PRIVACY NOTICE

1. Who we are

The IT Project Security Compliance Management System (short form Security Compliance web application) is a web application that helps small IT project teams manage security requirements, compliance evidence and its review.

The system is operated by Polina Soroka as a prototype developed for bachelor thesis. Polina Soroka acts as the data controller for personal data processed in this instance of the system. Where an organisation deploys the system for its own projects, that organisation becomes the controller for the data processed in its deployment.

2. What data we collect

The system may process the following categories of personal data:

- **Account data:** first name, surname, email address, password (stored only as an Argon2id hash), and the secret used for multi-factor authentication.
- **Project membership data:** the projects a user belongs to and their role in each project (project manager, contributor, reviewer, auditor).
- **Invitation data:** the first name, surname, email address and role of a person invited by a project manager. This data is provided by the project manager, not by the invited person.
- **Compliance data:** security requirements, evidence files and links, review decisions and comments, and gaps. Evidence files, such as screenshots or documents, may contain personal data, for example names or account lists.
- **Activity records (audit log):** actions performed in the system, such as logins, failed login attempts, evidence submissions and reviews, role changes and report downloads, with the user and time of each action.
- **Technical data:** server logs, such as IP addresses, browser type and access times, used for security and troubleshooting.

3. Purpose and legal bases

Personal data is processed for the following purposes:

- To create and manage user accounts and provide access to projects (performance of a contract, Article 6(1)(b) GDPR).
- To manage security requirements and evidence, and to produce compliance reports (performance of a contract; for invited users, the legitimate interest of the organisation in demonstrating security compliance, Article 6(1)(f) GDPR).
- To keep an audit log of actions, so that changes to evidence, reviews and access rights can be traced (legitimate interest in the integrity and accountability of compliance information, Article 6(1)(f) GDPR).
- To protect the system against unauthorised access, including multi-factor authentication and temporary account lockout after repeated failed logins (legitimate interest in the security of the service and its users, Article 6(1)(f) GDPR).

4. How long we keep your data

- Account data is kept while the account is active. Deactivated accounts are anonymised once the user is no longer a member of any project.
- Project data, including requirements, evidence, reviews and the project's audit log entries, is kept while the project is active and, after the project is archived, for the retention period defined for that project. It is then deleted.
- Invitations expire after 72 hours, and password reset links after 1 hour.
- Backups are kept for 14 days, so deleted data may remain in backups for up to 14 days before it is removed.
- Server logs are kept for no longer than 6 months.

5. How we protect your data

The system implements the following technical and organisational measures:

- **Password hashing** with Argon2id, a minimum password length of 12 characters, and temporary account lockout after 5 failed login attempts.
- **Multi-factor authentication** with time-based one-time passwords for all users.
- **Role-based access control**: users can access only the projects they belong to and the functions permitted by their role.

- **Evidence files stored in private storage**, accessible only to project members through access-controlled downloads, with an integrity check based on a SHA-256 hash.
- **Approved evidence that cannot be modified**, and an audit log that cannot be edited or deleted.
- **Encrypted connections (HTTPS)**, secure session cookies and automatic logout after 30 minutes of inactivity.
- **Daily backups** of the database and evidence files.

6. Who we share data with

Personal data is not sold. Within the system, project data is visible only to members of the same project, according to their role. Outside the system, personal data may be shared only with:

- **The hosting provider** (Oracle Cloud Infrastructure, data stored in the EU region, Frankfurt, Germany), which hosts the application and its database.
- **The email service provider** (Brevo), used to send invitations and password reset links.
- **Public authorities**, where required by applicable law.

Any such sharing is limited to what is necessary for the stated purpose.

7. Cookies

The system uses only cookies that are strictly necessary for it to work: a session cookie to keep the user logged in, and a security cookie that protects forms against cross-site request forgery. No analytics or advertising cookies are used.

8. Automated processing

The system automatically calculates the status of security requirements from submitted evidence and reviews. These statuses concern requirements, not individuals, and the system does not make decisions with legal or similarly significant effects on users within the meaning of Article 22 GDPR.

9. Your rights under the GDPR

Subject to legal conditions, you have the right to:

- access your personal data;
- have inaccurate or incomplete data corrected;
- have your data erased, unless it must be kept, for example in the audit log of a project within its retention period;
- restrict processing;
- receive the data you provided in a portable format;
- object to processing based on legitimate interests.

You can view and correct your name, download your personal data and request deletion of your account on the “My account” page. To exercise your other rights, including restriction and objection, contact us using the details below. Records in the audit log are kept for the project’s retention period, because they are needed to demonstrate the integrity of compliance information, and are not erased on request during that period.

10. How to contact us

If you have questions about this notice or wish to exercise your rights, please contact:

- Contact person: Polina Soroka
- Email address: pol-na.soroka@knf.stud.vu.lt

You also have the right to lodge a complaint with a data protection authority. In Lithuania, this is the State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija).

Controller: Polina Soroka

Last updated: Novemeber 2026