GDPR COMPLIANCE POLICY

cyber-sec.si and **academy.cyber-sec.si**

Version: 1.1

Last updated: 7. september 2025

TABLE OF CONTENTS

Executive Summary

This GDPR Compliance Policy describes the principles, procedures, and technical and organisational measures implemented by CYBER-SEC, informacijska in kibernetska varnost, d.o.o. ("CYBER-SEC") to ensure lawful, fair, and transparent processing of personal data on the cyber-sec.si website and the academy.cyber-sec.si learning platform. The document combines a public notice for individuals and an internal formal act to ensure compliance with the GDPR, the Slovenian ZVOP-2, and ZEKom-2 (cookies).

It includes:

- Types of personal data we collect
- Purposes and legal bases of processing
- Retention periods
- Technical and organisational security measures
- Individuals' rights and how to exercise them
- Personal data breach response plan
- Register of processors and international transfers (where relevant).

Statement of Applicability

This policy applies to all personal data processing activities carried out by CYBER-SEC in relation to:

- Main website: https://cyber-sec.si/
- Learning platform: https://academy.cyber-sec.si/
- Related services, user support, hosted content, event/training registrations, and enquiries.

All employees, contractors, and external processors must comply with this policy. Violations may result in disciplinary measures and/or legal consequences.

1. Privacy Policy

Controller

CYBER-SEC, informacijska in kibernetska varnost, d.o.o.

Tolstojeva ulica 41, 1000 Ljubljana, Slovenia

Tax ID (VAT No.): SI89630777 Registration No.: 9827021000

Email (data protection & requests): gdpr@cyber-sec.si

Contact point for data protection: gdpr@cyber-sec.si (A DPO has not been appointed because the company does not meet the conditions of Article 37 GDPR; this policy will be updated in case of changes).

Purposes and Legal Bases

• **Performance of a contract (GDPR 6(1)(b)):** creating/using user accounts, delivering courses, issuing certificates, processing orders/enquiries, service-related communications.

• **Taking steps prior to entering into a contract (GDPR 6(1)(b)):** preparing offers based on enquiries.

• **Legal obligations (GDPR 6(1)(c)):** accounting and tax compliance.

• **Legitimate interests (GDPR 6(1)(f)):** information security of systems, fraud/misuse prevention, service improvements, statistics using aggregated/anonymous data.

• **Consent (GDPR 6(1)(a)):** marketing communications, non-essential cookies/analytics.

Categories of Personal Data

- **Account/identity data:** first name, last name, email, interface language; hashed password.
- **Learning activity (Academy):** course enrolments, progress, test results, certificates, forum posts.
- **Payments/billing:** payer's name, billing address, transaction ID, payment provider, last four digits of card (via payment service provider).
- **Communications and enquiries:** message content, form data (e.g., company name, training interest).
- **Technical data and logs:** IP address (anonymised for analytics), session identifiers, device/browser data, cookie settings.

Recipients / Categories of Recipients

- **Hosting & infrastructure:** Hetzner (EU).
- **Email & productivity:** Microsoft Ireland Operations Limited (EU data centres where applicable).
- **Payments:** SaferPay → Worldline Financial Services Europe.
- **Analytics:** Google Analytics (Google Ireland Ltd.).

Processing by processors takes place under data processing agreements in accordance with Article 28 GDPR.

Retention

- Learning data (Academy): 1 year after last activity.
- Payment/accounting records: 10 years (per Slovenian tax regulations).
- Enquiries/communications: up to 2 years after conclusion of communication or earlier upon objection.
- Technical logs (web server, firewall): 90 days.
- Security incident logs: up to 12 months (or longer if necessary for incident investigation/legal obligations).
- After expiry of the periods, data are deleted or anonymised where appropriate.

Profiling and Automated Decision-Making

We do not carry out decision-making based solely on automated processing that produces legal effects concerning an individual.

2. Cookie Policy

Principles and Legal Basis

Essential cookies are required for the site to function (e.g., login, security) and are set without consent.

Non-essential cookies (e.g., analytics) are set only based on your explicit opt-in consent, as required by ZEKom-2, Article 225, and in line with the Slovenian Information Commissioner's guidance. The mechanism allows Accept all, Reject non-essential, and Settings (granular). You can withdraw consent at any time in the settings.

Categories

- Essential: authentication, security, session maintenance.
- Analytics: Google Analytics (with IP anonymisation).

Cookie Table

Category	Tool	Cookie name	Purpose	Retention	Provider
Essential	Session	PHPSESSID (or similar)	Maintaining login/session	Session	CYBER-SEC
Analytics	Google Analytics	_ga	Visit statistics (user ID)	2 years	Google Ireland Ltd.
Analytics	Google Analytics	_gid	Usage statistics	24 hours	Google Ireland Ltd.
Analytics	Google Analytics	_gat	Request rate limiting	1 minute	Google Ireland Ltd.
Analytics (pixel)	Google Analytics	collect	Device/behaviour data	Session	google-analytics.com

3. Data Retention Schedule

Data category	Retention period	Legal basis	Categories of recipients
Learning data (Academy)	1 year after last activity	6(1)(b)	Hetzner, Microsoft
Payment/accounting records	10 years	6(1)(c)	Microsoft
Letters/enquiries	Up to 2 years after closure	6(1)(b)/(f)	SaferPay / Worldline
Technical logs (web server)	90 days	6(1)(f)	Google Analytics
Security incident logs (EDR)	Up to 12 months	6(1)(f)	EDR solution

Data processing agreements under Article 28 GDPR are in place with all processors.

5. Technical and Organisational Measures (TOM)

- Privacy by design and by default (GDPR Arts. 5 and 25).
- RBAC/least privilege and audit trails.
- Encryption in transit (TLS 1.2+) and at rest (encrypted media/databases).
- Two-factor authentication for administrative accounts.
- Pseudonymisation/anonimisation for analytics.
- Regular updates, backups, and restore testing.
- Risk assessment and periodic reviews of TOM.
- Security of processing in accordance with GDPR Article 32.

6. Procedure for Exercising Data Subject Rights (DSR)

How to Submit a Request

Email gdpr@cyber-sec.si. (Contact forms on the site may also be used.) The request must enable identification of the individual.

Identity Verification

Appropriate verification (e.g., confirmation via the same email address, additional information; for Academy user accounts, verification via login/2FA).

Deadlines

Acknowledgement of receipt within 72 hours; response within 1 month of receipt (may be extended by 2 months for complex requests—we will inform you of reasons and any delay).

Rights

Access, rectification, erasure, restriction, portability, objection, withdrawal of consent (does not affect the lawfulness of processing before withdrawal).

Complaint to the Supervisory Authority

Information Commissioner of the Republic of Slovenia
Dunajska cesta 22, 1000 Ljubljana
Email: gp.ip@ip-rs.si · Tel: 01 230 97 30 · Website: https://www.ip-rs.si/

7. Personal Data Breach Response Plan

• **Detection:** via EDR and monitoring tools.

• **Containment:** system isolation, revocation of compromised credentials, disabling accounts.

• **Assessment:** types of data, scope, encryption/pseudonymisation, impact on individuals' rights and freedoms.

• **Notification:** to the Information Commissioner within 72 hours of becoming aware; to individuals without undue delay if there is a high risk to their rights and freedoms.

• **Documentation:** entry in the incident register, root-cause analysis, and corrective measures to prevent recurrence.

8. Consent and Preference Management

- Cookies: consent/withdrawal via the banner and “Manage consents” in the site footer (granular per category; non-essential cookies off by default).
- Marketing communications: explicit opt-in; unsubscribe via the link in emails or by replying.
- Recording proof of consent: timestamp, categories, banner/policy version.

9. Register of Processors

- Hetzner Online GmbH – hosting/infrastructure (EU).
- Microsoft Ireland Operations Limited – email services and productivity (EU data centres where applicable).
- SaferPay → Worldline Financial Services Europe – payments (EU).
- Google Ireland Ltd. – analytics (EU).

10. Statement on International Transfers

We use services that may involve transfers to third countries (e.g., when using certain functionalities of the Google/Microsoft group). In such cases, we implement appropriate safeguards, such as Standard Contractual Clauses (SCCs) and transfer impact assessments. Details are available upon request.