TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING PERSONAL DATA SECURITY

Meetpoint d.o.o. has implemented the following technical and organizational measures to ensure an adequate level of personal data security, while taking into account the nature, scope, context and purpose of the processing, as well as the risks to the rights and freedoms of natural persons:

I. Measures for ensuring personal data confidentiality

I./1. Facility access control

The purpose of facility access control is to prevent unauthorised individuals from gaining access to the facility where personal data is processed. Facility access control is carried out primarily using the following measures:

1. Reception desk in the office building, with receptionists on duty every business day from 8:00 a.m. to 4:00 p.m.; outside business hours, the office building is protected by a contracted security service.
2. Controlled access to business premises:
   - All external visitors are required to schedule a visit and register at the reception desk upon arrival by providing their name and surname and the reason for their visit. When departing, visitors are required to notify the reception desk.
   - The doors to the offices are locked at all times. Visitors must ring the bell to be admitted to the offices. When entering the offices, the visitor must be accompanied by an employee.
   - The maintenance and cleaning staff accessing the premises are registered by name.
3. The office building is protected by an alarm system.
4. Video surveillance of the office building:
   - Office building video surveillance covers the areas of the reception desk, stairwells and the parking garage.
   - Video surveillance is operated by the building manager.
5. Key and access card management
   - Each employee has their own access card used for entering the office building. The office is locked with a key that every employee has.
   - Lockers are locked and access to keys is restricted to certain employees only.
   - If an individual's employment is terminated, they must return the access card and key.

I./2. Computer access control

The purpose of computer access control is to prevent unauthorised persons from using computer systems for processing personal data. Computer access control is carried out primarily using the following measures:

1. Firewall and intrusion detection system.
2. Antivirus software is installed on all workstations by default.
3. Automated software updates (e.g. operating system, anti-virus software, browsers) are enabled by default.
4. Each employee has their own password-protected workstation.

5. Employees are required to lock workstations when not using them.
6. The screensaver password is set to lock the computer automatically after 3 minutes if the employee fails to lock the workstation.
7. Every tool we use for our business has a secure login that requires a username and password.
8. Minimum password requirements and password management:
    - Passwords must be longer than 6 characters and contain 1 upper case letter and special character.
    - Passwords must be changed at least once every 3 months.
    - Employees are prohibited from lending passwords or using group passwords.
9. In the event of termination of employment, the individual's access to all systems will be terminated.

I.3. Data access control

Data access control includes measures to ensure that users of data processing systems can access data on the basis of the access permissions granted and that data is not subject to unauthorised reading, copying, modification or deletion during processing, use and storage. Data access control is carried out primarily using the following measures:

1. Access to systems containing personal data is based on user accounts so that access requires a username and password.
2. The company appoints employees responsible for individual personal data filing systems. The users who have permission to access individual personal data filing systems are appointed.
3. Employees can only access the data they need to perform their work tasks and on a need-to-know basis.
4. The company separates between administrator and user roles. Only the administrator has full access to the systems, while users can only access data on a need-to-know basis.
5. We regularly review the scope of user rights and restrict them on the basis of the principles of necessity and minimisation.
6. We have implemented the four-eyes principle, which means that individual persons cannot gain access to systems or data without authorisation from a responsible person.
7. Software development is based on the "principle of data protection by design and by default".
8. We provide a basic audit trail for the processing of personal data (e.g. for modification, access, and deletion). We ensure that the processing logs are subject to the required retention periods.
9. The Meetpoint platform encrypts stored personal data (encrypted databases).
10. Data is deleted from the Meetpoint platform by deleting data from the database.
11. Data from storage media (e.g. computers that have been written off) is permanently erased before they are written off.
12. Internet access is encrypted using the https protocol. Users access servers via Citrix SSL-VPN.

I./4. Separation control

Separation control includes measures to ensure that data collected for different purposes is processed separately. Separation control is carried out primarily using the following measures:

1. By physically separating data and storing it on separate systems or storage media.
2. By separating the development, test and production environments.
3. By software-based logical separation of users.

II. Measures for ensuring personal data integrity

II./1. Transmission control

Transmission control includes measures for ensuring personal data cannot be subject to unauthorised reading, copying, modification or erasure during electronic transmission or storage. Transmission control is carried out primarily using the following measures:

1. Documents are protected with passwords.
2. VPN tunnels.
3. Data encryption.
4. Firewall and anti-virus protection as described in section I./2.

II./2. Input control

Input control includes measures that make it possible to go back and check and establish whether the personal data entered into data processing system has been modified or removed (input control) and by whom. Input control is carried out primarily using the following measures:

1. We provide a basic audit trail for personal data processing.
2. Employees can only access the data they need to perform their work tasks and on a need-to-know basis.
3. Access to systems containing personal data is based on user accounts.

III. Measures for ensuring personal data availability

Availability control includes measures for ensuring data is protected against accidental destruction or loss. Data availability control is carried out primarily using the following measures:

1. We back up data:
   - The backup interval: 24 hours.
   - Backup copy retention period: 3 months
   - Backups are stored in a remote location and are password-protected.
2. A smoke and fire detection system is installed in the building.
3. Firewall and anti-virus protection as described in section I./2.

IV. Organisational measures

IV./1. Employees and contractors

1. Recruitment procedures are set up for careful selection of employees (for example, a detailed CV is required along with a job interview with additional questions).
2. Employees who process or have access to personal data sign a written statement to ensure confidentiality when it comes to personal data processing.
3. Employees know how to identify social engineering attacks.
4. Employees adhere to a password policy.
5. Employees comply with the clean-screen, clean-desk policy.

6. Employees are trained to raise awareness about security and privacy:
    - Every new employee must complete the “Secure in the Office” webinar available at https://www.varnivpisarni.si/. Certificates of completed webinars are kept on file.
7. We have processes in place to carefully select service providers and monitor their performance. We have concluded appropriate data processing contracts with sub-processors, which include appropriate technical and organisational security measures and the right to perform reviews and audits.

IV./2 Auditing technical and organisational measures

1. We review the effectiveness of technical and organisational measures at least once a year. We introduce new measures or adapt existing ones to address any identified weaknesses.

IV./3. Actions in the event of a personal data breach

1. If we become aware of a personal data breach, we will notify the controller in writing without undue delay and at the latest within 24 hours of becoming aware of the breach. The written notification will include:
    - the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects and the types and approximate number of personal data records;
    - the likely consequences of a personal data breach;
    - the measures that the controller should undertake or that we propose the controller takes to address the personal data breach, as well as, where appropriate, measures to mitigate any adverse effects of the breach.
2. The notification will be sent by email to the address of the Data Protection Officer of the controller or to another contact person if the controller does not have a designated Data Protection Officer.

Ljubljana, 01.03.2023

Meetpoint d.o.o.