Technical and organisational measures
according Articel 32 par. 1 GDPR

(Revision November 2022)

1. Access control

- Use of alarm systems incl. motion detectors (Ulm site)
- Documented key management (keys are only issued to employees)
- Visitors
    - Visits only during visitor hours (regular business hours); exceptions only with prior approval
    - Supervision of the visit (i.e. only accompanied)
- Logging concept
    - Access to server and remote maintenance room only with dongle or key (group of persons strongly restricted)
    - Access control system to the remote maintenance room
    - Documentation of access to the remote maintenance room
    - Evaluations of the access control system
- IT server administration
    - Exclusively by the IT department

2. Permission control

- Existing authorization concept for granting rights to enter, change and delete data (regulated by Active Directory)
- Authentication with user name / password
- Assignment of user rights
- Administration of rights by system administrator
- Number of administrators reduced to Team Operations
- Access authorization concept
    - Instruction of all employees in the use of authentication procedures and mechanisms (declaration of consent to IT policy)
    - Regulated process for central administration of user identities, in particular for creation (e.g., new employees), changes (e.g., name change after marriage) and deletion (e.g., employees leaving)
    - Assignment of unique identifiers for each user
    - As far as possible, automatic implementation of the password policy for strong passwords within the framework of the IT policy for Active Directory in the systems with user IDs
    - Passwords are also blocked after a security incident, even if suspected, and must be reassigned by the user
    - When a new user logs in for the first time or the password is reset by IT (e.g. if the password is forgotten), the user must change the password.

- Passwords must not be passed on (not even to colleagues, superiors or the IT department) - in exceptional cases (e.g. prolonged illness) the password is reset by IT and this process is documented
- Inform employees that passwords may not be recorded on slips of paper or bulletin boards (IT policy)
- Do not send passwords by e-mail
- Automatic blocking over 60 minutes of accesses in the event of five failed attempts due to incorrect password
- Showing the number of failed logins for a user who successfully logged in
- Passwords in the relevant databases are not stored in plain text, but appropriate cryptographic methods are used
- Clocks of the information processing systems used (PCs, notebooks, etc.) are synchronized with suitable time sources to enable targeted analysis in the event of security incidents.

3. Data access control

- Exclusive access by authorized persons to corresponding/subordinate data. Annexes 1 and 2 of the employee agreement stipulate that personal data must not be read, copied, modified or removed without authorization during processing, use or after storage.
- File shredder, external file shredder, physical deletion of data media before disposal
- Regulations for the administration of roles (assignments, revocation) via Active Directory
- No administrative identification for users who do not perform any administrative activity
- Only competent and instructed persons are allowed to perform administrative activities on the servers
- Where possible and necessary, use of two-factor authentication procedures for applications that support this, especially for administrators;
- Agreement of a confidentiality obligation in the external service contract

4. Transfer control

- No disclosure to third parties other than the named subcontractors
- Encryption concept for documents containing personal data
- Remote maintenance for client IT administration purposes exclusively via encrypted connections after authentication by the administrator and release by the user
- Process for effective data deletion before handing over a terminal device to another employee
- A security concept for the use of printers, copiers and multifunction devices is in place (e.g., no unauthorized viewing of printed documents, adequate protection of stored information, proper disposal)
- When using remote maintenance software: Regularly install security updates and pay attention to information about known vulnerabilities or misconfigurations.
- Logging of remote maintenance by external service providers and limiting access only to the system to be maintained.
- Archiving concept
- Regulation on the obligation to retain data
- Do not archive data on media that are unsuitable for long storage periods.

5. Separation control

- Separation of productive and test environment
- Logical client separation (CargoFleet 3)
- Control via authorization concept
- Use of qualified data medium management
- Deletion period

6. Order control

- Personal data are processed only in accordance with the instructions of the customer
- Clocks of the information processing systems used (PCs, notebooks, etc.) are synchronized with appropriate time sources to enable targeted analysis in case of security events
- Systems are monitored using appropriate monitoring tools
- Monitoring processes are continuously adapted to the system
- Maintenance work is announced to the customer in advance

7. Availability control

- In case of failures, operation is informed via 24/7 support
- 24/7 support of the hoster in case of hardware failures
- Emergency plan for business continuity: regulations on which systems are restored in which order, which (external) persons/service providers can be consulted in the event of an emergency, and reporting obligations
- Regular review of the emergency plan
- Written backup concept
- Execution of backups
- Suitable physical storage of backup media (safe)
- There is a fire protection concept
    - Use of fire/smoke detection systems (as part of the fire protection concept)
    - Fire-retardant cabinets/vaults for storing essential components
    - Regular inspection, especially infrastructure
    - Fire extinguishers
- Use of equipment to ensure power supply to server systems (uninterruptible power supply, UPS), especially in the event of short-term power failures or fluctuations
- Use of backup and synchronization mechanisms to prevent major loss of data in the event of loss, damage or theft
- Security precautions due to attacks when using website and web applications
    - Use of HTTPS protocol according to the state of the art (TLS1.2 or TLS1.3) (Art. 25 par. 2 GDPR)
    - Remote access to web servers only with encrypted connections
    - Only trained or competent persons are allowed to perform administration activities on the servers
    - Regulated process for information about security updates and prompt installation of the same, especially for common content management systems (CMS)
- Security precautions due to attacks on the network
    - Use of a firewall at the central Internet gateway
    - Blocking of all services that are not required
    - Use of a web proxy through which all HTTP connections must pass (Art. 25 par. 2 GDPR)

- Use of suitable firewall architectures to secure purely internal systems (e.g. workstation, printer) to servers accessible via the Internet (e.g. mail server; web server, VPN endpoint)
- Use of WLAN guest access without access to the internal network
- Checking e-mails using anti-malware protection
- Blocking of dangerous e-mail attachments
- Connection of branch offices or home offices via strongly encrypted VPN connections with client certificate authentication
- Use of anti-virus software on clients

8. Privacy by Default and Privacy by Design

- Software development and selection
  - Restricted access to source code governed by Atlassian software
  - Standard software and corresponding updates are obtained only from trusted sources

9. Organisational measures for all areas

- Obligation of employees to maintain data secrecy
- Data protection training for employees promptly after commencement of employment
- Guidelines e.g. on e-mail/internet use, handling of damage reports
- Sensitization of employees who interact with external parties such as suppliers with regard to appropriate rules of engagement, guidelines, processes and behavior (e.g., what data may be disclosed and in what form, what may be security-critical)

10. data protection and data security management

- Data protection concept with corresponding measures has been drawn up

The following are available in writing

- - Internal rules of conduct: IT consent declaration
- - Special agreement on working in the mobile office
- - Risk analysis
- - Comprehensive data security and data protection concept
- - Recovery concept
- - Certificate: ISO 9001:2015
- - Certification Authority: EQZert
- - Other: Measures subprocessors (InterNet X, Microsoft Deutschland GmbH, MECOMO Aktiengesellschaft)