**INSTRUCTION**

**No. 49 dated 02.03.2020**

**"ON PROTECTION OF HEALTH-RELATED PERSONAL DATA"**

Pursuant to Article 30/1/c and Article 31/1/ (ç) and (f) of the Law No. 9887, dated 10.03.2008 "*On personal data protection*", as amended, the Information and Data Protection Commissioner

**INSTRUCTS:**

## Article 1

## General provisions

1. This instruction aims at regulating the processing of personal data and health related sensitive data, in order to ensure respect for the rights and fundamental freedoms of every individual, in particular, the right to privacy and protection of personal data under the legislation in force on personal data protection.

2. This instruction applies to all natural and legal persons operating in the health care system, either public or private, other bodies responsible for the supervision or control of the health care system, as well as data processors acting on their behalf.

3. This instruction also applies to the exchange and communication of health-related data through digital devices, insofar as it is not regulated by special law and bylaws in force.

4. The terms of this instruction have the following definition:

a. "Anonymization" refers to the procedure performed with personal data so that the data subjects are no longer identifiable, directly or indirectly;
b. "The Commissioner" means the Information and Data Protection Commissioner;
c. "Health professionals" are all professionals recognized as such by domestic legislation in the health care sector, whom are subject to the obligation of confidentiality and are involved in the provision of health care;
d. "Pseudonymization" means the processing of personal data in such a way that it can no longer be associated with a particular data subject without using additional information, held separately and subject to technical and organizational measures to ensure that personal data are not associated with an identified or identifiable individual;
e. "Genetic data" means any health data relating to the genetic characteristics of an individual, inherited or acquired during the early period of prenatal development, arising from the analysis

of the biological sample of this individual: chromosome analysis , DNA or RNA or any other element;

f. "Health-related data" refers to all personal data relating to the physical or mental health of an individual, including the provision of health care services, which contains information on the health of the data subject in the past, to present and future.

**Article 2**
**Principles of legitimacy of the processing of health data**

1. Every controller that process health-related data should respect and implement the following principles:

a. The data should be processed in a transparent, lawful and fair manner;

b. The data should be collected for clear, specific and legitimate purposes and should not be processed contrary with these purposes. Further processing with purpose of archiving in the public interest, for scientific, historical or statistical purposes, is not considered as incompatible with the initial purposes, when the appropriate assurances guarantee compliance with the rights and fundamental freedoms;

c. The processing of personal data should be proportional and necessary in relation with the legitimate intended purpose and should be carried out only on the basis of law or by obtaining consent of the data subject.

d. The data must be accurate, clear and not excessive, in relation to the purposes for which they are being processed and, if necessary, kept up-to-date;

e. Appropriate security measures should be taken, which should count on the state of the art technology, the sensitive nature of health-related data and the potential risk assessment, in order to prevent risks such as unauthorized access to data, destruction, loss, use, non-use, inability to access them;

f. The rights of individuals whose data are being processed, should be considered, in particular the right of access, information, rectification, deletion and objection to his/her data, as provided for by the legislation in force and this instruction.

2. Data controllers, and data processors who act on their behalf , must take all necessary measures to comply with their obligation regarding the protection of personal data and should be able to demonstrate, in particular to the competent supervisory authority, that the processing is being performed in accordance with these obligations.

3. Health-related data may be processed only where it is expressively foreseen by the specific legislation, under the appropriate safeguards and where the processing is necessary for:

a. preventive medical purposes, diagnostic purposes, administration of care or treatment, management of health services by health professionals and those of the health care or social welfare sectors;

b. public health protection purposes, such as protection from health threats, humanitarian action or to ensure a high standard of quality and security for medical treatment;

c. the protection of vital interest of the data subjects or of another individual;

d. reasons related to the controllers' obligation and the exercise of their rights or those of data subjects in relation to employment and social protection, in accordance with the law;
e. processing for archiving purposes in the public interest or for the purposes of historical or statistical research, according to the conditions determined by law;
f. protection of the public interest based on the law. In this case, the measures in question must be proportionate to the purpose pursued, respect the principles of the right to data protection and provide appropriate and specific measures to protect the fundamental rights and interests of the data subject;
g. when the data subject has given his consent. Where the law provides that the processing of health-related data may not be limited to the consent of the data subject, the latter shall be notified of the right to withdraw consent;
h. where the processing is necessary for the performance of a contract entered into by the data subject, or on his behalf, with a health professional, according to the conditions stipulated by the law, including the obligation to maintain professional secrecy;
i. when health-related data are made public with the consent of the data subject himself. In the case of juvenile patients who are unable to give consent, consent is given by the legal representative (parent or legal guardian of the minor).

4. With respect to the data related to the health of unborn children, such as data resulting from prenatal diagnosis and/or identification of the genetic characteristics of these children, the above guarantees should be applied, as far as possible.

## Article 3

## Genetic data

1. Genetic data should be collected only when the appropriate safeguards are in place, when it is provided for by the law and/or on basis of the expressed consent of the data subject.

2. Genetic data processed with a preventive, diagnostic purpose, treatment of the data subject or to a member of his biological family, or for scientific research, should be used only for these purposes.

3. Genetic data collected during a judicial proceeding, should be processed only when there are no alternative means of administering the evidences, necessary to prevent a real and immediate risk, or for prosecuting a particular criminal offense, according to the procedural guarantees stipulated in the Code of Criminal Procedure.

4. The data subject is entitled to know any information regarding his genetic data. The controller should provide guarantees on the right of access to the data subject, with the most appropriate

means and manners. The restriction to this right may only be applicable in cases provided for by the law.

## Article 4

## Disclosure of health data

1. When health-related data are disclosed by various health professionals, for the purposes of offering and administering health care to an individual, the data subject must be informed in advance, unless this is impossible due to the need and urgency.

2. When disclosure is based on the consent of the data subject, this consent may be withdrawn at any time. When the disclosure is determined by law, the data subject may object to the disclosure of his health data, in accordance with the provisions of the law.

3. The health professionals in various sectors of healthcare and social welfare, are subject to the rules of maintaining confidentiality.

4. The rules for data processing also apply to electronic medical records and communication with electronic addresses that enable the disclosure and exchange of health-related data.

5. In the exchange and disclosure of health-related data, the physical, technical and administrative security measures must be adopted, as well as the necessary measures to ensure the confidentiality, integrity and availability of health-related data.

6. Health related data may be transmitted with controllers/processors which are authorized by the law so as to have access to these data.

7. Insurance companies are authorized to have access to health-related data, up to the level provided by special law or to the extent that the data subject has given consent, applying appropriate safeguards in accordance with the law and the principles of this instruction.

8. Employees cannot be considered as authorized recipients to have access to data related to the health of individuals, except under the conditions provided by this instruction for the processing of personal data in the context of employment.

## Article 5
## Archiving and retention deadline of health data

1. Health-related data should not be stored in a form that allows the identification of data subjects for more than necessary, or in excess of the purposes for which they are processed, unless used for archiving purposes in the public interest, scientific, historical or statistical purposes.

2. The provisions of internal organizational measures for the storage, processing and security of data, must result in contemporary technical and organizational measures, regularly reviewed, in order to protect personal data related to health from any illegal or accidental destruction, any loss or alteration and to protect them from any unauthorized access.

3. Manual or electronic archiving of health data may be performed by the public or private controller himself, or may be delegated to other processors in accordance with legal procedures related to the processing delegation.

4. The term of storage of health data is determined in accordance with the specific legislation and the legislation on personal data protection.

5. The data processed manually or in automatic manner, upon the expiration of the deadline, shall be destroyed or anonymized in order to de-identify individuals.

## Article 6
## The rights of data subjects

1. The Data subject is entitled to know whether his personal data are being processed, receive without delay information in an understandable form on his data and be able to access the following information:

a. The purpose or processing purposes;
b. The relevant categories of data being processed
c. Recipients or categories of recipients of data and anticipated data transfers to a third country or international organization;
d. Storage period;
e. The reason for processing the data.

2. The data subject has the right to request the correction or deletion of data, when it is informed that the data about him are not regular, complete truths or have been processed and collected in violation of the law. Exceptions are cases where the data concerned are anonymous, when the processing is required by specific law, or when the controller demonstrates major reasons for continuing processing.

3. If the request to rectify or delete the data is refused, the data subject shall be informed of the legal reasons for this purpose. In the case of unfounded refusal, or inaction from the controller, the data subject is entitled to file a complaint with the Commissioner's Office according to the rules provided for by the law on personal data protection.

## Article 7

## Obligations of controllers and processors

1. The controller shall inform data subjects for the processing of their health-related data. The information should include:

a. identity and contact details of controller and processor as appropriate;
b. the data processing purpose and as appropriate, the relevant legal basis;
c. the term of data retention;
d. recipients or categories of recipients of data and anticipated data transfers to a third country or international organization;
e. the option to object their data processing according the provisions of personal data protection legislation;
f. conditions and available means to the data subject for the exercise, through the controller, of their rights to access, rectification and deletion of their data.

2. When necessary, and with the intention to ensure fair and transparent processing, the information should also include:

a. The option that their data may be further processed for a legitimate purpose, in accordance with the appropriate safeguards as provided for by the law and in line with the conditions set forth in this instruction;
b. The right of complaint with the Commissioner.

3. This information should be provided prior to the collection of data or at the first communication with the data subject.

4. The information should be understandable and easily accessible, in clear and plain language, so as to allow the data subject to fully understand the intended processing. In particular, when the data subject is unable to obtain the information, it must be given to the legal guardian.

5. The controller shall not inform the data subject where the processing is expressly provided by the law.

6. When processing is performed by automatic means, the controller/processor must guarantee to the data subject, according to the conditions determined by law, the transmission in a structured, interactive and readable format of personal data, aiming at transferring them to another controller.

7. The controller/processor ensures the security of health data information with information security management systems, according to the Instruction No. 47 of the Commissioner, dated 14.09.2018 "*On determining the rules for maintaining the security of personal data processed by large controllers*", and Instruction No. 48, dated 14.09.2018 "*On the certification of information security management systems, personal data and their protection*".

## Article 8
## Confidentiality and security of health data

1. The processing of health data is legal only when performed by health professionals who have the obligation to maintain professional secrecy and confidentiality of data, or by other persons who are subject to such an obligation.

2. Controllers must take the necessary security measures in accordance with the legislation in the field of personal data protection. These measures should be reviewed periodically.

3. In order to ensure confidentiality, integrity, accuracy of the processed data, security and protection of patients, appropriate measure should be taken:

a. to prevent any unauthorized person from accessing the installations used for personal data processing (installation access control);
b. to prevent unauthorized access to processed data in the information system, as well as any unauthorized consultation, modification or deletion of processed personal data;
c. to prevent the use of automated data processing systems by unauthorized persons through data transmission devices (use control);
d. to ensure the possibility of control and ascertainment for individuals or subjects which may receive health data through data transmission devices (communication control);
e. to ensure the possibility of investigating on individuals that might have had access to the system and what health data are introduced to the system, when and from whom (data entry control);
f. to prevent unauthorized reading, copying, alteration or deletion of health data when communicating personal data and transmission of the database (transmission control);
j. to protect data through copies of security.

4. Public and private controllers/processors administering medical files, shall develop an internal regulation in compliance with the principles set forth in the personal data protection legislation and those in this instruction.

## Article 9

## Scientific research

1. Processing of health data for scientific research purposes shall be subject to the appropriate safeguards provided by the law and from this instruction, ensuring the rights and fundamental freedoms of the data subject.

2. The need of processing health data for scientific research should be considered upon the view of research purposes, risks against the data subject, as well as concerning the processing of genetic data, in the context of the risk for the biologic family.

3. In principle, health data should only be processed in case of a scientific research project, if the data subject has given his consent in accordance with this instruction, except as otherwise provided by the law.

4. The data should be anonymized when the purposes of scientific research allow this. In the contrary, pseudonimization of data should be applied during the phase of sharing identification, so as to protect the rights and fundamental freedoms of the data subject.

5. In the case when the data subject withdraws from the scientific research project, the health data processed for that research purpose, shall be destroyed or anonymized in a manner that do not compromises the scientific validity of research, by informing the data subject.

6. Personal data used for scientific research should not be published in a manner that identifies the data subject, with exception to the case when the data subject has provided consent and/or when it is expressly anticipated by the law.

## Article 10
## Data processing through portable electronic devices

1. Concerning the data collected by portable electronic devices and which may reveal information on the physical and mental health of the data subject, the same principles and guarantees apply for the processing of other health-related data, provided for in this instruction.

2. Any use of portable electronic devices must be accompanied by appropriate security measures that guarantee the verification of the person concerned and encryption during data transmission.

**Article 11**
**International transfer of health data**

1. The international health data transfers may be performed when an adequate level of data protection is in place in accordance with provisions of the legislation in force and bylaws adopted by the Commissioner

2. Health data may be transferred to a country with no adequate level of data protection only if:
a. the data subject has given consent to such international transfer;
b. is necessary to protect a vital interest of the data subject;
c. upon the authorization of the Commissioner;
d. under any other case as provided for by the law and bylaws adopted by the Commissioner.

**Article 12**

**Final provisions**

1. Instruction No. 5, dated 26.05.2010 "*On fundamental rules concerning protection of personal data in the health care system*" and Instruction No. 23, dated 20.11.2012 "*On processing of personal data in the health sector*" of the Information and Data Protection Commissioner are repealed.

2. In case of failure to implement this instruction, sanctions as provided by the legislation in force on personal data protection will be applied.

This instruction shall enter into effect after its publication on the Official Gazette.

**COMMISSIONER**

**Besnik Dervishi**