



Republika e Kosovës
Republika Kosova-Republic of Kosovo
Qeveria - Vlada - Government
Ministria e Administrimit të Pushtetit Lokal
Ministarstvo Administracije Lokalne Samouprave
Ministry of Local Government Administration

REGULATION (MLGA) NO.02 /2026 ON THE PROTECTION OF PERSONAL DATA

Regulation (MLGA) No.02/2026 on the Protection of Personal Data, was approved by the Acting Minister of MLGA, on 20.07.2026

Ministry of Local Government Administration

In accordance with Article 93, (4), Articles 123 and 124 of the Constitution of the Republic of Kosovo, Article 11, paragraph 1, subparagraph 1.5 of Law No. 08/L-117 on the Government of the Republic of Kosovo (Official Gazette, No. 34/2022, 18.11.2022), Article 40, paragraph 2 of Law No. 06/L-082 on the Protection of Personal Data, Article 16, paragraph 1, point 1.1 of the Regulation (QRK) - No. 04/2026 on the Fields of Administrative Responsibility of Ministries, Article 16, paragraph 1.1, Minister and Ministries, the Minister of the Ministry of Local Government Administration, issues:

REGULATION (MLGA) NO. 02/2026 ON THE PROTECTION OF PERSONAL DATA

Article 1

Purpose

The purpose of this Regulation is to define the organizational and technical procedures during the processing of personal data of the employees of the Ministry of Local Government Administration (MLGA), the measures for the protection and security of personal data, as well as their storage and administration.

Article 2

Scope

The provisions of this Regulation shall be implemented by the officials of the Ministry of Local Government Administration (MLGA), in accordance with the legislation in force on the protection of personal data in the Republic of Kosovo.

Article 3

Definitions

1. The expressions used in this Regulation shall have the following meanings:

- 1.1 **Ministry** - refers to the Ministry of Local Government Administration;
- 1.2 **Agency** - refers to the Agency for Information and Privacy;
- 1.3 **Data Controller** - refers to the purpose and methods of processing personal data;
- 1.4 **Processor** - refers to the organizational units of the Ministry or third parties that process data on its behalf;
- 1.5 **Recipient** - refers to any natural or legal person or public authority that receives data;
- 1.6 **Data Subject** - refers to an identified or identifiable natural person;
- 1.7 **1.7 Personal Data** - refers to any information related to a person;
- 1.8 **Sensitive Data** - refers to data about origin, beliefs, and health;
- 1.9 **Data Processing** - refers to any action on personal data;
- 1.10 **Data Destruction** - refers to their complete destruction;

Article 4

Principles of processing personal data

1. **Principle of lawfulness, fairness and transparency** – personal data shall be processed in an impartial, lawful and transparent manner, without infringing the dignity of data subjects.
2. **Principle of purpose limitation** – personal data shall be collected only for specific, explicit and legitimate purposes and may not be further processed in a manner incompatible with those purposes. Further processing for archiving in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered incompatible with the initial purpose.
3. **Principle of data minimization** – personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed.
4. **Principle of accuracy** – personal data must be accurate and kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purpose of processing, are erased or rectified without delay.
5. **Principle of storage limitation** – personal data may be stored only for as long as necessary to achieve the purpose for which they were collected or further processed. Once the purpose of processing has been fulfilled, personal data shall be destroyed, erased, blocked or anonymized, unless otherwise provided by the relevant Law on State Archives or any other relevant law.
6. **Principle of integrity and confidentiality** – personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.
7. **Principle of accountability** – the controller must be responsible for and able to demonstrate compliance with all principles set out in this Article.

Article 5

Lawful processing of personal data

1. The ministry is responsible for making sure personal data is protected from:
 - 1.1 Damage to data – all information must be stored in a way that prevents damage, disappearance, or distortion;
 - 1.2 Loss of data – measures must be taken for backup, reserve copies, and physical/electronic storage;
 - 1.3 Unauthorized access – access to data must be restricted only to authorized persons;
 - 1.4 Unlawful processing – all processing must comply with the law and the purpose for which the data were collected.
2. Specific actions of the organizational units to fulfill these responsibilities:
 - 2.1 Control of access to computer systems and physical documents;
 - 2.2 Establishment of technical and physical protection measures;
 - 2.3 Recording of activities and possible incidents;
 - 2.4 Training of employees on security and confidentiality;
 - 2.5 Cooperation with the responsible officer and authorities regarding any incident.

Article 6

Processing of special categories of personal data

1. In accordance with Law No. 06/L-082 on Personal Data Protection, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as the processing of genetic data, biometric data for the purpose of unique identification, data concerning health, or data concerning the sex life or sexual orientation of the data subject, is prohibited.

2. By way of exception to paragraph 1 of this Article, the processing of special categories of personal data is permitted only if one of the conditions provided for in the relevant article of the law in force is met, including cases where:

- 2.1. the data subject has given explicit consent;
- 2.2. processing is necessary for carrying out obligations and exercising rights in the field of employment and social protection;
- 2.3. processing is necessary to protect the vital interests of the data subject or another person;
- 2.4. processing is carried out by non-profit organizations within the framework of their legitimate activities;
- 2.5. the data have been made public by the data subject;
- 2.6. processing is necessary for the establishment, exercise, or defense of legal claims;
- 2.7. processing is carried out for reasons of substantial public interest;
- 2.8. processing is necessary for health purposes or public health purposes;
- 2.9. processing is carried out for archiving purposes in the public interest, scientific, historical, or statistical research purposes.

3. In all cases, the processing of these data must be proportionate to the purpose of processing, respect the essence of the right to personal data protection, and be accompanied by appropriate technical and organizational measures to protect the rights and interests of the data subject.

4. The Ministry shall ensure that special categories of personal data are classified and protected with enhanced security measures in order to prevent unauthorized access, use, or disclosure, in accordance with the legislation in force.

Article 7

Processing of personal data relating to criminal convictions and offences

The processing of personal data relating to criminal convictions and offences or related security measures, based on the provisions of this Regulation, shall be carried out only under the control of an official authority in accordance with the relevant law. Any comprehensive register of criminal convictions shall be kept only under the control of an official authority.

Article 8

Transparency and communication with the data subject

1. In accordance with Law No. 06/L-082 on Personal Data Protection, the Ministry shall ensure that information relating to the processing of personal data is provided to data subjects in a clear, understandable, and easily accessible manner.
2. The information shall be provided in writing or in electronic form, and upon request may also be given orally, after verification of the identity of the data subject.
3. The Ministry shall handle requests from data subjects without delay and, in any case, within one (1) month of receipt of the request, with the possibility of extension in accordance with the legislation in force.
4. In the event of failure to act on the request, the Ministry shall inform the data subject of the reasons and of the right to lodge a complaint with the competent authority. The provision of information shall be free of charge, except where requests are manifestly unfounded or excessive.
5. The Ministry may request additional verification of identity where there are reasonable doubts.

Article 9

Right of access by the data subject

1. The data subject has the right to obtain confirmation from the controller as to whether or not personal data concerning him or her are being processed and, where that is the case, to access the personal data and the following information:
 - 1.1 Processing purposes;
 - 1.2 Categories of relevant personal data;
 - 1.3 Recipients or categories of recipients to whom the personal data have been or will be disclosed, especially recipients in third countries or international organizations where applicable, the expected time period during which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - 1.4 The existence of the right to request from the controller the correction or deletion of personal data or the limitation of the processing of personal data concerning the data subject, or to object to such processing;
 - 1.5 The right to submit a request to the Information and Privacy Agency;
 - 1.6 If the personal data are not collected from the data subject, any available information as well as their source;
 - 1.7 The existence of automated decision-making, at least in those cases, the appropriate information regarding the relevant logic, as well as the anticipated significance and consequences of this processing for the data subject.
2. Where personal data are transferred to a foreign country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Article 10

Information to be provided to the data subject

1. In accordance with Law No. 06/L-082 on Personal Data Protection (Articles 12 and 13), the Ministry shall ensure that the data subject is informed about the processing of personal data, including the identity of the controller, the purpose and legal basis of the processing, the categories of data, the recipients and, where applicable, transfers.
2. The Ministry shall also provide information on the retention period of the data, the rights of the data subject, including the right of access, rectification, erasure and complaint, as well as any other information necessary for fair and transparent processing.
3. Kada se podaci ne prikupljaju direktno od lica na koje se odnose, informacije se dostavljaju u rokovima propisanim važećim zakonima, osim u slučajevima kada je lice već informisano ili kada se primenjuju zakonske izuzetke..

Article 11

Right of access to personal data

1. In accordance with Law No. 06/L-082 on Personal Data Protection (Article 14), the data subject has the right to obtain confirmation as to whether his or her data are being processed and, if so, to have access to those data and relevant information concerning the processing.
2. The Ministry shall provide the data subject with a copy of the personal data being processed, in accordance with the legislation in force, while respecting the rights and freedoms of others.
3. Information and access to the data shall be provided in an intelligible form and, where appropriate, in electronic format.
4. Where personal data are transferred to a foreign country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Article 12

Right to erasure (“right to be forgotten”)

1. The data subject shall have the right to request the controller to erase personal data concerning him or her without delay, and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
 - 1.1 the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - 1.2 the data subject withdraws consent on which the processing is based;
 - 1.3 the data subject objects to the processing;
 - 1.4 the personal data have been unlawfully processed;
 - 1.5 the personal data must be erased for compliance with a legal obligation to which the controller is subject.

Article 13

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

1.1 the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

1.2 the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

1.3 the controller no longer needs the personal data for the purposes of processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims;

1.4 the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1 of this Article, such personal data shall, with the exception of storage, be processed only with the consent of the data subject or for the establishment, exercise, or defense of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 of this Article shall be informed by the controller before the restriction of processing is lifted.

Article 14

Notification and transfer of personal data

1. The Ministry shall notify recipients of any rectification, erasure, or restriction of processing of personal data, unless this proves impossible or involves disproportionate effort.

2. The data subject shall have the right to receive the personal data he or she has provided in a structured and readable format, and to transfer those data to another controller, where the processing is based on consent or contract and is carried out by automated means.

3. The exercise of this right shall not adversely affect the rights and freedoms of others and shall be implemented in accordance with the conditions laid down in the legislation in force.

Article 15

Right to data portability

In accordance with Law No. 06/L-082 on Personal Data Protection (Article 19), the data subject shall have the right to receive and transfer personal data to another controller, subject to the conditions laid down by law.

Article 16

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons arising from the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, designed to implement data protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism referred to in Article 43 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 17

Notification of a personal data breach to the Agency

1. In the case of a personal data breach, the controller shall, without delay and where feasible, not later than seventy-two (72) hours after becoming aware of it, notify the Agency about the personal data breach, except when the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification to the Ministry is not made within seventy-two (72) hours, it must be accompanied by the reasons for the delay.
2. Processors shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 of this Article shall at least:
 - 3.1. describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - 3.2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - 3.3. describe the likely consequences of the personal data breach;
 - 3.4. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where and insofar as it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the breach, its effects and the remedial action taken. This documentation allows the Ministry to check compliance with this article.

Article 18

Data protection impact assessment

1. In accordance with Law No. 06/L-082 on Personal Data Protection (Article 35), the Ministry of Local Government Administration shall carry out a data protection impact assessment prior to processing where the processing is likely to result in a high risk to the rights and freedoms of natural persons.

2. The assessment shall include a description of the processing, an assessment of necessity and proportionality, the risks to data subjects, and the measures for their protection.

3. The Ministry shall seek the advice of the data protection officer and, where appropriate, review the assessment when the risks resulting from the processing change.

Article 19

Prior consultation

1. The Ministry shall consult the Agency prior to processing where the impact assessment indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk.

2. The Ministry shall submit to the Agency the relevant information on the processing, including the purpose, safeguards and the impact assessment.

3. The Ministry shall act in accordance with the advice and requirements of the Agency, in compliance with the legislation in force.

Article 20

Designation of the data protection officer

1. The MLGA shall designate a data protection officer in every case where:

1.1 the processing is carried out by a public authority, except for courts acting in their judicial capacity;

1.2 the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or

1.3 the core activities of the controller or the processor consist of large-scale processing of special categories of data.

Article 21
Designation and position of the data protection officer

1. The ministry appoints an official for data protection when:
 - 1.1. processing is carried out by a public authority, except for courts;
 - 1.2. the core activities require systematic and large-scale monitoring of data;
 - 1.3. Special categories of data are processed according to the relevant Law on the protection of personal data.
2. One DPO may be designated for several structures or bodies, ensuring easy accessibility and reporting at a high management level.
3. The DPO shall perform his or her duties on the basis of professional qualities and expert knowledge in the field of data protection and may be a member of staff or engaged under a service contract.
4. The DPO shall not receive instructions regarding the performance of his or her tasks, shall not be penalized, and shall be bound by confidentiality. Data subjects may contact the DPO regarding issues related to their personal data.

Article 22
Tasks of the data protection officer

1. The DPO shall have at least the following tasks:
 - 1.1 inform and advise the Ministry and staff on their legal obligations regarding the processing of personal data;
 - 1.2 advise on and monitor the data protection impact assessment pursuant to Article 35 of Law No. 06/L-082;
 - 1.3 cooperate with and act as a contact point for the Personal Data Protection Agency, including prior consultation under Article 36;
 - 1.4 assess the risks associated with processing, taking into account its nature, scope, context and purposes.
2. The DPO shall ensure that every processing activity is carried out in accordance with the law and the prescribed protective measures.

Article 23

Certification

1. The official designated by the MLGA shall be certified by the Agency for Information and Privacy. The data protection certificate shall be issued by the Agency on the basis of the criteria and procedures set out in a bylaw.
2. To obtain the certificate, controllers, processors and legal entities/enterprises shall fulfill at least the following minimum conditions:
 - 2.1 demonstrate that they possess adequate knowledge in the field of personal data protection;
 - 2.2 where required, comply with the necessary international security standards;
 - 2.3 in cases where legal entities/enterprises engage controllers, processors and other personnel who have obtained certification;
 - 2.4 demonstrate that the performance of their functions in relation to data protection does not result in a conflict of interest.

Article 24

Remedies

1. The data subject has the right to submit complaints to the Agency if the processing of personal data violates Law No. 06/L-082 on the Protection of Personal Data.
2. The Agency informs the complainant about the progress and the outcome of the complaint, including the possibility of using judicial remedies.
3. The data subject may authorize a representative or a non-profit organization to exercise their rights in accordance with Law No. 06/L-082 on the Protection of Personal Data; the authorization must be in writing and certified by the competent authority.

Article 25

Liability and compensation

1. The controller or processor shall be liable for material or non-material damage caused by the processing of personal data in violation of the Law (Article 56).
2. Where processing involves more than one controller or processor, each shall be liable for full compensation of the damage.
3. The party has the right to seek compensation through the competent court in accordance with the provisions of Law No. 06/L-082 on the Protection of Personal Data.

Article 26

General provisions on camera surveillance

1. Camera surveillance shall be implemented in accordance with Law No. 06/L-082 on Personal Data Protection, Articles 75–78, unless otherwise provided by another law.
2. Controllers in the public sector must place a visible notice for the installation of cameras and identify the data controller, according to Law No. 06/L-082 on the Protection of Personal Data.

3. Data collected through cameras shall be processed only for necessary purposes, while respecting the rights and legitimate interests of data subjects.

Article 27

Personal data breaches

1. Any violation of the provisions of this Regulation on the protection of personal data by employees or structures of the Ministry of Local Government Administration (MLGA) shall be considered an administrative offense and sanctioned in accordance with Law No. 06/L-082 on Personal Data Protection and the legislation in force.

2. This includes: processing of data without a legal basis or the consent of the data subject, failure to inform employees about data processing, non-compliance with requirements for storage, cataloging or protection of data, unauthorized transfer of data outside the MLGA.

Article 28

Applicability

1. This Regulation shall apply only during the processing of personal data of employees of the Ministry of Local Government Administration (MLGA), measures for the protection and security of personal data, as well as their storage and administration.

2. The provisions of this Regulation are in harmony with the relevant law on personal data protection, and any issue or legal provision not regulated by this Regulation shall be governed by the provisions of the relevant law on personal data protection.

Article 29

Entry into force

This regulation enters into force after being signed by the Minister of the Ministry of Local Government Administration and seven (7) days after publication in the Official Gazette of the Republic of Kosovo.

Elbert Krasniqi

Acting Minister of Local Government Administration

20/07/2026