make
formerly Integromat

Technical and Organisational Measures for Make

This document describes the requirements and implementation of measures for secure and compliant processing of personal data. It considers Articles 24, 25, and 32 GDPR where applicable.

1. Confidentiality

1.1 Entry control

Requirements: Rooms in which personal data are processed or data processing systems are installed are not freely accessible. They are locked when employees are absent. Entry authorization is assigned on a need-to-know basis according to an established process and is reviewed for necessity at regular intervals. Rooms in which data processing systems are located (computing centre, servers, network distributors, etc.) have special entry protections and may be accessible only to IT administration employees (possibly management). Devices must be stored in appropriate locked cabinets. Visitors and non-company persons must be registered through an appropriate and documented process and are monitored while in the office space.

Make has implemented the requirements in the following manner:

X	Locked building	X	Locked building
X	Locked offices	X	Locked offices
X	Electronic security locking system	X	Electronic security locking system
X	Mechanical security locking system	X	Mechanical security locking system
X	Documented key issuance	X	Documented key issuance

1.2. Access control

Requirements: For every IT Service or system user, a personally assigned user must be set up with an at least 10-character password including upper and lowercase letters, numbers, and special characters. The system must require users to change passwords at least every 120 days. The network users must agree in documented form to comply with the user access guideline. A documented procedure is required when setting up, changing, and removing access authorization. All assigned access authorization must be documented and reviewed routinely regarding necessity. IT Service and System access to data must be monitored and logged, including any unsuccessful login attempts. The system must block any IT Service and System access automatically after no more than 10 failed login attempts.

Make has implemented the requirements in the following manner:

X	Complex Passwords	X	Secure line connection for external access (VPN)
X	Central authentication	X	Use of an up-to-date firewall
X	Access blocked after too many incorrect password entries	X	Multifactor access control

1.3 Usage control

Requirements: A documented, role-based authorization concept exists for use of personal data that limits use so that only authorised persons can use the personal data necessary for their job (minimization principle). The password rules from access control are also implemented for usage control. Administrative tasks must be limited to a small group of administrators. The tasks of administrators are monitored and logged to the extent technically feasible.

Make has implemented the requirements in the following manner:

X	Role-based authorization process	X	Protected access to data storage media
X	Application-specific authentication with username and password	X	Destruction of paper documents in compliance with data protection law
X	Logging user access and data processing	X	Encryption of mobile data storage media
X	Allocation of authorizations only after approval by the data owner	X	Restriction of Admin users incl. appropriate documentation

1.2. Access control

Requirements: Personal data must be separated by means of various storage locations or client separation.

Make has implemented the requirements in the following manner:

X	Separation of productive and test systems	X	Logical client data separation within the data processing system

2. Integrity

2.1 Transmission control

Requirements: During transmission control, it is necessary that only authorised persons can view the personal data. For transmission by email, protective actions (e.g., encryption of communication between the email servers) are required. Mobile devices or mobile storage media must be encrypted if personal data are stored on them.

Make has implemented the requirements in the following manner:

X	Communication end-to-end encryption (e.g. TLS)	X	Special protection when physically transporting data storage media
X	The use of private data storage media is prohibited		A VPN Connection is needed when accessing system critical resources from outside of the corporate network

2.2 Input control

Requirements: It must be possible to assign the input, modification, and deletion of personal data to the employee performing the task. The system must limit the modification and deletion of datasets to effectively prevent accidental modification or deletion.

Make has implemented the requirements in the following manner:

X	Traceability when assigning, changing and deleting user authorizations

2.3 Contractual order control

Requirements: In terms of contractual order control, it is necessary that the data processing procedures carried out on a subcontracted basis take place exclusively at the instruction of the Controller. To that end, the individuals involved in data processing must be trained and provided with instructions. Outsourced processing must be monitored through internal controls. The results of the controls are documented.

Subcontractors may be hired only on the basis of the rules agreed with the Controller. Transmission or use of personal data may only take place after the subcontractor has signed an outsourced processing agreement pursuant to Article 28 GDPR and has confirmed compliance with the rules of the data protection concept. The contractor’s duty to supervise its subcontractor is based on the outsourced processing agreement entered into with the Controller.

Make has implemented the requirements in the following manner:

X	Documentation of processing activities	X	Appropriate monitoring of the processor
X	Careful selection of processors (detailed assessment of provided guarantees)	X	Assuring compliant destruction or return of data upon completion of the assignment
X	Written agreement with the processor on the data protection minimum standard		

3. Availability and reliability

Requirements: Personal data must be processed on data processing systems that are subject to routine and documented patch management. Systems may not be connected within the network that are outside the maintenance cycles of the manufacturers. Security-related patching must be initiated within 72 hours after they are released. Redundant storage media and backups must be used to ensure continuous availability of personal data based on the latest technical standards. Computing centres and server rooms must meet the technical standards (temperature regulation, fire protection, flooding, etc.). The servers must have an uninterruptible power supply (UPS) allowing a controlled shutdown without loss of data.

Make has implemented the requirements in the following manner:

X	Regular patch management for servers	X	Physically separate redundant data storage or backup data
X	Regular patch management for end devices	X	Uninterrupted power supply
X	Initiate security-critical patches within 72 hours	X	Early fire detection in office buildings
X	Recovery procedures are established and tested at least annually		

4. Procedure for routine review, assessment, and evaluation

Requirement: A procedure must be implemented for monitoring data protection at the company. This procedure must include an agreement by employees to maintain data secrecy, training and education of employees, and routine auditing of data processing procedures. Likewise, the processing procedure carried out for the Controller must be documented before the start of data processing. A thorough reporting and management process must be introduced for data breaches and the protection of the rights of data subjects. This process must also include notification of the Controller.

Make has implemented the requirements in the following manner:

X	Appointment of Data Protection Coordinator	X	Regular auditing of the procedures
X	Regular documented training of employees involved in data processing	X	Regular review of the latest technical standards pursuant to Article 32 GDPR
X	Documented procedure for introducing, modifying, and discontinuing procedures	X	Regular auditing or other suitable verifications of the processors