PARAGON
Customer Communications

Technical and organizational measures for the protection of personal data

in relation to Act 110/2019 Sb. processing of personal data,
and Article 32 EU Regulation 2016/679 (GDPR)

Content:

Records of document review:

Date:	Result:	Reviewed by:
18.6.2018	Update of screen lock according new policy	Z. Sedlák
25.6.2019	The overall revision after the entry into force of Act No. 110/2019 Sb. processing of personal data	Z. Sedlák
25.11.2019	Added description of VLAN separation	Z. Sedlák

1 Scope

Applies to all employees and persons working for or on behalf of the organization and managed by organization (also referred to as employee or person).

2 Legislative Framework

2.1 Act 110/2019 Sb. Processing of personal data

§ 40 - Securing the processing of personal data

(1) The managing authority shall take such organizational and technical measures to ensure the level of security of personal data appropriate to the nature, scale, circumstances, purpose and risk of their processing.

(2) Where personal data are processed automatically, the managing authority shall take the necessary measures to ensure that:

(a) secure such personal data from unauthorized access, transmission, alteration, destruction, loss, theft, misuse or other unauthorized processing;

(b) to ensure the recoverability of such personal data;

(c) to provide the possibility to identify and verify the person who has entered the personal data or which has been transmitted or made available through the data transmission facility;

(d) to ensure the security and reliability of the information system containing such personal data, including error reporting;

(e) to prevent the unauthorized access to the medium of such personal data or to the equipment used for its processing.

(3) The management body's obligations set out in paragraphs 1 and 2 apply to processors as well.

§ 46 - Obligations of persons in securing personal data

(1) The Administrator shall take such technical and organizational measures to prevent unauthorized or accidental access to, alteration, destruction, loss, unauthorized transmission or other unauthorized processing or misuse of personal data. This obligation also applies after the processing of personal data.

(2) The controller is obliged to take technical and organizational measures to ensure the protection of personal data in accordance with the law and other legal regulations. The Administrator shall keep documentation of the technical and organizational measures taken, which shall be kept for the duration of the processing of personal data.

(3) Within the framework of the measures referred to in paragraph 1, the controller shall assess the risks related to the areas

(a) a compliance with the instructions for processing personal data by persons having immediate access to personal data;

(b) to prevent unauthorized persons from accessing and processing personal data

(c) to prevent the unauthorized reading, creation, copying, transmission, modification or deletion of records containing personal data

(d) measures to identify and verify to whom personal data have been transmitted.

(4) In the case of automated processing of personal data, the controller shall also be obliged under the measure pursuant to paragraph 1

(a) to ensure that only an authorized individual uses the system for the automatic processing of personal data;

(b) to ensure that an authorized natural person has access only to personal data corresponding to his or her authorization, on the basis of a specific user authorization established solely for that person,

(c) to make electronic records to identify and verify when, by whom and for what reason personal data have been recorded or otherwise processed;

(d) to prevent unauthorized access to data carriers.

(5) The obligations laid down in paragraphs 1 to 4 shall apply to processors as well.

2.2 Regulation of European Parliament and EU Council 2016/679 (GDPR)

Section 2 - Securing Personal Data, Article 32 - Processing Security

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

3 Taken technical and organizational measures

Paragon Customer Communications Czech Republic a.s. set, implement and periodically check compliance with the following technical and organizational measures within the framework of the applicable legislation referred to in point 2 of this documented procedure.

The regular inspection and review of technical and organizational measures takes place within the framework of the information security management system under according to ISO 27001: 2015. DI ISMS-DP01-Planning, Operation and Management of ISMS.

3.1 Physical access control

The organization has its offices located at the headquarters of the company at **Dr. Pavla Klementa 1082, 330 23, Nýřany**

- Physical access to objects is limited and controlled by a key system
- Access to data processing locations is governed by a special access authorization. (extra key, electronic access system)
- Every arrival of an external subject to the organization's premises is announced
- Areas are logically separated, access of the external subject is limited to the maximum extent possible
- Mandatory locking mode is set
- Physical access to servers and active components is only allowed to authorized employees only (or persons who have entered into an agreement to manage these devices)
- In separate (reserved) rooms these technical devices can be placed freely
- If these technical devices are located in rooms that are also used for purposes other than the location of technical devices, these devices must be located in a lockable rack. Only authorized persons has access to manage these technical devices.
- There is a camera surveillance system installed to monitor outside spaces.
- Object guard is available 24/7

3.2 Data Access Control (Authentication)

- Access to data is controlled by user accounts
- Each user uses a unique identifier (ID, name)
- Authentication is used to authenticate the user's identity and entitles the user to obtain the required services and access to applications and data.
- Password policy is defined (password length of at least 8 characters, the password must meet (where technically possible) a complexity requirement (3 out of 4 criteria), users are required to change the password after the first login, passwords are valid for 90 days, the last 12 passwords must be different
- The automatic screen lock is set to 15 minutes, stations with access to address-data are internally shortened and 5 minutes.

- Creating and removing user accounts and adjusting user accounts is approved by the appropriate executives.
- External access to data is controlled by encrypted SFTP, VPN SSL, corporate firewall (IP address access) and unambiguous user identification (name + password or certificate)
- IT infrastructure is protected against unauthorized access by firewall and defined VPNs
- IT infrastructure is protected against security threats using antivirus, firewall and domain policies (ransomware)

3.3 Hardware access control (Authorization)

- User has access only to defined coumputers (Active directory settings)
- An unambiguous identifier (Active Directory) is used to access the PC,
- Read / write access to HW equipment (USB disks, flash drives, digifoto) is governed by domain policies
- Access to network disks is resolved on the basis of Active Directory or Passwords (iSCSI Target)
- Anonymous accounts are not allowed
- External providers have limited access to the maximum possible amount (Active Directory account)

3.4 Data transfer (Encryption)

- Data must be transmitted only by a secure path, the encryption method is also dependent on the recipient.
- The encryption method is part of a processing agreement
- Personal data must not be transmitted by e-mail
- In the data exchange via digital media (DVD, USB), the minimum level of encryption is a password-protected archive, the password must meet the strong password criteria, the password is communicated to the addressee via another communication channel, such as e-mail or the SMS.
- Encypted data transfer SFTP or VPN must be used in automated data transfer. Encryption takes place based on PGP keys and need-to-know principles.
- SFTP or VPN encrypted data transmission is used in automated data transfer. SFTP encryption is based on RSA 4096 bit, VPN using SSL (SHA2 4096 bit).

3.5 Logging and monitoring

- Logging of all systems is done continuously. Employees are obliged to inform the Security Manager if a fault or any incident is detected
- Monitoring user activity. The records are being kept and, if possible, include:

  - user identifiers (user ID)
  - date and time of login and logout
  - a record of successful and rejected attempts to access the system
  - a record of usage of privileged accounts
  - a record of rejected attempts to access data and other resources
  - System configuration changes
- Data traffic monitoring and logging is running through the corporate firewall

3.6 Control of processing

- Orders are processed under a privacy agreement
- Orders are processed according to the agreed instructions according to customer's instructions
- Processes for processing customer data with regard to availability, confidentiality and data integrity are defined.
- Customer data is identifiable throughout the processing
- Customer has the right to perform random sample processing
- Automatic deletion of data after 3 months from receipt of data (unless otherwise specified)

3.7 System availability and resilience management

Measures are in place to ensure data availability. The measures introduced include:

- Uninterruptible power supplies for IT infrastructure
- Use of redundant HW servers and firewall
- Multi-level backup plan for servers and stations
- SW license usage tracking
- Defined IT Emergency Plan
- Providing external IT services in the form of contractual SLA terms
- Antivirus system
- Firewalls
- Server room air conditioning
- Fire safety concept

3.8 Separation management

- The individual LAN segments are separated by a VLAN
- Data is physically and logically separated in separate repositories or databases
- There is a separation between test and production environments
- Testing is done on logically or physically separate units (databases, virtualizations, sandboxes)

- Procedures for change management are defined

4 List of documents and attachments that supersede this document

ID:	Document name:
---	

5 List of Related Documents

ID:	Document name:
Act 110/2019 Sb.	§ 40 - Zabezpečení zpracování osobních údajů
Act 110/2019 Sb.	§ 46 - Povinnosti osob při zabezpečení osobních údajů
Directive EU 2016/679	Article 32 - Security of processing
ISMS-DP-01	ISMS planning, operation and management
ISMS-DP02	Data encyption

6 List of used abbreviations

GDPR – General Data Protection Regulation
DI – documented information
DP – documented procedure (ISO 27001:2015)
ISMS – information security management system (ISO 27001:2015)