also in Frankfurt, both 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: The application runs on Vercel in Frankfurt and all persistent data, the database and issued certificates, is hosted there too, within the EEA. The rate-limiting cache holds only hashed identifiers, never plain email addresses or IP addresses. 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 or deactivated through SCIM.

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 single-use link sent by email, valid for 15 minutes, or with Microsoft or Google sign-in (SSO). Varhugi stores no passwords. Rights that derive from an email address, invitations and signup links, are only granted to verified addresses. Sessions are stored server-side, last at most 30 days and end the moment a user signs out. Admin and manager sessions are also closed after four hours of inactivity.

See: Sign-in and access control

4. User provisioning

SSO users join automatically and roles sync from Entra app roles. SCIM provisioning for Entra ID creates members and deactivates leavers automatically; deactivated members keep their history and free their seat.

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 or deactivated through SCIM.

See: SCIM 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: an enforced Content-Security-Policy with nonces that only allows the site's own scripts, HSTS with preload, 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 few named accounts with access to the production environment. 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 the operations environment is limited to a few named accounts. All secrets live in the hosting platform's 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, SCIM events, policy confirmations and reports, each with actor, target, time and IP address. Admins can browse it under Settings and export it as CSV.

Separation between customers: Tenant separation is enforced on every single query: a user reaches only their own workspace's data and a department manager only their own department. Org-wide power is limited to admins.

See: Staff access

7. Security testing

Automated dependency audit on every change and weekly. Full code review in July and September 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 and again in September 2026 with a focus on tenant isolation, as described below.

A thorough security review of the service's entire codebase was carried out in July 2026 and again in September 2026, the latter focused on tenant isolation, role boundaries and authentication, and the resulting fixes were shipped. The review is repeated regularly. Automated authorization tests run on every code change and confirm that one company's data is never visible to another, that department managers only see their own department and that deactivated users cannot get in. An independent penetration test has not yet taken place; when it does, a summary will be published here.

If you find a vulnerability in the service, we welcome a report at info@varhugi.is or at the address in the site's security.txt file at varhugi.is/.well-known/security.txt, and will respond quickly.

See: Security review

8. Incident response

Notification without undue delay and as a rule within 48 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 without undue delay and as a rule within 48 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.

marketing.vinnslusamningur.sections.breach_body

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. Companies on the Pro tier or a custom agreement 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 and storing issued certificates, Frankfurt), Neon (Database, hosted in Frankfurt), Resend (Sending email), Stripe (Payment processing when a subscription is paid), Upstash (Cache for rate limiting and operational markers, hosted in Frankfurt).

At the end of the service the company has 30 days to retrieve its data in a common machine-readable format; after that, or earlier on request, personal data is deleted. Issued certificates belong with the individual and remain stored so they can be verified on the public verification page; for that retention Varhugi is an independent controller, and a certificate holder may request deletion at any time.

marketing.vinnslusamningur.sections.transfers_body

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