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

GUIDELINE

No.05, dated 16.07.2025

ON

PERSONAL DATA PROCESSING BY COMPETENT AUTHORITIES

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
Scope

The scope of this Guideline is to determine the rules for the lawful processing of personal data by the competent authorities[1], who during their activity process personal data administered manually and electronically, pursuant to Part III of the Law.

Article 2
Purpose

This sub-legal act guides the competent authorities on the manner of lawful processing of personal data collected for the purpose of preventing, investigating, detecting or prosecuting criminal offences or the execution of criminal convictions, including the protection and prevention of threats to public safety, defence or national security.

[1] Article 5, paragraph 1 of the Law provides that: *"1. "**Competent authority**" is the court, the prosecution office and any public body which mandate is the prevention, investigation, detection, or prosecution of criminal offenses or execution of criminal sentences, including the protection and prevention of public security threats, the protection of national security or any other institution which is vested the right to exercise public functions, tasks or powers by law for one or more of such purposes.*

Article 3
Definitions

1. *"Anonymization"* is the process of using a set of techniques whereby personal data are processed in such a way that it is no longer possible for a natural or legal person to attribute the data to an identified or identifiable natural person.

2. "Data Protection Officer" is an expert in personal data protection legislation who has an advisory and awareness-raising role in relation to the controller or processor in the implementation of the Law. Data protection officers monitor internal compliance, inform and advise on obligations arising from data protection legislation and act as a point of contact for data subjects and the Commissioner. In essence, they ensure that the controller/processor processes personal data lawfully.

3. "Data profiling" means any form of automated processing of personal data consisting of the use of data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning his/her performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. This includes the use of data to take decisions that significantly affect the private life of the individual.

4. Other terms used in this Guideline have the same meaning as those in Article 5 of the Law.

Article 4
General provisions

1. Competent authorities shall process data, whether or not by automated means, for the purposes of public or national security and for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties / convictions [2].

2. For data processed for these purposes, the competent authorities shall in any case ensure that the principles of lawfulness, purpose-specific processing, data minimisation, data accuracy, storage time period restrictions, integrity and confidentiality, and accountability are applied[3].

3. The competent authorities shall designate a data protection officer

[2] Pursuant to article 3, paragraph 1, and article 47 of the Law.

[3] Foreseen in article 6 and 48 of the Law

Article 5
Scope of application

1. This Guideline applies to all processing of personal data carried out by the Competent Authorities, which are included in the scope of application of Article 47 of the Law.

2. Any other institution, which has been granted by law the right to exercise public functions, duties or powers, based on the legislation in force[4], shall also be considered a competent authority.

3. The competent authorities shall apply the provisions of this Guideline only with regard to personal data processed for these specific purposes. With regard to other personal data processed as data about staff or for purposes not directly related to those specified in article 5, paragraph 1, of the Law, the general provisions of Parts I and II of the Law shall apply as to any controller.

Article 6
Categories of personal data

1. Personal data processed by the competent authorities are categorized as follows:

a) General identification data;

b**)** Sensitive data**,** including ethnic or racial affiliation, political opinions, religious beliefs, trade union membership**,** biometric and genetic data, data on health, life or sexual orientation;

c) Data related to criminal convictions, criminal offenses and security measures in relation to them, etc.

2. In cases of processing of personal data based on personal assessments, a separate register must be kept, specifying the reasons or circumstances for this assessment.

Article 7
System interaction

1. The competent authorities shall communicate through the interaction of state databases or systems, documented in accordance with the purpose of their activity.

2. In cases where information about the personal data subject results to be inaccurate or must be erased under article 57 paragraph 6 and 7 of the Law, the controller shall communicate this information to each recipient of these data, so that they are corrected or deleted in any database or system that has been registered for this purpose of processing.

[4] In interpretation of article 5, paragraph 1 of the Law, other bodies that do not have this as their primary scope of activity, but also process data for one or more of these purposes, will also be considered as competent authorities *(local authorities are also included in the definition, when they pursue cases that may be considered criminal offenses and are subject to fines).*

3. All cooperating competent authorities shall guarantee that the processing of data and their dissemination, in accordance with the Law, is carried out confidentially and only by authorized employees.

4. Data processing is carried out only to the extent necessary to achieve the purpose without exceeding the latter.

5. Sensitive data shall be processed only in the cases provided for in article 52 of the Law.

6. Through the interoperability of databases or systems, the competent authorities must guarantee traceability regarding the actions performed on the processed personal data, according to article 62 of the Law.

Article 8

Rights of personal data subjects

1. The competent authority shall be obliged to ensure that the data subject can exercise his rights pursuant to articles 55, 56 and 57 of the Law, by providing the information in a concise, transparent, intelligible and easily accessible form[5].

2. When the data subject cannot be provided with access to his personal data due to legal obstacles for the case, the latter's request may be delayed, restricted or refused to the extent and to the extent that it is proportionate, in order to avoid the obstacles[6] or to protect national security.

3. In any case, the competent authorities must document the facts and legal grounds for denying the right to access, under paragraph 2 of this article.

4. Data subjects have the right to request from the Commissioner a review of the response given by the competent authorities, regarding their request and the lawfulness of the processing of personal data.

Article 9

Transfer of personal data

1. Transfers of personal data by the competent authorities shall be carried out only in accordance with articles 70-74 of the Law.

2. In case of transfers of personal data in the absence of an adequacy decision, competent authorities shall inform the Commissioner of the categories of transfers that have been carried out pursuant to paragraph 2 of article 72 of the Law.

[5] Provided for in article 54, paragraph 1 of the Law.

[6] This does not preclude the inquiries, investigations, procedures conducted by the competent authorities or judicial processes.

Article 10
Security measures

1. The competent authorities shall take measures to achieve specific security objectives, by carrying out a data protection impact assessment, where the data processing activities are likely to result in a high risk to the rights and freedoms of data subjects. This impact assessment shall include both the identification of the risks and the determination of the measures to be taken to mitigate them[7].

2. In case of use of various technological systems or devices, the competent authorities shall take measures to protect data by design and by default. The protection of personal data during processing operations will be better respected when it is integrated into the technology from the moment it is created. Consequently, technical and organisational measures must be taken from the time of planning a processing system to protect the security of these data.

3. Pursuant to article 61 of the Law, the competent authorities must maintain documentation of processing activities, including information on the use of profiling.

4. The competent authorities must ensure the level of data security, including security plans, updating IT systems and organizational measures, conducting impact assessments *(especially when using new technology)* and recording specific processing operations[8].

5. The competent authorities, as controllers, must notify the Commissioner and the data subject in the event of a data breach.

6. All employees of the competent authorities, subject to this Guideline, are obliged to keep the data processed during the exercise of their function confidential even after its termination.

7. The processing of sensitive data, especially biometric and genetic data, requires special protection and dual control measures, including separate and physically protected administration or in dedicated systems.

Article 11
Confidential reporting mechanisms

1. Competent Authorities shall establish and use secure and confidential mechanisms or channels that guarantee the reporting of violations of the Law[9].

2. Reporting mechanisms that guarantee confidentiality by competent authorities are:

[7] The data protection impact assessment is provided for in article 64 of the Law.
[8] The obligation to register is provided for in article 62 of the Law.
[9] Example: *A police officer finds that information on detainees is stored on insecure platforms or distributed on WhatsApp, in groups, in an unauthorized manner. The officer can report this violation as unlawful processing of personal data, through an internal mechanism, such as a physical reporting box, an online portal or a dedicated email.*

a. Dedicated email with limited access;

b. Online platform for internal use, according to authorized access;

c. Dedicated physical reporting boxes/devices, located on the premises of the institution;

d. Verbal reporting with record minutes kept in a designated office.

e. Any other form of reporting that meets the requirements of the Law.

3. In each reporting case, competent authorities are obliged to guarantee the confidentiality of the identity of the reporter and the persons involved.

4. Each competent authority must adopt clear internal procedures for handling reports, as well as deadlines for their storage and destruction, in order to document and fulfil legal obligations, according to article 69 of the Law.

Article 12
Data storage and erasure

1. Competent authorities should provide in their regulatory framework for appropriate time periods for the erasure of personal data, for periodic review of their storage periods and take concrete measures to ensure that these time periods[10] are complied with.

2. Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed. Personal data should therefore be erased or made anonymous as soon as they are no longer necessary for the purposes for which they were lawfully collected by the competent authorities[11].

3. Personal data, when processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, may be kept for a longer period than is necessary for the purposes for which they were collected. This is subject to the implementation of appropriate technical and organisational measures, such as, in particular, pseudonymisation or anonymisation, in order to protect the rights and freedoms of data subjects in accordance with the *"principle of time- restricted storage"*[12].

4. The competent authorities shall, within their area of competence, monitor all processing operations involving personal data, ensuring that the data are accurate and that retention periods are respected. Personal data shall be updated when they are no longer accurate and

[10] Measures to comply with deadlines can be carried out automatically through the system (*privacy by design*) or manually by designating a responsible person.

[11] According to article 57 of the Law

[12] Provided for in article 6, paragraph 5 of the Law and article 45 of the Law.

erased from the database when they are no longer necessary for the purpose for which they were collected[13].

5. Where personal data have been rectified or erased, the Competent Authority shall notify all recipients of the personal data concerned. [14].

Article 13
Criteria for reviewing the need for continuity of data storage

In determining the need for the continued storage of personal data, the following criteria should be taken into account:

a) The age of the data subject, paying particular attention to minors and elderly persons.

b) Completed sentences, where a person has completed his/her imprisonment sentence and in the meantime the first review period has elapsed, his/her personal data should be deleted, unless there is evidence that the data are necessary for other ongoing investigations. In the case of sensitive data, they should be deleted, unless it is necessary to retain them for other ongoing investigations.

c) Judicial decisions, in particular decisions of acquittal relating to certain criminal offences, where all information on the cases should be erased, unless there is evidence that the data are necessary for other ongoing investigations. In the case of processing sensitive data, they should be deleted, except in cases where it is necessary to retain them for other ongoing investigations. The same criteria may apply in cases of amnesty or rehabilitation.

Neni 14
Final provisions

1. All competent authorities are responsible for the implementation of this Guideline

2. Guideline no. 17, dated 11.05.2012 *"On determining the retention period of personal data processed in electronic systems by state police bodies for the purposes of prevention, investigation, detection and prosecution of criminal offenses*", is repealed.

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

COMMISSIONER

Besnik Dervishi

[13] Pursuant to Articles 6 and 57 of the Law

[14] Duty quoted in article 57, paragraph 7 of the Law.