Privacy Policy — Version 1.0

Last updated: 28 Nov 2025

At Viti Science AB ("we", "us", "our"), your privacy is important to us.
This Privacy Policy outlines how we collect, use, store, and protect your personal data when you:

- visit or interact with our **website**,
- communicate with us through **e-mail, forms, meetings, or events**,
- participate in **research activities, surveys, or scientific studies** conducted by Viti Science,
- engage with us as a **client, partner, or service provider**, or
- use any of our **digital products, software tools, or online services** ("our Services").

It also explains your rights under GDPR, including how to access, correct, or request deletion of your data and how you can exercise control over how your information is used.

---

1. Who We Are

Role	Details
Controller	Viti Science AB
Reg. No.	559379-5510
Address	Stopvagen 91, 168 36 Stockholm, Sweden
E-mail	mate.szilcz@vitiscience.se
Data-Protection Officer (DPO)	Mate Szilcz — mate.szilcz@vitiscience.se — +46 (0) 72-171 95 05

---

2. What Data We Collect

Category	Typical items	Source
User-Account Data	Name, e-mail, organization, hashed password, roles/preferences	You
Usage & Technical Data	IP address, device/browser, pages visited, error logs, timestamps	Automatic
Uploaded / Generated Data	Digitized KM curves, pseudonymized or empirical IPD, model settings, outputs, documents uploaded through our Services	You / our Services
Cookie & Tracking Data	Session cookies (necessary), analytics cookies (optional)	Automatic

Important:
We do not require identifiers such as patient names, IDs, addresses, or dates of birth.
If you upload real IPD or research data containing personal information:

- you **must have a lawful basis** under GDPR or applicable ethics rules,
- you must remove direct identifiers wherever possible, and
- you remain responsible for ensuring compliance when uploading such data.

---

3. How & Why We Use Your Data (Purposes and Legal Bases)

Purpose	Legal basis (Art. 6 GDPR)	Examples
Provide and secure our Services	Contract (Art. 6(1)(b))	Account management, authentication, processing uploads
Improve functionality, fix bugs, aggregated statistics	Legitimate interest (Art. 6(1)(f))	Feature analytics, performance metrics
Send service e-mails	Legitimate interest	Security advisories, maintenance notices
Send marketing newsletters	Consent (Art. 6(1)(a))	Product updates, events, webinars

You may withdraw consent at any time without affecting processing that occurred prior to withdrawal.

---

4. Cookies & Similar Technologies

We use:

- **Essential cookies** — required for authentication and core functions
- **Analytics cookies (Matomo Cloud)** — optional and opt-in only

You can manage non-essential cookies via our cookiebanner or your browser settings.

---

5. Data Storage & Security

Hosting locations

- **AWS eu-north-1 (Stockholm)** — encrypted object storage (SSE-S3)
- **Microsoft Azure EU** — application servers, Postgres databases
    - *All project data stored in Azure databases is encrypted at rest using AES-256.*

Transmission security

- TLS 1.2+ for all traffic

Access control

- Role-based access control (RBAC)
- Least-privilege IAM policies
- Access logging

Security practices

- Regular penetration tests
- Automated vulnerability scans
- Server hardening
- Encrypted backups

Authentication & Identity

We use **Auth0 (EU tenant)** for identity and access management:

- Credentials stored only in Auth0
- Mandatory TLS 1.2+
- Mandatory **2FA** (TOTP or WebAuthn)

Auth0 is a GDPR-compliant sub-processor under SCCs and a DPA.

---

6. Data Sharing & Sub-Processors

We **never sell** personal data.
We share data only with vetted sub-processors located in the EU/EEA or under EU-approved safeguards:

Category	Provider	Location	Purpose
Cloud infrastructure	Amazon Web Services	Stockholm (eu-north-1)	File storage, backups
Application hosting	Microsoft Azure	North Europe	Compute, managed Postgres
Identity & SSO	Auth0 (Okta)	EU	Authentication, MFA

We enter Data-Processing Agreements (DPAs) with all sub-processors.

---

7. International Data Transfers

If limited support access outside the EEA is required, we rely on:

- **Standard Contractual Clauses (SCCs)** (2021/914/EU), plus
- Supplementary measures (encryption, RBAC, access logs)

8. Data Retention

Data type	Retention rule
Account data	While your account is active + 6 months (then hashed/anonymised)
Uploaded / generated project data	Until you delete it, or 24 months after last access
Logs & backups	90 days (logs), 30 days (encrypted backups)
Marketing consents	Until withdrawn + 12 months for audit

9. Your Rights

You have the right to:

- Access
- Rectification
- Erasure ("right to be forgotten")
- Restrict processing
- Data portability
- Object to processing based on legitimate interests
- Withdraw consent
- Lodge a complaint with IMY

Contact our DPO at **mate.szilcz@vitiscience.se** to exercise any right.
We respond within one month (Art. 12 GDPR).

10. Automated Decision-Making

We do not use automated decision-making or profiling with legal or significant effects (Art. 22 GDPR).

11. Children's Data

Our Services are not intended for children under 16.
We do not knowingly collect personal data from children.

12. Data Breach Notification

If a personal-data breach occurs, we will notify the supervisory authority within 72 hours and affected users without undue delay (Articles 33–34 GDPR).

---

13. Changes to This Policy

If we change how we process personal data, we will update this document and notify registered users by e-mail at least 30 days before changes take effect.
The version number and date appear at the top of this page.

---

14. Contact

Viti Science AB – Privacy Office
Stopvagen 91, 168 36 Stockholm, Sweden
E-mail: mate.szilcz@vitiscience.se
Phone: +46 (0) 72-171 95 05