	Procedure Name:	Procedure version:
Promedica Care Sp. z o.o.	**Notification procedure of a personal data breach**	**1**

I. Definitions:

"Company" means each of the companies forming the capital group of Promedica Care Sp. z o. o. in which there may be a personal data protection breach.

"GDPR" – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC.

"Personal data" means information on an identified or identifiable natural person; an identifiable natural person is a person, who can be directly or indirectly identified, in particular on the basis of an identifier such as first name and surname, identification number, location data, internet identifier or one or more specific factors, which determine physical, physiological, genetic, psychological, economic, cultural or social identity of a natural person.

"Personal data breach" means any breach of security leading to the accidental or unlawful destruction, loss, modification, not authorised disclosure or nit authorised access to personal data transmitted, stored or otherwise processed, which can lead to e.g. the emergence of prejudice to physical, damage to property or non-physical persons, such as the loss of control over their own personal data or limitation of rights, discrimination, theft or forgery of identity, financial loss, unauthorised inversion of pseudonymous information, violation of reputation, breach of the confidentiality of personal information protected by professional secrecy or any other economic or social damage.

“Processing of personal data” 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.

"Processor" is a natural or legal person, public authority, agency or any other body that processes Personal Data on behalf of the Controller.

II. Purpose of the Procedure:

2.1. The purpose of this procedure is to fulfill the legal obligation resulting from the GDPR.

2.2. In the event of a personal data breach in the organization, the Company shall, without undue delay, within 72 hours after having become aware of the breach, be obliged to notify the personal data breach to the supervisory authority.

2.3. Failure to notify the supervisory authority about the breach within 72 hours will result in an administrative penalty of up to EUR 10,000,000 or up to 2% of the total global annual turnover of the company from the previous financial year – the higher penalty will apply.

III. Recipients of the procedure:

3.1. The entire staff of the Company is responsible for the implementation of the procedure.

3.2. In order to manage the breach, a Team of Breach Analysis (ZAN) is established in the Company, which is formed by the employees of the Promedica24 Legal Department.

3.3. Notification of breaches should be directed:

- by e-mail to the following address: daneosobowe@promedica24.pl or
- by phone: +48-507-062-298 (Ewelina Szymczak – Legal Department)

IV. Scope of application of the procedure:

A personal data breach which is subject to a notification to the supervisory authority and to the data subject, is in particular:

- **consultation with the personal data by a person not authorized to access it,**
- **unauthorized disclosure of personal data on the Internet,**
- **loss, theft of information carriers containing personal data,**
- **destruction of personal data, e.g. accident, fire,**
- **loss, theft of computer equipment, information carriers, in particular a laptop computer or a mobile phone.**

V. Procedures

5.1. In the case of a personal data breach, every employee of the Company is obliged to immediately inform an immediate supervisor.

5.2. An immediate supervisor is required to:

- in case of becoming aware of a personal data breach, immediately take actions necessary to stop the undesirable effects of the breach and determine the causes or perpetrators of the personal data breach.
- gather necessary information about the breach and prepare the **personal data breach notification form** constituting **Annex 1**, which is available in paper and electronic version on the company's intranet and to send it to the Team of Breach Analysis (on the above e-

mail address),
- omission, as far as possible, of further planned undertakings that are related to a personal data breach and may hinder the documentation or analysis of the event.

VI. If it is impossible to contact an employee stating a personal data breach with a direct superior, the employee is obliged to immediately report the breach directly to the Team of Breach Analysis (on the e-mail address or telephone number provided above).

VII. The Team of Breach Analysis or a person designated by it, is obliged to:

7.1. receive notifications of personal data breaches by e-mail or telephone;

7.2. collect detailed information on breaches necessary to make a decision on further actions based on, among others Personal Data Breach Form from the notifying person;

7.3. document and register all personal data breaches in the Breach **Register** constituting **Annex 2** to this procedure;

7.4. preparation of the **Notification of a Breach**, in accordance with the guidelines of the competent supervisory authority in the scope of personal data protection – if the personal data breach was classified by the Team of Breach Analysis as a personal data breach to be notified to the appropriate supervisory authority in the scope of personal data protection;

7.5. submitting a draft of the **Notification of a Breach** to the Management Board of the Company in which a personal data breach occurred in order to submit a signature according to its representation rules. The Management Board of the Company signs the Notification of a Breach within 24 hours.

7.6. send to the competent personal data protection supervisory authority, not later than 72 hours after having become aware of a personal data breach signed by the Management Board of the Company,

7.7. prepare and send a notification to the data subject about a personal data breach in accordance with the Personal Data Breach Notification Form constituting **Annex 3** to this procedure, if the personal data breach may result in a high risk to the rights or freedoms of natural persons.

7.8. is responsible for saving the Personal Data Breach Notification Form in the folder on the network drive under the address \\pm24.local\fileshare$\Projects\RODO\Zespol_Sterujacy\naruszenia

VIII. In order to implement this Procedure, all subcontractors of the Company (entities processing personal data on behalf of the Company) must be obliged in the contract to provide information immediately to the Team of Breach Analysis, in accordance with the Personal Data **Breach Notification Form constituting Annex 1** to this procedure.

IX. Table of Annexes:

Annex 1 – **Personal Data Breach Notification Form**
Annex 2 – **Register of Breaches**
Annex 3 – **Personal Data Breach Notification Form of a data subject**