R E P U B L IC OF ALBANIA
RIGHT TO INFORMATION AND PERSONAL DATA PROTECTION COMMISSIONER

GUIDELINE

No.02, dated 30.04.2025

ON

PROTECTION OF HEALTH PERSONAL DATA

Pursuant to article 82, paragraph 1, letter "d", article 85, paragraph 1, and article 97, paragraph 2, of Law No. 124/2024 "On Protection of Personal Data" (hereinafter referred to as "the Law"), the Information and Data Protection Commissioner, hereby issues the following,

GUIDELINE:

Article 1
General Provisions

1. This Guideline aims to regulate the processing of personal and sensitive data related to the field of health, aiming to guarantee respect for the fundamental rights and freedoms of every individual, in particular, the right to the protection of personal data and a private life according to the Law.
2. It is applicable to all public or private natural persons and legal entities operating in the healthcare system, other bodies responsible for the supervision or control of healthcare, as well as data processors acting on their behalf.
3. This guideline is also applicable to cases of exchange and communication of health-related data by means of digital devices, as far as not specifically regulated by special legislation.
4. In this Guideline, the following terms are defined as follows:
    a) "Healthcare professionals" are all professionals recognized as such by domestic legislation in the healthcare sectors, who are subject to the obligation of confidentiality and who are involved in the provision of healthcare;
    b) Other terms used in this Guideline have the same meaning as in the Law.

Article 2
Processing of health data

1. Any controller processing data relating to health, which are categorised as sensitive, must respect and apply the principles laid down in the personal data protection legislation.
2. Data controllers and processors acting under their responsibility must take all appropriate measures to comply with their obligations in relation to data protection and must be able to demonstrate, in particular to the competent supervisory authority, that the processing complies with these obligations.
3. Data relating to health may be processed only where expressly provided for by specific legislation of the controller/processor, 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) the purposes of protecting public health, such as protection against health risks, humanitarian actions or to ensure a high quality and safety standard for medical treatment;
    c) the purpose of protecting the vital interests of the data subject or of another person;
    ç) the reasons relating to the obligations of the controllers and the exercise of their rights or those of the data subjects relating to employment and social protection, in accordance with the law;
    d) processing for archiving purposes in the public interest or for historical or statistical research purposes, under the conditions laid down by law;
    dh) protection of the public interest on the basis of law. In this case, the measures in question must be proportionate to the aim pursued, observe the principles of the data protection law and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subjects;
    e) when the data subject has provided consent, except in cases where the legislation in force prohibits the processing of such data even on the basis of consent;
    ë) when the processing is necessary for the implementation of a contract concluded by the data subject, or on his behalf, with a health professional, under the conditions laid down by law, including the obligation to maintain professional secrecy;
    f) when the data relating to health are made public with the consent of the data subject himself.

4. In the case of minor patients who are incapable to provide consent, consent shall be given by the legal representatives (minor parent or legal custodian).
5. For data related to the health of the fetus, such as data resulting from prenatal diagnosis and/or from the identification of its genetic characteristics, the above guarantees shall apply, to the extent possible.

Article 3
Genetic data

1. Genetic data are sensitive data and shall be processed only in the cases provided for in article 9 of the Law.
2. Genetic data shall be collected only when appropriate protection measures are in place, when provided for by law and/or on the basis of the consent expressed by the data subject.
3. Genetic data processed for preventive, diagnostic purposes, treatment of the data subject or a member of his/her biological family, or for scientific research, shall be used only for these purposes.
4. Genetic data collected during a judicial proceeding shall be processed only when there are no alternative means for the administration of evidence, necessary to prevent a real and immediate risk, or for the prosecution of a specific criminal offense, according to the procedural guarantees provided for in the Code of Criminal Procedure.
5. The data subject has the right to be informed of any information regarding his/her genetic data. The controller must guarantee the data subject the right of access in the most appropriate form and manner. The restriction of this right may only be applied in cases expressly provided for by law.
6. Any controller processing data relating to health, which are categorised as sensitive, must respect and apply the principles laid down in the personal data protection legislation.
7. Data controllers and processors acting under their responsibility must take all appropriate measures to comply with their obligations in relation to data protection and must be able to demonstrate, in particular to the competent supervisory authority, that the processing is in compliance with these obligations.

Article 4
Dissemination of health data

1. When health-related data are disseminated by different health professionals, for the purposes of providing and administering health care to an individual, the data subject must be informed in advance, unless this is impossible due to necessity and urgency.
2. Where the dissemination is based on the consent of the data subject, this consent may be withdrawn at any time. Where the dissemination is determined by law, the data subject may object to the dissemination of his health data, in accordance with the provisions of the Law.
3. Health professionals in different sectors of health care and social welfare must be subject to data confidentiality obligations.
4. The rules on data processing also apply to electronic medical files and communication with electronic addresses that enable the dissemination and exchange of health-related data. In any case, the most appropriate and secure route must be chosen, and personal addresses or applications (such as WhatsApp) must not be used for this dissemination.
5. In the exchange and dissemination of health-related data, physical, technical and administrative security measures must be adopted, as well as the necessary measures to guarantee the confidentiality, integrity and availability of health-related data.
6. Health-related data may be communicated to controllers/processors who are authorized by law to have access to these data or when the data subject himself gives consent to this dissemination.

7. Insurance companies are authorized to have access to health-related data, to the extent provided for by special law or to the extent that the data subject has given consent, by implementing appropriate safeguards in accordance with the Law and the principles of this guideline.
8. Employees cannot be considered as authorized recipients to have access to data related to the health of individuals, except under the conditions provided for by this guideline for the processing of personal data in the employment context.

Article 5
Health data archiving and storage period

1. Health -related data shall not be kept in a form which permits identification of data subjects for longer than is necessary or for purposes for which they are processed, unless they are used for archiving purposes in the public interest, scientific, historical or statistical purposes.
2. The provisions on the internal organisational measures on the storage, processing and security of data shall produce state-of-the-art technical and organisational measures, regularly reviewed, in order to protect health -related personal data against any unlawful or accidental destruction, loss or alteration, and to protect them from any unauthorised access.
3. Paper -based or electronic archiving of health data may be carried out by the public or private controller itself, or may be delegated to other processors in accordance with the legal procedures regarding the delegation of processing.
4. The time period for which health data is stored shall be determined in accordance with the specific legislation under which the controller/processor operates and the legislation on the personal data protection.
5. Manually or automatically processed data after the expiry of the period shall be destroyed or anonymised so that individuals are not identified or become identifiable.

Article 6
Rights of the data subject

1. The data subject has the right to know whether his/her personal data are being processed, to receive information about the data without delay in an intelligible form and to have access to the information in accordance with the provisions of the Law.
2. The data subject has the right to request the rectification or erasure of data, when he/she becomes aware that the data about him/her are inaccurate, true or complete or have been processed and collected in violation of the law.
3. If the request to rectify or erase the data is rejected, the data subject must be given legal grounds for this purpose. In the event of an unfounded rejection or failure to act by the controller, the data subject has the right to lodge a complaint with the Commissioner in accordance with the rules provided for in the Law.

Article 7

Controller and processor obligations

1. The controller shall inform data subjects about the processing of their health-related data in accordance with the provisions of the Law.

2. This information shall be provided to the data subject before the data are collected or at the first communication with him. The information shall be intelligible and easily accessible, in clear and appropriate language, to enable the data subject to fully understand the intended processing. In particular, where the data subject is incapable of receiving the information, it shall be provided to the legal custodian.
3. The controller shall not be required to inform the data subject where the processing is expressly provided for by law.
4. Where the processing is carried out by automated means, the controller/processor shall guarantee to the data subject, under the conditions laid down by law, the transmission in a structured, interactive and readable format of personal data in the event of their transfer to another controller.

Article 8
Health data confidentiality and safety

1. The processing of health data is lawful only when carried out by health professionals who are obliged to maintain professional secrecy and confidentiality of the data, or by other persons who are subject to such an obligation.
2. Controllers must take the necessary security measures in accordance with the personal data protection legislation. These measures must be periodically reviewed.
3. In order to ensure the confidentiality, integrity and accuracy of the processed data, the security and protection of patients, appropriate measures must be taken in order to:

   a) to prevent any unauthorised person from having access to the installations used for the processing of personal data (control of access to installations);

   b) to prevent unauthorised access to the data processed in the information system, as well as any unauthorised consultation, modification or deletion of the processed personal data;

   c) to prevent the use of automated data processing systems by unauthorized persons by means of data transmission devices (control of use);

   ç) to guarantee the possibility of control and ascertainment for individuals or entities to whom health data may be communicated by means of data transmission devices (control of communication);

   d) to guarantee the possibility of control over who has had access to the system and what health data have been entered into the information system, when and by whom (control of data entry);

   dh) to prevent unauthorized reading, copying, modification or deletion of health data during the communication of personal data and the transmission of the database (control of transmission);

   e) to protect the data by making backup copies.

4. Public and private controllers/processors of medical documentation must draft internal regulations that reflect the principles set out in the personal data protection legislation and in this Guideline.

Article 9
Scientific research

1. The processing of health data for the purposes of scientific research shall be subject to appropriate safeguards provided for by law and this Guideline, while guaranteeing the fundamental rights and freedoms of the data subjects.
2. The necessity of processing health data for scientific research shall be assessed in the light of the research purposes, the risks to the data subject while, as regards the processing of genetic data, in the context of the risk to the biological family.
3. Health data shall, in principle, only be processed in the context of a scientific research project if the data subject has given his consent in accordance with this Guideline, except where otherwise provided for by law.
4. The data shall be anonymised where the purposes of the scientific research so permit. Where the purposes of the research do not permit, pseudonymisation of the data shall be applied at the stage of identification separation, in order to protect the fundamental rights and freedoms of the data subjects.
5. When the data subject withdraws from a scientific research project, the health-related data processed in the framework of that research shall be destroyed or anonymised in a manner that does not compromise the scientific validity of the research, with the data subject being informed.
6. Personal data used for scientific research shall not be published in a form which allows identification of the data subject, except where the data subject has given his/her consent and/or where expressly provided for by law.

Article 10
Data processing through mobile electronic devices

1. The same principles and guarantees for the processing of other health-related data as provided for in this Guideline shall apply to data collected from mobile electronic devices and which may reveal information on the physical and mental health of the data subject.
2. Any use of mobile electronic devices shall be accompanied by appropriate security measures ensuring the verification of the person concerned and encryption during data transmission.

Article 11
International transfer of health data

The international transfer of health data is carried out in accordance with provisions 39 - 42 of the Law, as well as the sub-legal acts approved by the Commissioner.

Article 12
Final provisions

1. All public and private controllers/processors in the territory of the Republic of Albania, which exercise activities in the field of health, are responsible for implementing this Guideline.
2. Failure to implement this Guideline is punishable in accordance with the provisions of article 94 of the Law.
3. Guideline no. 49, dated 02.03.2020 "On the Protection of Personal Health Data", shall be repealed.

This Guideline shall enter into force upon publication in the Official Gazette.

COMMISSIONER

Besnik Dervishi