Privacy & Data Protection (GDPR Compliance)

Effective Date: 14 December 2025
Last Reviewed: 14 December 2025

Fyrtorn Security AB ("Fyrtorn", "we", "us", or "our") is committed to protecting your personal data in compliance with the **General Data Protection Regulation (EU 2016/679, GDPR)** and Swedish data protection laws. This policy explains how we collect, use, store, and safeguard personal information.

1. About FYRTORN Security AB

Fyrtorn Security provides security consulting services to Swedish schools, including:

Security assessments

Training programs

Micro-learning platform

Our services may involve processing personal data of school staff and other individuals. This policy applies to all such processing, including data collected via our **School Nexus platform**, Micro-learning modules, security assessments, and consulting engagements.

Data Controller:

Organization: FYRTORN Security AB

Organisation Number: 559546-1533

Address: Östra Torpagatan 3, 553 30 Jönköping, Sweden

Email: info@schoolsecurity.se

Website: www.schoolsecurity.se

Contact Person: Marko Cabric, CEO

2. Personal Data We Process

We may collect and process the following categories of personal data:

2.1 School Staff Information

Full name and professional title

Work email address

Department or role within the school

Work contact number

2.2 Micro-learning Training Data

Module completion status and dates

Quiz and assessment results

Time spent on training modules

Progress tracking data

Certificate issuance records

2.3 Technical Data

IP addresses and device identifiers

Browser type and version

Login timestamps and session data

3. Where Your Data is Stored

Storage Platforms

Platform	Data Stored	Security Measures
Zoho Workspace	Client communications, contracts, invoices, CRM data	Two-factor authentication (2FA), encrypted storage, EU data centers
Google Workspace	Training materials, reports, internal documents	2FA, encrypted storage, EU data region
School Nexus	Micro-learning data, completion records, assessments	TLS encryption, secure authentication, EU-hosted infrastructure

All platforms comply with GDPR and store data within the **European Economic Area (EEA)** or under equivalent safeguards.

Platform Security Standards

Two-factor authentication (2FA) required for all accounts

Encryption of data in transit and at rest

Regular security audits (ISO 27001, SOC 2)

Automatic security updates and vulnerability patching

Activity logging and audit trails

4. Who Can Access Your Data

Access is strictly limited to authorized personnel based on the **principle of least privilege**.

Roles with access:

CEO / Data Protection Lead: Full access for governance and compliance oversight

Courses Facilitator: Access to training materials and results for course management

Access Control Principles:

Least privilege access

Quarterly access reviews

Immediate revocation upon role change or termination

Confidentiality agreements signed by all personnel

5. Legal Basis for Processing

We process your personal data under the following GDPR Article 6 legal grounds:

Performance of Contract (6(1)(b)) – to deliver and track training services

Legitimate Interests (6(1)(f)) – for service improvement, platform security, and aggregate training analysis

Legal Obligation (6(1)(c)) – to comply with Swedish law and regulatory requests

6. Purposes of Data Processing

We use personal data to:

Deliver and manage security training programs

Track and report training completion

Issue certificates of completion

Provide technical support

Analyse and improve training effectiveness

Maintain platform security

Comply with legal and regulatory requirements

7. Data Retention

We retain personal data only as long as necessary:

Data Type	Retention Period
Training records	Duration of service agreement + 3 years
Account/contact information	Service relationship + 1 year
Technical logs	Maximum 12 months
Contractual documents	7 years (Swedish accounting law)

Personal data is securely deleted or anonymized upon request or after service termination unless legally required to retain it.

8. Your GDPR Rights

You have the right to:

Access your data

Correct inaccuracies

Request deletion (where applicable)

Restrict processing

Receive data in a portable format

Object to processing based on legitimate interests

To exercise your rights: contact **info@schoolsecurity.se** or your school's designated contact. We respond within **30 days**.

9. Security Measures

We implement appropriate measures to safeguard personal data:

TLS/SSL encryption in transit and at rest

Two-factor authentication (2FA)

Role-based access controls

Regular security assessments

Staff training on data protection

Data processing agreements with sub-processors

Backup and disaster recovery planning

Incident response and breach notification

Strong password policies and credential rotation

10. Sharing Data

We may share personal data with:

Client Schools: Training completion reports for compliance

Trusted Sub-processors: e.g., Zoho, Google (EU-based with GDPR-compliant agreements)

Legal Requirements: When required by law or to protect rights and safety

We **do not sell personal data** or share it for third-party marketing purposes.

11. International Data Transfers

Data is primarily processed within the **EEA**. Transfers outside the EEA are protected by:

Standard Contractual Clauses (SCCs)

GDPR-compliant data processing agreements

EU data residency configurations

12. Data Breach Procedures

In case of a breach:

Assess scope and impact immediately

Notify Swedish Authority for Privacy Protection (IMY) within 72 hours if necessary

Notify affected schools without delay

Inform individuals if high risk exists

Document breach and remediation steps

13. Data Processing Agreements

When acting as a **data processor**, we enter into **Data Processing Agreements (DPA)** with client schools as required by GDPR Article 28. Schools can request a copy at any time.

14. Supervisory Authority

If you believe your rights are violated, you can contact:

Integritetsskyddsmyndigheten (IMY)

Box 8114, 104 20 Stockholm, Sweden

Website: www.imy.se

Email: imy@imy.se

15. Policy Updates

We may update this policy to reflect changes in our services or legal requirements. The **current version is always available** upon request.

16. Contact Us

FYRTORN Security AB

Marko Cabric, CEO

Östra Torpagatan 3, 553 30 Jönköping, Sweden

Email: info@schoolsecurity.se

Website: www.schoolsecurity.se

Organisation Number: 559546-1533