Medika Group

Zagreb, 23 April 2018.

Personal Data Protection and Privacy Policy

In the process of alignment with the General Data Protection Regulation (GDPR), the common principles for the protection of personal data are established for all the Companies and Institutions that are part of the Medika Group, while each Company and Institution will handle any other specific requests by a separate document or a separate tabular display of the Data Collection that is required to keep.

Content:

1. INTRODUCTION
2. RULES AND PRINCIPLES-
3. RIGHTS AND OBLIGATIONS
4. PERSONAL DATA COLLECTIONS of the MEDIKA d.d. and PRIMA PHARME PHARMACY
5. VIDEO SURVEILLANCE
6. DATA PROTECTION OFFICER
7. CODE OF CONDUCT

1. INTRODUCTION

This policy ensures the adequate support for the protection of personal data and privacy of all participants in the business processes of Companies and Institutions that are part of Medika Group: employees, members of supervisory and administrative bodies, business partners, suppliers, customers, service users, patients and members of the Pharmacy Loyalty Program.

The policy applies to the Companies:
Medika d.d., Zagreb, Capraška 1,
Primus nekretnine d.o.o. (Primus Real Estate Ltd) , Zagreb, Capraška 1, and Institutions
PRIMA PHARME PHARMACIES,
Pharmacy Ines Škoko
and the Companies and the Institutions which were founded by Medika d.d or PRIMA PHARME PHARMACY.

The Policy explains all relevant information related to the collection, processing and use of Personal Data and Privacy Principles.

The policy shall provide guidance, ways to acquire knowledge and understanding of your obligations.

The Policy enters into force on the date when it is made.

2. RULES AND PRINCIPLES

Policy and Code of Conduct contain basic rules on Personal Data Protection and Privacy Policy. The rules and principles are in line with the values of the European acquis and with the current regulations governing the protection of privacy and the protection of personal data. In this way, it wishes to emphasize the obligation of all employees to deal with Personal Data.

All employees have a specific responsibility for compliance with the obligations set out in this Policy.

Employees are expected to be able to recognize whether they are intruding on someone's privacy or processing someone's personal data. Employees must be aware of the general rules and postulates so that in case there is a violation of these rules and principles, they may file a complaint to the Data Protection Officer.

This section explains the basic concepts essential to the understanding of Personal Data Protection.

CONSENT: means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

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, 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.

SENSITIVE PERSONAL DATA: 'data concerning health' means Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Personal Data are collected and processed fairly and transparently in accordance with the law.

This Policy prescribes the following obligations for all the employees:

1. The collection and processing of Personal Data is possible, if there is a legally defined basis (eg.: agreement, consent or law).

2. The person whose Personal Data are collected must be informed about the processes of collection and processing od the Data.

3. Personal Data collection may relate to the fulfillment of a particular business purpose (customer data, supplier information, service user data, intervention import, direct marketing, Prima Pharme Loyalty Program), and such collection may only be made with explicit notice and consent of the Data Subject.

4. Use of Personal Data is possible only in a manner that will not affect the persons to whom the Data relate, unless it is provided by the law.

5. ANONIMIZATION or PSEUDONIMIZATION is used as much as possible

ANONYMISATION: The adjustment process of personal data in which the natural persons can not be identified.

PSEUDONYMISATION: 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, under condition that such additional information are kept separately and are subject to technical and organisational measures in order to ensure that the personal data are not attributed to an identified or identifiable natural person.

Responsible management of collected Personal Data is an essential element of the protection of such Personal Data and privacy protection. Once Personal Data are filed in any of the Personal Data Systems under any of the permitted grounds for collecting and processing, Personal Data may not be changed. Any eventual change may depend on the will of the person to whom these personal details relate, or or if such changes are foreseen or permitted by law.

PREDEFINED PRIVACY (Privacy by default): ensure that only the Personal Data which are necessary for each particular purpose of processing are processed as a starting value and, in particular, to ensure that Personal Data are processed only within the minimum necessary frame required for these purposes (quantity, storage period).

Privacy by design: represents an access to projects (projects run by the Institution) that promote privacy compliance and Personal Data Protection from the very beginning of the project.

IMPACT ASSESSMENT on Personal Data Protection - Data Privacy Impact Assessments (DPIAs) is an analysis (tool) that strives to identify possible risks that would affect Privacy and the Protection of Personal Data.

Every employee of Medika Group Companies and Institutions responsible for collecting and processing Personal Data must take care of:

1. Accuracy of collected Data (from collection and processing to destruction)

2. Prohibition of sharing of personal information with other persons within the non-authorized Company / Institution and prohibition of sharing of the Data Outside the Company / Institution towards Third Persons

3. IT security when processing and storing Personal Data

4. Preventing the misuse of Personal Data

5. Ensuring the tracking of the Personal Data while they are still needed

6. Collecting and processing Personal Data while the purpose for which they were initially collected and processed still exists, and the length of processing can be defined by law

7. Personal Data and Privacy Breach and "leaking" of Personal Data beyond each of the Companies or Institutions.

6. RIGHTS AND OBLIGATIONS

This Policy defines the rights and obligations of all natural persons (employees, supervisory and administrative bodies, business partners, suppliers, customers, service users, patients and users of the Pharmacy Loyalty Program) which are subject to the Personal Data entered in the Personal Data Systems in accordance with legally permitted grounds.

Postoje određene kategorije osobnih podataka koje Društvo/Ustanova mora prikupljati da bi ispunila zakonom i podzakonskim aktima propisane obveze, npr. Zakon o radu, Zakon o mirovinskom osiguranju, Zakon o zaštiti na radu, Zakon o zdravstvenoj zaštiti, porezni propisi itd.. Podaci koji se prikupljaju na temelju zakona i podzakonskih akata moraju biti točni i ažurirani.

There are certain categories of Personal Data that must be collected by the Company / Institution in order to fulfill the obligations prescribed by the legal act and bylaws, such as the Labor Law, the Pension Insurance Law, the Occupational Health and Safety Act, the Law on Health Care, Tax regulations etc. The Data collected on the basis of laws and regulations must be accurate and up to date.

Individuals to whom that Data relate (primarily employees) have an obligation that in case of any Data changes given to the Company / Institution, to report that change to the relevant Department in order to enable the accurately update (eg.: change of name, address, or any other similar change of the personal status). The notification of

changes must be made as soon as possible, in person or through a legal representative, and at the latest within 8 days when the change has occured.

The employee as well as every natural person has the right to be informed by the Company / Institution about the Personal Data that the Company / Institution has upon. He or she may exercise his/her right by submitting a written request to the Company / Institution that has the obligation to respond to that request within 30 days. (Article 19 of the Personal Data Protection Act).

Employee as well as any other natural person whose Personal Data are in the Company's Personal Data Systems has a "Right to Delete".
The „Right to Delete“ initiates a procedure in which all Data about that natural person / employee are deleted from all records in which their Personal Data have been collected on the basis of CONSENT (exceptions are Personal Data collected on the basis of laws and other regulations that are kept within the deadlines provided by the laws and by bylaws).

An employee as well as any other natural person whose Personal Data are in the Personal Data Systems of the Company / Institution shall have the right to submit a COMPLAINT on the processing of Personal Data or the RESTRICTION OF PROCESSING of Data relating to him in accordance with the Article 6 (1) (e) or (f) (Lawfulness of Processing) of the General Regulation on the Protection of Personal Data, including the Creation of a Profile based on those Terms.
The Processing Manager may no longer process Personal Data unless the Processing Manager proves that there are convincing legitimate reasons for processing that go beyond the interests, rights and freedoms of the Data Subject or for the establishment, enforcement or defense of legal requirements.

In the case that the Personal Data is entered incorrectly (error in writing), employee / natural person has the right to request from the Company / Institution correction of this Personal Data. The correction will be realized by setting a written request to the Company / Institution. An application must be enclosed with a document containing the correct Personal Data for correction. The correction will be made as soon as possible i.e. in the shortest possible time.

Service users – customers- of the Interim Import, Direct Marketing and Loyalty Program of PRIMA PHARME PHARMACIES are entitled to transfer the given Data based on the Consent to another legal / physical person who processes the Personal Data. The transfer right is achieved by submitting a written request to the Company / Institution.

The Company / Institution has the right to request a correction of the Personal Data from the employee / natural person, if in any case, there is any suspicion that the Data may be incorrect or untruthful.

DATA PRIVACY BREACH (Data Privacy Breach) covers any unauthorized access, processing, use, disclosure, unauthorized collection, destruction, or any act that is unauthorized by an authorized person regarding Personal Data and Privacy. If the

breach or the leakage occurs, each employee is obliged to notify the Company / Institution and the Personal Data Protection Officer for taking measures to detect the problem, prevent further breaches and remedy the resulting damage. The Company / Institution has an obligation to notify the Regulatory Authority (Personal Data Protection Agency) of any Breach that has serious consequences within 72h of the Breach.

7. PERSONAL DATA COLLECTION

For the purpose of fulfilling the statutory obligations, the Company / Institution must have in its possession the Personal Data of its employees. Personal Data are collected and processed to the extent as provided by laws and regulations in a transparent manner. The processing of Personal Data of the employees of the Company / Institution is in the competence of authorized persons of the competent services that perform legal affairs, personnel affairs, salary calculation and accounting and financial affairs.

In order to realize the Rights and Obligations arising from employment, and partly because of business reasons, the Personal data of employees are submitted to the relevant government bodies such as the Croatian Institute for Pension Insurance, Croatian Health Insurance Institute, the Croatian Institute for Public Health, the Tax Administration, and due to the specific activities of vocational organizations such as the Croatian Pharmacy Chamber, the Croatian Chamber of Commerce, the Croatian Employers' Association. All of these institutions, for their part, will take all necessary measures to protect Personal Data.

In addition to the law, the compulsory collections of the Company / Institutions have Collections of Personal Data, which they have formed by themselves, for business reasons, with the aim of better work organization and marketing purposes. These Collections are formed on the basis of the consent of natural persons through explicit written permission, or those are the Data obtained from hospitals, institutions where the patient has been treated or the from the chosen physician, and all for the purpose of achieving the health care of the person and exercise the right to get the remedy.

Processing of Personal Data within the Company / Institution (Personal Data of all participants in the business processes of the companies and institutions of the Medika Group: employees, members of supervisory and administrative bodies, business partners, suppliers, customers, service users, patients and members of the Pharmacy Loyalty Program) is done electronically with the appropriate manual file. All Personal Data are adequately protected. The right to access the manual files and electronic access belongs only to the authorized persons.

Processing of Personal Data can only be done if this is necessary for the business activities of the Institution itself. It is not allowed to authorized persons to perform processing of Data on their own initiative, that is not in consent with the goals set by

the Institution. Employees are not allowed to any processing of Personal Data unless authorized to do so, by the Company / Institution.

The collections of personal data available to the companies / institutions are listed in the tabular display, separately for the Company and separately for the Institutions. The tabular display contains the basis of the collection and the date of the retention of Personal Data. Deadlines are defined by law.

This Policy states the contents of Personal Data Collections. For each collection, the purpose / basis of collection, locations, measures taken to keep personal data and the statutory deadline for keeping Personal Data are stated.
For all categories of Personal Data it is common that, by expiration of the term or termination of the purpose of processing them, the Personal Data are destroyed in such a way that their renewal is not possible.
The data collections are contained in a written document, available on request.

By taking into consideration all business requirements and tasks associated with doing business, it has been appealed to all the employees who come into contact with the above-mentioned Personal Data Collections to use those collections with increased attention.

If during the work process, the copies of the materials contained in the Collections occur, it is necessary to archive the mentioned material by the completition of the work process, as it is determined by positive regulations or internal acts, or to destroy them (by tearing the paper to the inability of restoration or fragmentation - destruction of the documentation).

If an employee finds some materials that are, by their content, an element of the Personal Data Collections, he / she must contact the Personal Data Protection Officer who will archive it, or determine how those found materials should be destroyed.

Employees who print or photocopy material containing personal data or represent internal documents defining SECRET DATA are obliged to take over these materials as soon as possible. This prevents unauthorized persons from having the right to inspect or manipulate those materials. If an employee finds out that the content material refers to the Secret Data, he or she must immediately destroy it and contact the Personal Data Protection Officer.

The purpose of these actions is to reduce the risk of losing and transferring Personal Data and classified information.

8. VIDEO SURVELLIANCE

Pursuant to the Act on the Implementation of the General Data Protection Regulation (GDPR) and the provision of Article 43 paragraph 1 Occupational Safety Act, as a separate law, it is regulated that employers may use surveillance devices as a means of protection at work, under the conditions prescribed by the same Act.

Video surveillance does not include i.e. it prohibits the establishment of supervision over personal hygiene facilities and rooms for the dressing of workers (dressing rooms). The rooms under the video survelliance are marked with appropriate signs that unambiguously inform and notify all the workers and third parties that the room is under the video survelliance.

Data obtained by the usage of video survelliance in accordance with the provisions of the Act on the Implementation of the General Data Protection Regulation are adequately protected because the right of an access has only the authorized person. Third parties have no access to it.

Data may be provided to the competent and competent entities at their request.

9. DATA PROTECTION OFFICER

In accordance with the positive regulations of the Republic of Croatia and EU Legislation Medika d.d. and Prima Pharme Pharmacies have appointed the Personal Data Protection Officer.

Tasks of the Data Protection Officer:

1. The Data Protection Officer shall perform at least the following tasks:

(a) informing and consulting on Data Protection- the Processor Manager or Processor and also the employees who are performing the processing, about their obligations under this Regulation and other provisions of the Union or a Member State.

(b) monitoring of compliance with this Regulation and other provisions of the Union or the Member State of Data Protection and Policy of Processing Manager or processor in relation to the Personal Data Protection, including the distribution of responsibilities, awareness-raising and training of staff involved in processing and related auditing;

(c) providing the advice, when requested so, with regard to the assessment of the effect on the Data Protection and the monitoring of its execution in accordance with Article 35;

(d) cooperation with the supervisory body;

(e) acting as a contact point for the supervisory body on processing matters, including the prior consultation referred to in Article 36 of the Regulation and, where appropriate, consulting on all other matters.

2. The Data Protection Officer shall,while performing his duties, take into account the risk associated with the processing operations and shall take into account the nature, scope, context and purpose of the processing.

For all questions and queries regarding this Policy and questions arised from the practical application of this Policy and general questions about the Protection of Personal Data and Privacy of employees / patients / customers / members of the Pharmacy Loyalty Program, the Personal Data Protection Officer is available.

CONTACT

PRIMA PHARME PHARMACIES : szop@primapharme.hr
Pharmacy INES ŠKOKO : szop@primapharme.hr
Medika d.d.: szop@medika.hr

10. CODE OF CONDUCT

General Regulation on the Protection of Personal Data encourages drafting rules / Codes of Conduct for the purpose of the proper application of the principles contained in the Regulation and the Act on the implementation of the General Regulation on the Personal Data Protection.

a) processing of Personal Data must be legitimate, fair and transparent

b) The Processing Manager must have a legal basis and legitimate interest in processing of Personal Data

c) the Collection of Personal Data must comply with the applicable regulations and this Policy

d) When processing Personal Data, the Processing Manager should use as much pseudonymization of Personal Data as possible

e) The Processing Manager must transparently inform the Data Subject (worker / patient) about the Personal Data he / she collects for his / her needs

f) The Processing Manager must legally, transparently and unambiguously inform the Data Subject on the exercise of his rights guaranteed by this Policy and the positive regulations

g) The Processing Manager must pay special attention to the processing of Personal Data of children and the protection of children and the manner of obtaining the consent of parental responsibility over the child

(h) The Processing Manager shall take all the necessary measures and procedures with a goal to fulfill the security obligations laid down in Articles 24 and 25 and the measures to ensure the security of processing referred to in Article 32 of the General Regulation on the Personal Data Protection

i) Report to the supervisory bodies about the violation of Personal Data and informing the Data Subject of such violations within the time limit set by the Policy

(j) enable the transfer of the Personal Data to third countries or international organizations

k) enable the complaints to the processing of Personal Data only in the part relating the Data Subject

Prima Pharme Pharmacies Medika d.d.