seduo

TECH SPECS & SECURITY BASICS

Seduo is a multi-tenant web-based online education platform. Helps students to improve their skills in numerous areas of their professional career. Of course, in compliance with EU legislation. It' s secure. Effective. Comfortable.

Following document focus on company accounts and their users only.

Software as a Service

Seduo run as a SaaS (Software as a Service), which simply means:

- it is operated in a private cloud
  - require access to Internet
  - require web browser and/or mobile client (Android, iOs)
  - cannot be operated in house in customer IT environment
- it is located at multiple data centers due to high availability
- its servers & data are located in multiple data centers within the EU
- Alma Career as an Application Service Provider (ASP) ensures continuous operation

Personal Data Protection

Data we collect

For each student Seduo knows following personal data:

- name, surname, email address, name of business department and name of superior/manager (if particular information was provided)

From studying perspective Seduo also knows for each student:

- courses student started, finished
- courses assigned by administrator or superior / manager
- study plan of the student (if particular feature was used)
- last activity for each course
- positions in course, last lesson studied
- statistics of Seduo usage

In technical logs we collect also

- IP address of the incoming requests

Segregation of Roles

We recognize the following roles from the very nature of the user request handling:

- Customer Care [40+] - receives customer requirements and try to process (in the first line)
- Support [20+] - technical support staff (second line of processing pipeline)
- Business [20+] - to solve functional requirements for products, campaigns, etc. (3rd line)
- System administration [10+] - to maintain tech resources (servers, backups...)

Above described roles have to (or potentially may have) access to a part/complete user data. Indicative numbers of staffing may help to depict the size of support inevitably accessing personal data.

Access Restrictions

- User data can be accessed only by a restrictive group of authorized staff.
- Concerned to sensitive data, security measures always include a full track of operations and activities associated with the operator identity.

Consents and terms of the service

Each student (user) has to agree with the terms of the service in the first time of login. This is a standard behavior for non-company students. Besides this mandatory agreement in several scenarios optional consent of user to Alma Career with privacy data processing might be given as well.

User Personal Data Deletion

Deletion procedure of the personal data of users possible manually only. There is currently no automatic process. Deletion of user personal data is an irreversible step. Recovery of deleted student is not possible due to all related dat a is permanently anonymized.

There is an option to delete student in the list of students. The deleted student will disappear from all views in the application and exports.

There is no way behind this point, how to gather any info (including most of auditing info) about such a deleted user or related activities.

Technical Security Measures

- User access is provided by encrypted connection - only
- Non-production (development / testing) environment separated out of production - grade data
- User data confined within production, non-production uses synthetic/obfuscated data corpus
- Security - relevant activities on production systems are monitored, logged and timely evaluated
- Activation of components/services (per user request) is always validated at Alma Career side
- Seduo platform is continuously developed and tested (functionality and security together)
- Updates and patches are released on several days in week basis (or faster in case of a serious trouble)

Compliance (GDPR)

- Processing and protection of user data is ensured in accordance with EU legislation (GDPR).
- All detected breaches of personal data protection are reported to both the supervisory authority and the data subject within the reporting obligation (according to GDPR).
- The scope and content of the report is precisely specified by the legislation (EU Regulation 2016/679, Articles 33, 34), which we strictly follow.

The full text of the GDPR directive is available at European Commission official site at https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?uri=CELEX:32016R0679&from=CS

seduo

TECH SPECS & SECURITY BASICS

User Support

Support requests are collected and registered using HelpDesk and processed by Customer Care in the shortest possible time, obviously during common business days and hours (Mon - Fri, 08 - 17 CET).

Compatibility & Minimum Requirements

Web browser access

- Seduo is accessible through the web browser (it is compatible with major browsers - Firefox, Chrome, Explorer/Edge, Safari at least in last two versions)
- Support of JavaScript and cookies is required for proper functionality.

Mobile client access

- Android - if app is available in PlayStore for particular phone version
- iOS - phone only

SECURITY

Data in Transit

Web access allows HTTPS (encrypted) connections only.

- Supports protocol TLS 1.1, 1.2, 1.3
- The X509v3 SSL certificate is signed by trusted CAs (accepted by all major web browsers)
- The client certificate is not required

Separation of individual client sessions is ensured by the cookie mechanism.

All production system traffic in both directions is filtered and only HTTPS for user interaction and encrypted access (SSH protocol with key authentication) for maintenance / updating of the application is enabled.

seduo

TECH SPECS & SECURITY BASICS

Authentication

Student user's authentication (Sign-in) involves a single-factor, form-based (user/password) mechanism.

Company administrators and managers of Seduo are accessing their Seduo administration via time limited one-time hash-based login. Hash is sent to user email from login gateway.

Student accounts are treated as individual (Alma Career strongly discourage to share accounts among multiple users). The plain text password is never stored and is present only in-memory at the time of user login in. Passwords are stored only hashed. The hashing algorithm is continually modified to respond to the changing state of technology.

Logon parameters must meet password policy. The current setting follows:

- The username is an email address.
- The minimum enforced password length is 8 characters.
- The password change is not enforced (i.e. the password does not expire), therefore the history of the used passwords is not recorded.
- The password hashing algorithm is bcrypt, 1M iterations, "salted" individually per account.

Authorization (Roles) in Company administration

Particular user actions are authorized based on predefined role granted to the individual user. Self-care role management is administered by mandated users of each tenant (registered company space) individually.

The following user roles are defined:

- **Administrator** - role has access to the all managers, students and can see their studying). Can create managers, can import new students, delete students, assign courses to be studied and export statistics etc.
- **Manager** - role has an access only to specified group of students in particular company. Can see studying progress, assign new courses, create

study plan and see group statistics. The student group is defined by Administrator.

Data at Rest

Seduo code runs in docker containers as PHP or Node application built-up on the top of hardened Linux operating systems.

All components run virtualized (OpenStack) on the private cloud solution due to high-availability and fast disaster recovery options.

Data are kept in the PostgreSQL databases.

Data are continuously synchronized and mirrored to multiple locations, also backup is made on the regular basis.

Backup takes place according to a defined plan (retention is implicitly set for 14 days):

- Transaction log backup is ongoing (to ensure data recovery within 8 hours far from the crash)
- Snapshot of the cloud platform takes place daily
- Full data backup data runs weekly

Multi-level backup system is used:

- Online replication of data to multiple locations
- Backup of private cloud itself
- Internal backup systems

Monitoring & Supervision

The operations monitoring runs continuously (24x7).

The status is supervised (and any issues notified) daily (07-22 CET):

- External monitoring services together with internal systems are employed to check the status

seduo

TECH SPECS & SECURITY BASICS

Auditing

Audit records are taken as a track of all significant activities of the users. Audit (logging) is layered, descending from the application level to the system as follows:

- History (of user activities) - Postgres DB (permanent)
- Application log – Seduo use Graylog (records are stored max. 6 months)

Development Cycle

The development, integration and testing environments are fully virtualized and run on a private cloud platform. The environments are logically split (by firewalling). Access rights to different environments are different. Mentioned again, the production environment is fully separated (physically) from non-production environments.

Planning, development and testing of any updates/new releases of Seduo takes place in the framework of agile development (We cycle using weekly or bi-weekly SCRUM's sprints).

All used components (including in-house developed) are tested for stability, availability, and security prior to production deployment, so that vendor / platform manufacturer support is always maintained.

In the case of identified security flaws, updates (patches/fixes) are applied after testing in the shortest possible time.

Testing takes place in a continuous and multi-level development:

- Prior to accepting any change in the source code, a developer review (local Lint and four-eye control principle) takes place.
- In the framework of code quality control, static code analysis is performed (using the code review instruments).
- Regular (annual) independent assessment of application security (through penetration testing) is also carried out by a specialized 3rd parties.

Passed tests will open release management process to move the new code to production. This is fully automated (no hand-intervention allowed) deployment process with full audit track (to ensure rollback to the last good version, when deployment fails).

Each record is tied with the timestamp and the user identity. Records are kept in the log(s) for the period specified for particular audit track.

Security Assurance

All the main principles, measures and technical solutions used to safely develop and operate Seduo and protect personal user data are listed on this page.

Upon request, we provide our business partners with a detailed description of Alma Career security measures in the format defined by the ISO/IEC 27001.

This level of providing security information to third parties is final (no further security info, like Test Reports, Internal Security Guidelines etc. are provided outside Alma Career).

As a matter of principle, we do not provide other materials or greater detail of our security measures.

****

This document was updated January 11, 2024. In case of any comment, please contact *Alma Career* data protection officer of the country where you have contract at the following e-mails *dpo-cz@almacareer.com, dpo-sk@almacareer.com, dpo-pl@almacareer.com*