Whistleblower system

Application

The LES Whistleblower Platform is fully managed by Tempus Serva ApS.

The system supports the following roles and usecases

- Case Triager: Assignes cases to applicable lawyer
- Lawyer: Handles whistleblower cases
- Tenant user: Handles whistleblower cases
- Whistleblower: Anonoumous users that creates new cases

Whistleblower has the option to return to his/her case, using a randomized code generated during the report process.

Backup

Backups are securely stored in a redundant environment. Data is stored in encrypted form and adequate measures enable recovery in case of system failure or interruption. The environment is backed up as follows:

- **A) Daily** full server backups, stored for 30 days, after which they are overwritten.
- **B) Monthly** full server backups, stored for 3 months, after which they are overwritten.

The purpose is to ensure that Recovery Point Objective and Recovery Time Objective for environments are 24 hours where possible. For data recovery older than 60 days, a time frame of at least 72 hours is required.

Hosting Setup

The LES Whistleblower Portal is hosted by Amazon Webservices EC2 in the data center in Stockholm, which complies with the following standards PCI DSS 3.2 Level 1 Service Provider, FIPS 140-2, ISO 27001. The server is protected by 2 layers of firewalls and utilizes the following supported services:

- SSL certificates are automatically updated monthly from LetsEncrypt
- UptimeRobot polls the server each minute checking: Access to database, Storate- and RAM-sufficiency
- Database is dumped nightly, replicated to encrypted storage in EU
- Office365 SMTP service for sending emails

Security Setup

The following security and compliance features are enabled and active:

- **Password policy** The enabled policy forces users to create passwords based on the following minimum criteria: Minimum 8 characters, Must contain uppercase and lowercase letters, Must contain numbers, Must contain special character(s).
- **Multi-factor authentication** Access to case management for attorney/lawyer at LES (ombudsman) and contact persons in the company, respectively, is protected with a username and password, followed by a randomized, session-specific OTP (One-Time-Password) sent to the users mobile phone as either a regular or Flash SMS, to verify the user's identity.
- **Storage encryption (AWS + LUKS)** Storage is encrypted with LUKS (Linux Unified Key Setup – 256-bit AES disk encryption). Thus, persons with physical access to hardware cannot access stored data.
- **Encryption During Transmission** Communication is protected with SSL certificates and HTTPS (TLS). Numeric suites for HTTPS are continuously updated.
- **Activity and data logging** Activity and Data Logging is enabled. However, IP logging on server requests is deliberately disabled to ensure the anonymity of external users.
- Versioning
- **GDPR Deletion Policies** In accordance with applicable data protection rules, archived data is automatically anonymized after 60 days. In order to ensure an independent fourth party, a written agreement has been entered into that the sub-data processor may not give LES users access to the server and backend.
- **Event and system logging** Is enabled to automatically log unsuccessful login attempts, system events, user errors, etc.
- **Scrubbing of files** All files uploaded via the portal are cleaned of personally identifiable meta-data such as name, initials, geotags, etc. LES Whistleblower Portal supports all common file formats, including: MS O ce files, PDF, image formats like PNG, JPG, BMP etc., as well as media files MP3 and MP4.

See Security setup for additional information on security and compliance features available on TS No-code Platform.

Technology Stack

The technological stack consists of:

- LES Whistleblower Portal
- TS No-code Platform
- Apache Tomcat
- MySQL
- Amazon Linux 2