PERSONAL DATA PROTECTION POLICY

of a Promedica24

Group Company

Approved by:

…… ……..
Place and date

.....
Signatures of authorised representatives

TABLE OF CONTENTS

1. Definitions

1.1. **Personal data –** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number (such as the PESEL number, ID document number or system ID,) location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.2. **Attributes of security:**

- confidentiality - ensuring that personal data are made accessible only to authorised persons;
- integrity - ensuring that personal data are accurate and complete, and that methods of their processing are accurate and complete;
- availability - ensuring that the authorised persons can access the personal data only when there arises such a need.

1.3. **Personal data breach** - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

1.4. **Controller** - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law;

1.5. **Pseudonymisation** - means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

1.6. **Genetic data -** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question**;**

1.7. **Biometric data -** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

1.8. **Data storage device** - any object on which information, including personal data, can be recorded (such as USB flash drives, disks, magnetic stripe cards;)

1.9. **Restriction of processing** - means the marking of stored personal data with the aim of limiting their processing in the future;

1.10. **Processing** - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure

by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.11. **Personnel** - persons employed under an employment agreement, civil-law agreements (such as a contract for the performance of a specific work or a contract of mandate), sole proprietors, trainees, interns, persons directed to work within agreements concluded with temporary employment agencies, who perform works related to the processing of personal data at the PDC.

1.12. **Abbreviations:**

- **Controller / PDC -** Promedica Care sp. z o.o. and other Promedica24 Group Companies
- **OPDP -** Office for Personal Data Protection **-** a body appointed for matters pertaining to the protection of personal data,
- **GDPR** - THE REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- **Policy** – this Personal Data Protection Policy.

2. Introduction

2.1. In accordance with Article 32 of the GDPR (Section 2, "Security of personal data,") the Controller implements appropriate technical and organisational measures to ensure a level of security for personal data appropriate to the risk of breaching the personal data or breaching the freedom of natural persons.

2.2. In selecting the technical and organisational measures, the Controller takes into account the nature, scope, context and purposes of processing the personal data.

2.3. The above measures include the implementation of this Policy on part of the Controller.

2.4. The aim of this Policy is ensuring an adequate level of security for the processed personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.5. The obligations set forth in the Policy are applicable, accordingly, for:

- all Personal data processed by the Controller, both in the case where they process them as a controller, and in the case where they process them on behalf of another controller;
- all Personal data processed, irrespective of the storage device (including paper documents, as well as documents in electronic form;)
- all Locations of the Controller in which the personal data are processed;
- the whole Personnel of the Controller.

2.6. This Policy should be regularly reviewed, at least once per year, so that it remains adequate, useful and effective.

2.7. This Policy is approved by the management and presented as a document for the internal use of the Controller.

2.8. Infringements of the provisions concerning the Controller's obligations with respect to the security of personal data are subject to administrative fines up to EUR 10,000,000.00, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, in accordance with Article 83 of the GDPR. Infringements of the obligations arising from this Policy and of provisions concerning the protection of personal data may be deemed as a gross violation of employment duties, and be subject to disciplinary and penal sanctions.

3. Duties with respect to personal data protection

3.1. **The Controller must:**

3.1.1. ensure adequate technical and organisational measures to establish an appropriate level of security for the processed data

3.1.2. implement organisational procedures, with respect to the following principles:

- **lawfulness** – the personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- **purpose limitation** – the personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- **data minimisation** – the personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **accuracy** – the personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- **storage limitation** – the personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- **integrity and confidentiality** - the personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **accountability** - the Controller is responsible for complying with the above principles, and must able to demonstrate compliance therewith.

3.1.3. implement organisational arrangements with respect to honouring the following rights of data subjects:

- the right to access their personal data,
- the right to rectify their personal data,
- the right to have their personal data erased,
- the right to restrict the processing of their personal data,
- the right to be notified regarding rectification or erasure of personal data or restriction of processing, being an obligation on the part of the Controller,
- the right to move their personal data,
- the right to object,
- the right to receive information concerning:
  - the PDC,
  - the Data Protection Officer (where applicable,)
  - the purpose and legal basis for the processing of their personal data,
  - legitimate interests pursued by the PDC or a third party,

- recipients of personal data and categories of recipients, if such categories exist,
- the intention to transfer personal data to a third country (where applicable,)
- the period for which the personal data will be stored,
- the existence of the right to request access to personal data from the controller,
- the existence of the right to withdraw consent at any time,
- the existence of the right to lodge a complaint with the OPDP,
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and what the possible consequences of failure to provide such data are;
- the existence of automated decision-making, including profiling;

3.1.4. implement a procedure concerning data protection by design and by default;

3.1.5. implement a procedure for notifying a personal data breach to the supervisory authority (the OPDP) and notifying data subjects of personal data breaches;

3.1.6. implement a procedure for carrying out a data protection impact assessment and consulting the supervisory authority prior to processing, where necessary;

3.1.7. maintain a record of processing activities and a record of categories of processing;

3.1.8. appoint a Data Protection Officer (where applicable;)

3.1.9. conclude agreements with entities processing personal data on behalf of the Controller;

3.1.10. monitor whether the transfer of personal data to countries outside the European Economic Area (EEA) is consistent with the law.

4. Organisational security

4.1. Every person who is to be granted access to the personal data should first be acquainted with their duties and responsibilities arising from provisions of law related to personal data protection and from internal procedures.

4.2. Every person who is to commence work should sign a document declaring that they have read internal confidentiality regulations and that they assume responsibility for all operations carried out while processing the personal data.

4.3. Roles and responsibilities with respect to personal data security should be clearly defined and assigned to particular persons or positions.

4.4. With respect to processing personal data, persons carrying out implementation works should not carry out scrutiny operations.

5. Risk assessment

5.1. The Controller analyses and identifies risks related to the processing of personal data.

5.2. The analysis is done regularly, at least once per year, and after every significant change which might impact the security of personal data.

6. Physical security

6.1. The Controller or the security personnel appointed by the Controller implement measures ensuring physical security for personal data transmitted, stored or otherwise processed against accidental or unlawful destruction, loss, alteration, unauthorised disclosure thereof, or access thereto.

6.2. In particular, the Controller:

- designs and implements physical measures protecting the access to rooms and facilities, and measures for entries to such rooms and facilities in particular;
- designs and implements physical measures protecting personal data against natural disasters;
- supervises access points to buildings, such as delivery areas, loading areas and other points through which unauthorised persons can enter the rooms and facilities.

6.3. The adequacy of the measures is determined through the risk assessment.

6.4. In particular, the processing locations are protected through and by:

- CCTV,
- alarm systems,
- the security personnel,
- reception workers,
- smoke detectors,
- fire extinguishers and automatic fire suppression systems,
- locked office rooms,
- locked cabinets and lockers,
- entry cards,
- paper shredders.

6.5. The Personnel should follow the clean desk principle, meaning that only the documents necessary for a given work should be kept on the desk, and documents containing personal data should be deposited in cabinets after a given work is completed.

6.6. Destroying unnecessary paper documents or storage devices containing personal data should be done by using paper shredders of a P-3 security level or higher (in line with DIN 66399) or by placing them in a special-purpose sealed containers.

6.7. Documents containing personal data must be regularly checked for whether they are stored in a manner that prevents unauthorised disclosure of or unauthorised access to data.

6.8. The Controller should implement regulations which will ensure that the Personnel accompany any members of the public (e.g. guests) in processing locations.

6.9. The Personnel should immediately inform their superiors of any irregularities in the functioning of the physical security system, and especially of any sightings of unaccompanied members of the public in the processing locations.

6.10. Persons bringing out paper documents containing personal data must take special care in duly securing those documents against loss or access by unauthorised persons.

7. ICT security

7.1. General principles

7.1.1. Information systems used for processing personal data are protected against risks by such measures that ensure confidentiality, integrity and availability of the data.

7.1.2. The adequacy of the measures is determined through the risk assessment.

7.1.3. ICT protection measures should be kept up to date in light of the changing laws, ongoing technological developments, and new risks.

7.1.4. Emergency plans should be made for important elements of the IT system to ensure that there is no threat to business continuity.

7.2. Stock-taking of equipment and IT software

An inventory of the equipment and software used for processing personal data should be drafted and kept up to date.

7.3. Use of equipment

7.3.1. The Personnel must not use Company equipment for private purposes, unless otherwise stated in different regulations.

7.3.2. The Personnel must not use private equipment for work-related purposes, unless otherwise stated in different regulations.

7.4. System Access Management

7.4.1. Granting and enjoyment of the access to IT systems is limited and monitored.

7.4.2. Every User receives their individual username and password used for identification purposes within the IT system.

7.4.3. Access to the ICT resources is limited, depending on the authorisations granted to the given User.

7.4.4. Access to systems processing personal data is granted to the Personnel only for the time of performing a given work or a given contract.

7.4.5. The Personnel are granted access only to such resources that are relevant to their obligations and agreements which they concluded, and which are essential to the performance of their duties, within the scope of their actions and responsibilities.

7.5. Software and updates

7.5.1. The software must be used in accordance with the provisions of respective licenses to ensure business continuity.

7.5.2. Only software that is approved by the Controller may be installed.

7.5.3. Up-to-date system patches must be monitored, especially with respect to the security level at which they operate.

7.5.4. Antivirus software, as well as virus definitions should be kept up to date on servers, workstations and mobile devices.

7.5.5. No software from unknown sources may be installed.

7.6. Network security

7.6.1. The ICT network should be managed in a manner that ensures fail-safe and uninterrupted communication between the systems.

7.6.2. Network devices should be configured and monitored in a manner that minimises risks.

7.6.3. Encrypted communication should be implemented.

7.6.4. Separation of networks should be introduced, and in particular, a separate network for guests should be used.

7.6.5. If the workstation is connected to a public network, logical or physical safeguards should be implemented to protect the system against intruders or unauthorised access to the system, such as a firewall, an IDS/IPS (detecting and blocking attacks in real time) or PROXY.

7.6.6. Only necessary network traffic should be allowed in production ICT infrastructure. The network traffic configuration should allow only specified and essential IP addresses, and only specified source and destination ports, and specified protocols.

7.7. Printers

7.7.1. All printing equipment present in the network must be identified and actively managed to ensure accordance with security regulations applicable in the Company.

- Firewall rules should take into account the IP addresses of the printers.
- Default log-in methods and passwords should be changed to such methods and passwords that are consistent with the password policy.
- Unused ports, such as FTP or Telnet should be disabled, only such service ports which are necessary for the performance of a given work should be enabled.

7.7.2. Before a printer is withdrawn from use or given to the service point, personal data stored on printer hard drives must be removed.
7.7.3. Unauthorised computers should have limited communication with the printers.
7.7.4. Printing must be authorised in case of open-space printers, allowing only those logging in to the device with a PIN or card to print.

7.8. Encryption

7.8.1. Encryption systems and techniques are used to protect confidentiality of data.
7.8.2. Encrypting mobile storage devices is recommended.
7.8.3. Credentials and personal data should be sent using encrypted communication.
7.8.4. When transferring files that contain personal data, the Personnel must protect the files with a password.
7.8.5. If an e-mail message is sent to a group of people not acquainted with one another, its addressees should be concealed using blind carbon copy.

7.9. Mobile devices and remote working

7.9.1. Depending on the equipment and its specific nature, the safety measures are chosen adequately to the risks and technical capacities.
7.9.2. Due to the specific nature of risks related to the use of mobile devices, special regulations minimising those risks specified in Point 7(16)(2)(5) are applicable.

7.10. Data storage devices

7.10.1. Personal data can be stored and transferred only on authorised storage devices (disks, USB flash drives, etc.)
7.10.2. Personal data must not be transferred to any private storage devices.
7.10.3. Mobile storage devices are subject to encryption and anti-virus control.
7.10.4. Permanent and irreversible removal of the data is recommended particularly in the cases of:
- changing the computer's user;
- returning the device to the manufacturer under a guarantee.

7.10.5. Before handing over equipment which contains disks and other data storage devices to a service point or for disposal, any disks or storage devices contained therein must be removed.
7.10.6. Documentation confirming disposal of equipment and storage devices shall be drafted.

7.11. Back-up

7.11.1. Back-ups of personal data are made in order to maintain their availability.
7.11.2. Rules specifying the process of making back-ups of personal data should be documented.
7.11.3. The following safeguards are implemented with respect to back-ups:
- storage devices containing the back-ups should be protected against unauthorised access;
- storage devices containing the back-ups should be stored in a way which minimises the risk of damage or unauthorised modification thereto;

- back-ups should be stored in a different room from the one in which the server that processes the personal data on an ongoing basis is located;
- back-ups are regularly verified in terms of their usefulness. If the back-ups are deemed as no longer useful, the storage devices are disposed of in a way which prevents further read-outs.

7.11.4. The back-ups are regularly verified for appropriate recovery of the data stored.

7.12. Accountability in IT systems

7.12.1. Users are held accountable for their actions.

7.12.2. Accounting for operations consists in collecting information on who performed what operations within the given IT systems.

7.12.3. System logs should be regularly reviewed and analysed to trace any undesired operations.

7.12.4. The storage period for system logs and the manner of their storage should be determined.

7.12.5. The owner of the application (system), who is responsible for the functionality, content, monitoring and development of the system and for handling any of its malfunctions or incidents related to it, should be identified.

7.12.6. Authorisations of User accounts should be regularly reviewed.

7.13. Server room

7.13.1. The servers and network devices should be protected against loss and power outages.

7.13.2. Servers and network devices responsible for sending network traffic should be placed in separate rooms, such as a server room or junction rooms.

7.13.3. Those rooms such be protected against unauthorised access with additional safeguards, such as reinforced doors, further authorisation procedures, reinforced or grill windows or an access control system.

7.13.4. The server room should be resilient to any natural risks such as a fire, flood or overheating. Its temperature should be controlled, and it should satisfy the norms for the ICT equipment contained therein.

7.14. Reporting incidents and abusive practices related to IT security

7.14.1. The Personnel should immediately inform their superiors of any irregularities in the functioning of the ICT equipment (such their computer, mobile phone, tablet, printer, etc.) or software.

7.14.2. Loss or theft of computer hardware should be immediately reported by the Personnel to their superiors or to a relevant organisational unit.

7.14.3. Equipment intended to be disposed of (scrapped) should be checked and prepared by the person responsible for stock-taking the equipment.

7.14.4. Failures of the computer hardware potentially putting the security of personal data at risk should be reported and documented.

7.15. System audits

7.15.1. Regular audits for ICT systems are recommended, so that the systems are checked with respect to their consistence with the Policy, adopted guidelines and standards.

7.15.2. The results of audits should serve as the basis for any preventive measures combating lower security levels.

7.16. Personnel duties

7.16.1. The Personnel are responsible for ensuring the safety of their workplace with respect to limiting unauthorised access thereto and using ICT equipment in line with its purpose.

7.16.2. The Personnel are obliged to comply with the following rules:

a. the Personnel must use ICT resources only for work-related purposes;
b. the Personnel must use system resources in line with the authorisations granted to each member, and each member must immediately inform their superiors of being provided with broader authority than before;
c. the Personnel must not share computers or mobile phones with third parties or make them accessible thereto;
d. the Personnel must not bring out the equipment or documents without the consent of their superior;
e. in case of mobile devices:
    - the Personnel must take special care when using the devices in public places, meeting rooms or hotels (with the risk of unauthorised persons viewing the protected data;)
    - the Personnel must use physical safeguards against theft if feasible, e.g. by not leaving the devices without any supervision;
    - in cars, the Personnel must hold the portable computers either in the locked trunk or on the passenger seat floor;
    - the Personnel must not make portable computers accessible to third parties;
    - portable computers should be regularly inspected for their security;
    - mobile devices operated from other locations than the Company's office should have a limited and encrypted access to Company infrastructure (e.g. through a VPN;)

f. the Personnel must read and implement the applicable laws related to personal data protection;
g. the Personnel must guard the confidentiality and integrity of their private key used in their electronic signatures;
h. the Personnel must follow **the clean desk principle**, meaning that only the documents necessary for a given work should be kept on the desk;
i. the Personnel must not eat in front of their computers;
j. the Personnel must ensure that when they leave their workstation, the access to the computer is blocked (e.g. by using a password-protected screensaver or by logging out of the system;)
k. the Personnel must immediately report any suspicions of an unauthorised person coming into possession of an authentication element, such as an access card or a password;
l. the Personnel must not share their passwords with other Users and third parties;
m. the Personnel must not write down any personal data on post-it notes, in notepads, notebooks, planner notebooks etc. and must not leave such data on their desks or in other generally accessible locations;
n. the Personnel must not log into accounts of other users;
o. the Personnel must not share PINs or codes to the printers;
p. the Personnel must inform their superiors of any irregularities discovered which result in lower levels of personal data protection;
q. the Personnel must not connect any unauthorised devices to the workstation (e.g. USB flash drives, etc.) without immediately scanning them with an anti-virus software first;
r. the Personnel must not modify the computer hardware at their disposal on their own;
s. the Personnel must destroy paper documents and storage devices containing personal data by placing such documents in paper shredders or placing such devices in special-purpose containers;
t. the Personnel must not transfer the following abroad without the consent of their superiors:
    - records of phone calls,
    - unencrypted documents,
    - screenshots of CRM and SharePoint;
u. the Personnel must not send Company documents to private addresses;
v. the Personnel must ensure that documents containing personal data are stored in locked cabinets or in any other way that prevents unauthorised access thereto;
w. the Personnel must ensure that any members of the public (e.g. guests) in processing locations are accompanied by the employees;
x. the Personnel must change passwords granting access to the operating systems or applications used for processing personal data, if it suspected that a given password is no longer confidential;
y. with respect to access passwords:
    - passwords must be saved only in encrypted form;
    - passwords must not include words that are generally used, and must not include dates, names, surnames, initials, vehicle registration numbers or telephone numbers in particular;
    - passwords must be at least 8 characters long, contain uppercase and lowercase characters, digits and special characters;

z. the Personnel must be particularly careful when receiving e-mail messages from unknown accounts or messages with a suspicious subject or suspicious attachments;
aa. the Personnel must not open links and attachments from unknown sources;
bb. the Personnel must ensure that the computer is equipped with an adequate anti-virus software that is kept up to date;
cc. the Personnel must ensure that the monitor screen is placed in a way that prevents other parties viewing the personal data processed in an unauthorised manner;
dd. the Personnel must not disclose any information concerning the customers, medical care personnel or other persons whose data are processed at the Company in private conversations;
ee. the Personnel must inform people outside the Company that calls on VoIP are recorded. The following is an example script of outgoing and incoming calls:

OUTGOING CALL -> Good morning/afternoon/evening. This is ... at Promedica24. Am I speaking with ...?
First, I must inform you that to ensure the high quality of our services, our conversation will be recorded.
INCOMING CALL -> Good morning/afternoon/evening. Promedica 24, ... speaking. How can I help you?
I must inform you that to ensure the highest quality of our services, our conversation will be recorded.