Envoria - Technical and Organizational Measures

Version: 21.08.2025

Introduction

The processor ensures an appropriate level of protection for the specific commissioned data processing. This is described as follows:
Order processing in accordance with instructions is ensured through the technical and organizational separation of responsibilities between the controller and the processor. Commissioned data processing only occurs in exceptional cases through services such as system setup, support, training, software development, or reproducing application functionality.

The SaaS Solution

To operate its cloud infrastructure, Envoria relies on established data center and cloud service providers. The hosting environment is operated within modern, cloud-based data centers provided by Exoscale (for the Envoria platform) and Hetzner Online GmbH (for Contavio). This infrastructure is located within the European Union or in countries that have been granted an adequacy decision by the European Commission.

Further details on the security standards and measures of the cloud providers can be found on the official security pages of Exoscale and Hetzner Online GmbH.

Overview

The processor implements the following technical and organizational measures to ensure data security in accordance with Art. 32 GDPR:

Physical Access Control

- The processor's business premises are located in an office building. The entrance door is secured by a locking system.
- Access rights for employees and third parties are implemented and documented.
- Cleaning personnel are carefully selected.
- Access to the data center is logged, monitored, and traceable.
- Reception staff is present at the entrance.
- Mandatory visitor registration.
- Visitors are only permitted when accompanied by an employee.
- Security personnel are present outside regular working hours.
- Cleaning personnel are selected with care.

System Access Control

- Authorization concept defined by the system administrator
- Password policy including rules on length and complexity
- Secure storage of data carriers
- Physical erasure of storage media before reuse
- Proper destruction of data carriers
- Login with username + password + optional 2FA

- Login with biometric data
- Automatic desktop lock
- Management of user permissions
- Creation of user profiles
- Secure password policy
- Data deletion and destruction policy
- Clear Desk and Clear Screen policy
- Instructions for manually locking the desktop

Data Access Control

- Access to data is restricted by differentiated user permissions
- Assignment of user rights and profiles with password protection
- Authentication via username and password
- Automatic logout after periods of inactivity, with re-authentication required
- Use of antivirus software, firewall software, and, where appropriate, VPN technology
- Logging of access events
- Implementation of permission management concepts

Data Separation Control

- Physical separation of data on different systems or storage devices
- Development of an access rights concept
- Separation of production and test systems
- Control through the permission management system

Pseudonymization and Encryption

- Pseudonymization is not applied, as original data is needed to reproduce software issues under realistic conditions.
- Disk encryption is implemented using Windows standard tools.
- Data transfers over the internet are always encrypted using state-of-the-art technologies or secured via modern access-controlled file exchange platforms.
- Internal guideline: whenever data is transferred or after legal retention periods expire, personal data should be anonymized or pseudonymized wherever possible.

Transmission Control

- Dedicated connections or VPN tunnels are established only with the controller's involvement
- Email encryption
- Logging of data transfers
- Provision of data only over encrypted channels (e.g. HTTPS)
- Documentation of recipients and scheduled retention/deletion periods
- Careful selection of transport routes
- Careful selection of personnel

Input Control

- Overview of which programs process which data
- Use of personalized user accounts only – no generic accounts

Availability Control

- Fire and smoke detectors installed in the building
- Backup & recovery concept in place
- Regular verification of backup processes
- Regular testing of data recovery procedures, including documentation of results
- Backup media stored at two geographically separate locations

Review, Evaluation, and Assessment

- Regular or ad-hoc review of the effectiveness of technical security measures
- Appointed data protection officer
- Employees are trained and bound to confidentiality and data secrecy
- Regular employee awareness training, at least annually
- The organization fulfills its information obligations under Articles 13 and 14 GDPR
- Documentation of security incidents and data breaches
- No more personal data is collected than is necessary for the intended purpose
- Easy technical means for data subjects to exercise their right to withdraw consent

Order Control

- Prior review and documentation of the processor’s implemented security measures
- Careful selection of the processor, especially regarding data protection and data security
- Conclusion of required data processing agreements
- Written instructions provided to the processor
- Confirmation that processor employees are bound to data secrecy
- Obligation for the processor to appoint a DPO if legally required
- Agreement on effective audit rights
- Provisions regarding the involvement of subprocessors
- Ensuring the deletion or return of data after the end of processing