AGJENCIA PËR INFORMIM DHE PRIVATËSI
AGENCIJA ZA INFORMACIJE I PRIVATNOST
INFORMATION AND PRIVACY AGENCY

OSCE Organization for Security and Co-operation in Europe
Mission in Kosovo

GUIDE FOR MUNICIPAL OFFICIALS ON

PERSONAL DATA PROTECTION AND ACCESS TO PUBLIC DOCUMENTS

Table of contents

1. Introduction

The Guide for municipal officials on protection of personal data and access to public documents (Guide) is dedicated to municipal officials responsible for issues pertaining to access to public documents, protection and processing of personal data, as they are the primary focal points for ensuring data safety while adequately serving the public interest of transparency. In this vein, the aim of this Guide is to provide public institutions with guidelines to orient their work and resolve recurrent challenges in balancing the right to access public documents and the protection of personal data.

Mindful that the line dividing the need for personal data protection and transparency is very thin – and, therefore, special attention must be paid to balancing these two needs – the Information and Privacy Agency (IPA) and the Organization for Security and Co-operation in Europe (OSCE) Mission in Kosovo developed this publication to support municipalities in these efforts.

The content of this Guide is based on discussions and questions brought up by municipal officials at five regional workshops organized in 2023 jointly by the IPA and the OSCE Mission in Kosovo with a view to streamlining and clarifying the implementation of the Law No. 06/L-082 on Protection of personal data and Law No. 06/L-081 on Access to public documents at municipal level.

These workshops themselves originated from early ad-hoc requests from the municipalities of Rahovec/Orahovac and Dragash/Dragaš in 2022, who appealed for support and guidance to improve the municipalities' responsiveness and timeliness to requests for access to public documents. The OSCE Mission in Kosovo teamed up with the IPA to deliver two workshops, where municipal officials received detailed and nuanced answers to their specific questions.

Thenceforward, the IPA and the OSCE Mission in Kosovo initiated a path to develop the capacities of municipal officials on data privacy and access to public documents throughout the above-mentioned series of regional workshops, which also served to present the IPA's legal basis and mandate, and led to the drafting of the present publication.

2. How to use this Guide?

This publication is composed of four interrelated sections which can be read as a whole or individually consulted when municipal officials responsible for issues pertaining to access to public documents and protection of personal data need guidance on their work. These are:

- The *Section 3* describes the mandate and role of the IPA;
- *Section 4*, contains frequently asked questions (FAQs). These are curated from the workshops for municipal officials organized in 2023 by the OSCE Mission in Kosovo and the IPA and reviewed to ensure their accuracy. This section is composed of different thematic sub-sections to allow for quick searches within the publication, thereby facilitating the use of this Guide.
- *Section 5* presents scenarios based on real-life examples along with recommended actions, which may prove useful to municipal officials with similar cases. Albeit real, the examples are anonymized and devoid of personal data that would make the case identifiable to third parties.
- *Section 6*, included as an annex to the Guide, includes a summary of principles and considerations on the Law No. 06/L-082 on protection of personal data and Law No. 06/L-081 on access to public documents.

3. What is the Information and Privacy Agency?

The IPA is an independent agency responsible for overseeing the implementation of laws on Protection of personal data and Access to public documents[1], to protect the fundamental rights and freedoms of persons with the processing of their personal data, as well as ensuring access to public documents.

The IPA acts with full independence in the discharge of its duties. The duties and powers of the IPA are defined in the provisions of the respective laws, mentioned above, for which it is responsible to oversee and implement.

The IPA has an advisory role and provides legal opinions on the basis of complaint/s and/or request/s on cases deriving from protection of personal data and access to public documents. On the later, the IPA also monitors municipal websites to ensure that their content complies with the Law on Access to Public Documents.

The head of the IPA, the Commissioner,[2] is appointed by the Assembly of Kosovo for a five-year mandate and is responsible for representing and organizing the work of the Agency.

For more information on the principles of data protection and on the right to access public documents, please refer to the Annex.

[1] LAW NO. 06/L –082 ON PROTECTION OF PERSONAL DATA (rks-gov.net) and LAW NO. 06/L-081 ON ACCESS TO PUBLIC DOCUMENTS (rks-gov.net)
[2] Ms. Krenare Sogojeva Dërmaku.

4. Frequently Asked Questions

4.1. Personal Data Protection

What is the difference between the right to protection of personal data and privacy and the right to access to public documents?

When a person assumes public office, he or she may partially lose the right to personal privacy, in view of public scrutiny of his or her actions. While access to public documents requires transparent and free access to everything that is public, the right to privacy restricts this right, in the interest of protecting the Constitutional rights of the individual to a certain level of personal privacy. This thin line is not always easily identifiable. The IPA therefore seeks to raise awareness of the standards, based on EU peer agencies and the jurisprudence of the European Court of Human Rights, and stands ready to support municipalities in finding this thin line when specific cases arise.[3]

What is personal data and what is the scope of the Law No. 06/L-082 on Protection of Personal Data?

Personal data is any information related to a natural person (i.e., a data subject) who can be identified directly or indirectly through that data, particularly by reference to an identifier such as a name and surname, 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.

Therefore, personal data is any information that renders any natural person identifiable either directly or indirectly. Even when direct information is anonymised, many identifiable information is often left open. This is particularly relevant to smaller settlements, where persons are easily identifiable through one or two factors – and so anonymization may not be enough to adequately protect an individual's right to personal data protection.

Who is covered by the personal data protections outlined in Law No. 06/L-082 on Protection of Personal Data?

The Law only covers an identified or identifiable natural persons (i.e. data subject) and precludes deceased persons. In addition, the protection offered by the Law does not extend to legal persons, such as business entities.

[**Info box** on the main principles of personal data processing, as per Article 4 of the Law on Protection of Personal Data]

Who is responsible for carrying out data protection functions in public institutions?

Every public institution should have a data protection officer and it may not necessarily be a dedicated position. The IPA, nonetheless, recommends assigning a dedicated officer in view of the importance of personal data protection. The IPA acknowledges staff limitations and therefore recommends that the mayor or the head of the institution assigns a Data Protection focal point. There are presently efforts underway to list data protection officer as a dedicated position under the civil service Job Catalogue. In October 2022, the IPA sent an official note to mayors and responsible officers clarifying what officials may qualify to discharge this function. There are certain positions that are excluded by virtue of their official position, such as human resources and IT officers, as it could constitute a conflict of interest. Recommended posts include

[3] In line with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) and its Additional Protocol (CETS No. 223).

legal officers or any a position that municipality decides as long as it does not constitute a conflict of interest as mentioned above.

What is the role of the data protection officer and who may assume this function?
The data protection officer should assist, inform and advise municipal officials and the relevant staff in ensuring that relevant data protection rules are observed and properly implemented, and co-operate with the IPA as a contact point. Assigning a data protection officer is a legal requirement, who shall regularly monitor the proper use of data processing programs and the measures and procedures in place to ensure secure data processing.[4] Therefore, the IPA urges all mayors to assign a data protection officer, for access to public documents.

What data can I publish when holding public meetings, such as public consultations or budget hearings?
While it may be necessary to collect and process personal data (insofar as necessary to meet a specified, explicit and legitimate purpose), municipalities shall refrain from publishing lists of participants from public meetings or initiatives. If needed, name, surname are sufficient for publication purposes; institutions should not publish data on residence, phone numbers, personal numbers, gender, etc. Municipalities should also consult their respective local regulations on transparency to ensure compliance with provisions thereunder. If, in the interest of transparency, an institution decides to publish the list of participants of these meetings, the institution shall duly notify the participants that the list will be published, while exercising due care to ensure that minimal amount of data is published. In these cases, institutions should also consult any regulations that may require their publication for specific purposes.

The storage period of these information is not determined by any legal provision, however, the IPA considers that the time-period of one year, from the time of the information published by the municipality, is sufficient to achieve the goal of transparency after which the information can be deleted.

Can I publish photos and/or videos taken at a public meeting?
A standard boilerplate disclaimer shall be put at the entrance of the venue, notifying individuals that the organizers will take photos and/or film at the event and, if they do not wish their photos or videos to be published, they should indicate such decision in the participants list (by ticking the adequate checkbox). Lists of participants shall also contain a notice on the purpose of this list (for example, stating that the list will only be used for documenting participation and not for any other purpose).

Are there any data that are restricted to access even by an auditor?
Restrictions apply to third parties who possess no legal authorization to access such data. However, the auditors are vested with legal authority to access and audit data, in line with the purpose of the audit. However, it remains under the responsibility of the institution to evaluate which data to transmit to the auditor in order to fulfil his/her duties and not to give access to data that is not relevant for the auditing.

Will the ranking of my institution in the Municipal Performance Grant or other schemes be jeopardized by restricting or not publishing documents containing personal data?
In case of concerns related to insufficiency of data when competing on various schemes (such as the Municipal Performance Grant) the Ministry of Local Government Administration (MLGA) should be aware of the obligations of municipalities to protect personal data in the documents,

[4] Required under Article 37 paragraph 1.1 of the Law on Protection of Personal Data

however, the institutions should note that they will be held accountable for publishing documents containing personal data without adequate legal basis, as such publication may cause damage to data subjects. Ultimately, and if in doubt, municipalities may avail themselves of the opportunity to consult with MLGA and/or IPA on specific cases related to MLGA schemes and personal data.

What are some considerations involving digital data?
Data protection is rendered all the more important in the view of ever-expanding digital development and lifecycle of artificial intelligence systems. The EU's General Data Protection Regulation and Council of Europe (CoE) Convention on AI[5] are the overarching legislation on data protection. Posting on social media is already posing serious security and privacy risks; therefore, more awareness campaigns are required to elevate the understanding among the public as well.

How can I publish lists of children admitted to kindergarten?
Children enjoy an elevated level of protection compared to adults, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.[6] As such, institutions should exercise extreme caution when publishing data associated with children. No information (including name and surname) should be published without the consent of parents or legal guardian, which should be sought during the application process. However, it is a good practice to not publish names at all. Public interest is served only to the extent of ascertaining compliance to procedures. The IPA recommends publishing the application codes/numbers only.

Can I consult the IPA on personal data protection issues?
Municipal officials are encouraged to call or write to the IPA[7] for consultations in case of uncertainties, especially when developing legislation. Depending on the number of cases received, there may be delays however, the IPA will certainly respond. The deadline for response, according to the Law on Protection of Personal Data, is eight (8) weeks from the moment the request for consultation was submitted. However, this deadline may extend to additional six (6) weeks depending on complexity of the matter. [8] The IPA advises that Data Protection Officers are engaged in all activities involving personal data processing.

4.2. Access to public documents

Who can request access to public documents?
Every person has the right of access to public documents in the same and equal manner, and upon request. This request can be made in writing, electronical or via verbal communication. Even when the request is made orally by the requesting person, the official of the public institution responsible for access to public documents is obliged to draft the written request for further proceeding. The applicant requesting a public document is not obliged to provide reasons for the use of public documents in order to access these. In addition, the applicant has the right to remain anonymous in relation to third parties.

[5] The General Data Protection Regulation is a Regulation in EU law on data protection and privacy in the EU and the European Economic Area. See: https://eur-lex.europa.eu/eli/reg/2016/679/oj ; Convention 108, and CoE Convention on AI: CM(2024)52-final (coe.int)
[6] Please consult Article 7 of the Law No. 06/L-082 on Protection of personal data on children age limit.
[7] Contact – Information and Privacy Agency (rks-gov.net).
[8] Article 33.2 of the Law No. 06/L-082 on Protection of personal data.

Restriction of this right shall be done only in limited and specific cases determined by the legislation in force. The "Damage and Public Interest Test" described below will provide responsible officials with guidance on granting or refusal of access to public documents.

What is the "Damage and Public Interest Test"?
In 2021, the IPA developed the "Damage and Public Interest Test", a set of guidelines to help responsible officials when considering requests for access to public documents. The test describes the steps to be followed for determining public interest while weighing considerations on data privacy. All in all, the test must be conducted by responsible officials in order to ascertain their decision to approve, limit or deny access to a public document.

What is the deadline for responding to requests for access to public documents?
The Law on Access to Public Documents stipulates that public institutions shall, within seven days from the date of recording the request, issue a decision to grant access to the requested document or render a justified decision for the full or partial refusal, and inform the applicant of the right to request a reconsideration of the request, as well when and where to submit such request.

The public institution may extend the deadline to a maximum of 15 additional days if the document has to be searched within a large number of documents or outside the public institution; or if the applicant requests, with a single application, a large number of public documents. In these two cases, the public institution should notify the applicant immediately of the progress and the reasons causing the extension of the deadline, but no later than eight days after receiving the request.

However, if the requested public document is deemed as necessary for the protection of the life or liberty of a person, the public institution is obliged to provide an answer within 48 hours.

In what languages should public documents be available and provided to applicants?
Documents published by public institutions shall be made public in the official languages of Kosovo, as per the Law on Use of Language.[9] In addition to Albanian and Serbian languages, in municipalities inhabited by a community whose mother tongue is not an official language, and which constitutes at least five per cent of the total population of the municipality, the language of the community has the status of official language in the municipality and shall be in equal use with the official languages. Exceptionally, in the municipality of Prizren, Turkish language has the status of official language.

In the case of municipalities where a community's mother tongue has the status of language in official use, members of that community have the right to present oral or written submissions and documents, and to receive a reply in their own language, from municipal institutions and officials, if they so request.

Where a public document is available in more than one language, access to the public document shall be granted in the preferred language of the applicant.

Can I allow access to public documents without a written decision from the responsible official?
The IPA reiterates the obligation of institutions to develop and issue written decisions. It also reiterates that only the responsible official (i.e., mayors, heads of institutions) can approve the

[9] No. 02/L-37 on the Use of Languages.

decision, although responsibilities for drafting may be delegated to focal points. Municipal staff and public officials shall refrain from allowing access to public documents based on a verbal instruction from the responsible official.

Can a focal point for access to public documents override rulings of municipal directorates regarding what information is to be published or withheld?
There may be cases whereby specific municipal directorates choose to withhold information, while the focal point for access to public documents believes that such information should be made public. For example, the directorate of agriculture may withhold information on names of beneficiary NGOs and the amounts of the subsidies, but the focal point or the municipal information officer believes that this approach is too restrictive.

Municipalities should note that the law holds responsible officers (in the case of municipalities: the mayor) primarily responsible before the law, but not focal points. Focal points may only advise mayors as responsible officers to the letter of the law; however, the ultimate responsibility lies with the mayor.

In cases of staff limitations, can an institution forego any of the provisions of personal data protection and access to public documents?
Limitations in staffing capacities or political fall-out do not constitute grounds for failure to observe and implement the legal framework. Under no circumstances shall limited administrative capacities be deemed acceptable grounds for restricting access.

Can I provide minutes of meetings that are not adopted at the subsequent meeting?
In principle, the IPA recommends waiting for the adoption of the minutes. The minutes are not deemed as final unless they are adopted by all. However, the Law on Access to Public Documents deems all documents held and produced by public institutions as public documents, including drafts. Therefore, the IPA recommends anonymizing such documents, where appropriate, and allowing access, as appropriate. The IPA recommends notifying the applicant that the document is not final.

Should I report on requests for access to public documents to the IPA if data is incomplete?
The IPA recommends a careful consideration of rules and procedures to ensure that all applications for access to public documents are adequately recorded and reported. In cases where such data is lacking, responsible officials shall provide an estimated number, with accompanying explanation as to the reasons behind incomplete information, as well as steps that the municipality is taking to address such gaps in the future.

Is it possible to restrict the scope and/or volume of data that is requested and can be delivered, especially in cases where CSOs and other external parties request data that takes long to process and prepare (e.g., data ranging over multiple years)?
Every natural person's right to access public documents, and the guarantee and fulfilment of this right by public institutions, constitutes one of the foundations of democratic and transparent institutions. Therefore, applicants may request access at any time and in any form, period, volume, etc.

The IPA notes that public institutions should proactively publish public documents, which will in itself reduce the number of requests for access to these documents. In this vein, an increasing workload may be attributed to backlog in the proactive publication of data. Equally, another bottleneck occurs due to the misguided perception that only the focal point is responsible for publishing data. In fact, every official has the responsibility to publish open data proactively, to

ensure transparency. All in all, the IPA strongly urges municipal officials to take a proactive approach and publish public information as soon as possible upon production, in order to curb the flow of requests.

Furthermore, the IPA encourages municipalities to organize conferences and roundtables with representatives of civil society organizations and media to raise their awareness of access to public documents, but also sensitivities involving personal data protection of individuals.

Can I issue civil status documents to third persons other than the holder of the document (i.e., the person whose name appears in the document)?
The Ministry of Internal Affairs (MIA) has determined that, by default, civil status documents are only issued to the concerned individual, close family members (i.e., parents, siblings, children, spouse), an authorized person or the custodian authority;[10] however, there are exemptions. For example, in cases involving family disputes, access to civil status documents may be restricted for an applicant requesting access to a birth certificate of his/her sibling.

Can I disclose data from representation or hospitality events?
There is a court precedent which allows journalists access to all invoices from such events.[11] Previously, the Kosovo Agency for Protection of Personal Data (predecessor to IPA) ruled that disclosing what items were served at the event (e.g., food and drinks) may disclose religious or other convictions of the officials concerned; however, the decision was overruled by the competent court stating that accountability interests take precedence over other considerations.

The new Law on Access to Public Documents establishes the rule of accessibility of *all* information on expenditure of public money.[12]

Can I disclose names of donors and amounts donated to any fund administered by a public institution?
Before publicising the names of donors and amounts, the institution shall develop a mechanism (e.g., a form) to seek and obtain consent from donors to disclose such information.

Can I provide access to the payroll?
Names of civil servants, and their titles are public. Access to payrolls can be granted upon request;[13] however, personal data such as personal number, date of birth, address, bank account details should be anonymized.

4.3. Subsidies and support schemes

What data can I publish when notifying results of a call for medical subsidy or assistance?
Special care should be exercised regarding health data,[14] as not only is such data protected by Law, but also enjoys an elevated level of protection. In the cases of subsidy for medical treatment, only the responsible officer should be allowed access to data regarding the medical condition of the applicant, rather than the entire municipality. One notable exception in this case are the auditors, as they are public officials with specific mandate to ensure accountability

[10] Administrative Instruction (MIA) No.01/2022 on Civil Status Documents, Article 7.
[11] Available [in Albanian] at: BIRN Fiton Rastin Gjyqësor Ndaj Zyrës së Kryeministrit (kallxo.com)
[12] Law on Access to Public Documents, Article 3, paragraph 3.1.
[13] Ibid Article 17 paragraph 3.1.
[14] Personal data related to physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status" see Article 1.21. of the Law No. 06/L-082 on Protection of personal data.

of public spending. The data published should be anonymized, and the beneficiaries should not be identifiable for external parties, but only to responsible officer.

There are cases when a municipality grants subsidies on the basis of diagnosis, and the names of beneficiaries are subsequently published on the municipal website. In these cases, alternative methods of notification are recommended, such as using protocol numbers, application numbers or similar. The notification detailing beneficiaries may contain the purpose of subsidy (e.g., medical treatment), protocol number and amounts awarded. The IPA also recommends to adopt codes for diagnosis. Please note that, even if certain authorities working on accountability (such as auditors) may be allowed access to information, such access is not granted to the general public. Publishing the name and surname of beneficiaries only is not advised either, as it may trigger undue curiosity about the disease or diagnosis. In these cases, data protection considerations override public interest.

Medical data is sensitive data and such data shall, under no circumstances, be published. This restriction applies not only to subsidy or grant schemes, but also to any notifications issued by municipal directorate of health. Such data should be coded and ensured appropriate technical and organisational security measures. These codes shall be known to municipal officials, but the transparency interests are sufficiently served by disclosing codes, the purpose of award or subsidy and amounts. Access to these data is restricted to relevant municipal officers and auditors.

The IPA notes with concern that medical details are often disclosed by virtue of their publication in a mayor's decision, archives, documents submitted to director of finance for payment and processing, etc. All these officials are privy to data on diagnosis and disease of the applicant; while these data should only be processed and handled by the responsible officer.

Can I publish names of beneficiaries of support schemes in case of accidents or subsidies?
Some accidents (such as house fires) are a matter of public knowledge; therefore, publishing the names of beneficiaries would not violate the privacy of individuals. In the case of subsidies, the transparency interests are served sufficiently by publishing names, surnames and amounts awarded. However, please note that such lists shall not contain any personal information such as phone, address, personal number or similar.

Can I publish the parent's name of a subsidy beneficiary?
The names of parents should only be used in cases when there are two same names in the list, in which case the parent's name shall be initialized. There are no justified reasons to publish parents' names of all individuals in the list, which may often exceed 100 or more beneficiaries. The principle of data minimization, contained in Article 4 of the Law on protection of personal data, shall apply in any personal data processing. In addition to the Law on State Aid and the Regulation on Criteria, standards and procedures for public financing of NGOs[15] by the Ministry of Finance, municipalities also have internal regulations for the allocation of subsidies, which shall be adequately consulted and aligned with data protection provisions.

Can I supply the names of beneficiaries of assistance schemes to municipal assembly members?
Members of the municipal assembly are deemed public officials and, therefore, subject to rules and regulations governed by law. In this sense, as this information serves to fulfil their

[15] LAW NO. 05/L-100 ON STATE AID (rks-gov.net); REGULATION MF - NR - 04/2017 ON CRITERIA, STANDARDS AND PROCEDURES ON PUBLIC FUNDING OF NGOs (rks-gov.net)

legislative oversight and accountability function, they should be granted access. However, members of the municipal assembly shall refrain from making such personal details public.

4.4. Procurement and job competitions

Can I provide access to public documents for an open tendering process?
The e-procurement platform already lists documents detailing tendering procedures, therefore referring the applicant to this platform is sufficient for the purposes of the request for access to public documents.[16] However, if the procedure is disputed, no access should be allowed, pending resolution of the contest procedure.

Are bidding prices made as part of a public tender procedures deemed as a business secret?
No, bidding prices do not constitute a business secret. If the offer submitted to a call for tenders contains personal data or matters of business secrecy, that particular data should be anonymized and access to the rest of information should be allowed.

What data can institutions publish related to job vacancies?
The IPA understands the sensitivities involving recruitment processes, as well as the significant number of persons affected by these processes. Many of the lists of applicants are automatically generated by Human Resources Management Information System (HRMIS) and are published 'as is', unfiltered, whereas, based on the law, these lists should be filtered[17]. While the lists may be retained for official records, the lists shall be cleared of any personal information (e.g., personal number, phones, etc.). In addition, municipalities shall refrain from publishing lists of all candidates who applied, or lists of unsuccessful candidates. Unsuccessful candidates are issued direct notices through HRMIS and, therefore, their names should not be published. In case of doubt, officials should refer to Regulation No. 15/2023 on Admission Procedure in the Civil Service and comply with legal provisions thereunder.

Can I allow access to an application document to third parties?
As a matter of rule, the higher the public position, the less restricted are privacy considerations. In cases of public vacancies, including for schools, the overriding public interest to know who the public official is takes precedence over personal data protection of persons involved in the process. Opposing candidates may be allowed access to application documents to ascertain that the winning candidate met the eligibility criteria of the competition; however, some restrictions apply. Access to diplomas, degrees, training certificates, post-university degrees may be allowed for viewing only. Please note that access to other public documents involving recruitment, such as commission members and evaluations may be allowed on request.

Can I disclose results of written tests from opposing and/or winning candidates?
As stipulated in Article 11 of the Regulation No. 15/2023 on Admission Procedure in the Civil Service, the admission committee shall prepare the final list of candidates who passed the threshold of 70 per cent of the total points, including the name and surname of the successful candidate, and the points obtained in the written test, the verbal interview and total points of each candidate. The list shall be published in the HRMIS, on the institution's website and in other appropriate means of information.

[16] e-Procurement platform.
[17] Law on Access to Public Documents, Article 4, paragraph 3.

What information should I disclose to any requester regarding a subsidy allocation scheme for civil society organizations?
NGOs are not subject to the Law on Protection of Personal Data, as they are legal entities. From the perspective of access to public documents, if a public institution awards funding for NGOs, all data on such funding should be disclosed.

4.5. Video surveillance and visual images

What should I take into consideration for video surveillance?
Public institutions, including municipalities, may install CCTV cameras for the purpose of safety of people and the property, or for protecting the confidentiality of documents inside the municipal premises. However, the municipality should not install CCTV cameras in public areas. Installation of such cameras falls under police authority and is regulated by separate legislation.

Face and voice recognition features in such cameras are prohibited (e.g., at schools, buses, etc.), as such features are in contradiction with their monitoring purpose. The IPA advises municipalities to exclude face or voice recognition features in their tender specifications. Similarly, private businesses should not install cameras incorporating such features in their premises. The IPA has developed a guide on video surveillance for data controllers. Fines for non-compliance range from EUR 4,000 for minor offences to EUR 40,000 for serious violations, or even from 2% to 4% of annual turnover for businesses.

Can teachers, directors and schools post pictures of activities involving children?
The IPA Commissioner has developed a template of privacy policy and distributed it to municipal departments of education, as well as a template of parental consent form for the publication of photographs of children during school activities.[18] This should provide legal basis for schools to engage in any information activities. These documents should also extend to any activities involving third-party organizations (NGOs and similar), whereby the school and these organizations should make adequate arrangements. The form should allow parents the possibility to accept or refuse the publication of a photo. In such cases, adequate arrangements shall be made: for example, taking photos of all children is allowed; however, during publication, adequate masking tools are applied (such as smiley emoji's or blurring).[19]

Are CCTV cameras allowed to operate in schools?
The primary consideration is to ensure that CCTVs do not have face and voice recognition features, as this is inconsistent with the purpose, while also prohibited by Law, especially in schools. Cameras shall not be installed in classrooms, teachers' lounges, toilets and changing rooms and should only cover school perimeters and corridors. Video surveillance systems must be publicly announced and easily identifiable, at the latest where the video surveillance begins. The IPA developed a guide on camera surveillance systems for data controllers including the templates of warning signs.[20]

What CCTV camera brands are allowed or prohibited?
The IPA does not restrict any brand of CCTV cameras; rather, it focuses on features. However, please note that the Public Procurement Regulatory Commission issued guidance related to specific brands of cameras, which may not be offered as part of tendering procedures.

[18] https://aip.rks-gov.net/download/politikat-e-privatesise-drafti-per-shkolle/
[19] The form can be found here: https://aip.rks-gov.net/download/pelqimi-i-prinderit-kujdestarit-per-fotografimin-dhe-incizimin-e-femiut-ne-kopsht-shkolle/
[20] Guide on Camera Surveillance Systems for Data Controllers; Templates of warning signs.

4.6. Relations with the media

Can journalists be denied access to municipal premises?
Journalists serve a public interest; therefore, they will be allowed access to public premises, including without prior notice. However, limitations apply. In case civil servants believe their privacy has been violated by journalists, responsible municipal officials are encouraged to approach the IPA and claim violation of their privacy rights.

Can I deny an interview to a journalist?
Public servants are required to divulge public information as a matter of rule. However, if the institution has media relations and public communication officers, a public servant may refer all questions to such designated officers.

5. Scenarios and recommended actions

Scenario 1: A fight breaks out in a cafeteria and recordings of the fight are posted online. The video recordings also contain audio recordings of conversations in the cafeteria. This may potentially lead to scenarios where casual, private conversations over coffee with friends in the bar where the episode occurred are shared online.

- ↳ **Recommended action:** Recordings produced by cameras installed inside a facility should not be released publicly. If an action has occurred requiring investigation by police authorities, the recordings may be handed over to such authorities. However, recording audio inside a cafeteria is not permitted.

Scenario 2: As there are multiple personal information databases in operation, a municipality and utility companies discuss about merging their databases of addresses. Some utility companies claim that the Kosovo Electricity Distribution Services (KEDS) has the most accurate data.

- ↳ **Recommended action:** KEDS will refuse to share data as it has a contract with residents, which details, among others, how it handles data. Therefore, KEDS should not share them with utility companies and the municipality. A potential solution may be to make a separate database and connect it to property tax.

Scenario 3: To cover and broadcast a donation of five desktop computers to a school by a municipality, TV crews enter classrooms, record children and publish the recording on TV. The mayor posts information of the activity on his/her private Facebook account and on the official municipal webpage.

- ↳ **Recommended action:** Schools should ensure that adequate parent consent has been obtained, preferably at the start of the academic year, but also subsequently for specific events involving publication of personal data or images. To aid schools in the process, the IPA has developed Privacy Policies and Parent Consent Forms which were distributed to municipal departments of education. These policies will govern actions of schools regarding various activities, as the IPA understands the challenges associated with publishing photos or personal information from school activities.

Scenario 4: A retired teacher requests data from his/her employment record in order to arrange a pension claim abroad. The responsible official notes that the documents requested contain data of other persons as well.

- ↳ **Recommended action:** Copies of data records can be shared, provided that data of third persons (e.g., other teachers or individuals) in the list are anonymized.

Scenario 5: An NGO obtains data from a municipality regarding the progress of a building construction project; however, that NGO takes it upon itself to verify the actual status on the ground. The building security, hired by the municipality, notifies the municipality of the incident, and the municipality restricts access to the NGO, arguing that the project is incomplete. The NGO complains to the IPA.

- ↳ **Recommended action:** The IPA would reject the complaint from the NGO because it does not meet the criteria to be considered a request for access to public documents, since the object of the request was to access a publicly owned building.

Scenario: A natural person (i.e., an individual) asks a municipality for access to public documents from a number of years, requiring excessive time to process and teams of persons to respond.

- ↳ **Recommended action:** The IPA would advise the applicant to stagger the request, as the data could not be reasonably produced within the prescribed legal timeframe.

Scenario 6: A former municipal official, who has previously processed official data and documents, submits requests for access to public documents, which he alone handled and possibly hidden. As the municipality is unable to find and provide said data, the IPA is required to issue a fine to the municipality.

- ↳ **Recommended action:** In such case, the IPA would advise municipalities to work closely with the applicant to help identify exactly the kind of data that the applicant requires and allow access, as appropriate.

Scenario 7: A health professional forgets a jacket at a venue covered by CCTV cameras; however, when s/he returns to the site, the jacket is not there. The doctor then asks the responsible officer to view the CCTV footage to identify the potential thief.

- ↳ **Recommended action:** The right to access personal data by the subject of data alone is guaranteed under Law on Protection of Personal Data. In such cases, the responsible officer shall allow access to the subject of data, but will blur the faces of other subjects in the images/sequences. In cases when recordings are asked by the Kosovo Police or the Prosecution, the responsible officer shall maintain a log of access to recordings, which shall contain the name and surname, rank, and identification number of the police officers accessing the records. This is to ensure that recordings are not used for any other purpose. The IPA has developed a guide on video surveillance for data controllers.

Scenario 8: A journalist asks a public institution for access to a 300-page contract of that same institution.

- ↳ **Recommended action:** the responsible officer should anonymize sections and bits of text not deemed relevant for the purpose of the request, regardless of the number of

pages. However, please note that legislation on public procurement provides for a myriad of procedures, rather than a single one. In this regard, the IPA advises to consult other procurement processes to ensure that there is no confidentiality issue due to business and company secrets which would constitute legal grounds for refusing access to public documents.[21] In other words, there can be cases when public procurement files contain information that can qualify as confidential. The IPA is aware of focal points for access to public documents being under pressure to provide access to underlying data, even if the municipality publishes codes. Ultimately, it is the responsibility of the highest administrative official of the public institution, which in the current context is the municipal mayor, to decide on granting that is refusing the access to requested public document.[22]

6. Annex: Principles and considerations on data protection and access to public documents

Principles of data protection

The legal basis on data protection is the Law on Protection of Personal Data.[23] The law specifies seven main principles as cornerstones for access to public documents and data privacy.[24] These are:

1. *Principle of lawfulness, justice and transparency* – personal data are processed in an impartial, lawful and transparent manner, without infringing the dignity of data subjects.

2. *Principle of purpose limitation* – data are collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose.

3. *Principle of data minimization* – personal data shall be adequate, relevant and limited to the purposes for which they are further collected or processed.

4. *Principle of accuracy* – personal data shall be accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. *Principle of storage limitation* – personal data may be stored insofar as necessary to achieve the purpose for which are further collected or processed. After the fulfilment of processing purpose, personal data shall be erased, deleted, destroyed, blocked or anonymised, unless otherwise foreseen in the Law on Archives or in another relevant law.[25]

[21] Article 17 para 2.2.7 of the LAW NO. 06/L-081 ON ACCESS TO PUBLIC DOCUMENTS (rks-gov.net)
[22] *Ibid* Article 11 para. 2.
[23] LAW NO. 06/L –082 ON PROTECTION OF PERSONAL DATA (rks-gov.net)
[24] These principles are listed in Law No. 06/L-082 on Protection of Personal Data article 4 (principles of personal data processing).
[25] LAW NO. 08/L-111 ON ARCHIVES (rks-gov.net)

6. *Principle of integrity and confidentiality* – personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. *Principle of accountability* – the data controller shall be responsible for, and be able to demonstrate compliance with all principles set forth in this article.

While the Law on Protection of Personal Data lays out general principles of data processing, it allows processing of special categories of personal data under specific circumstances (art 8.2).[26]

Municipalities are required to adopt by-laws specifying measures and rules for data security and to assign responsible officers to carry out data processing (art. 37).

Principles on the right to access public documents

As per Article 4 of the Law on Access to Public Documents (basic principles on the right to access public documents):[27]

1. Every person's right to access public documents, and the guarantee and fulfilment of this right by public institutions, constitutes one of the foundations of democratic and transparent institutions.

2. Access to public documents shall be done through proactive publication of public documents by public institutions and upon a person's request for access of public documents.

3. Each person shall have the right to re-use public documents under the conditions and restrictions set forth in the above-mentioned law.

4. The disclosure of data and transparency in the public sector serve for public accountability in terms of social, economic and democratic development and advancement.

5. The right to access public documents belongs to all persons in the same way and equally. Public institutions shall not favour one person in exercising the right to access public documents while disfavouring the others.

6. Restrictions on the right to access public documents shall be made only in limited and specific cases determined by the legislation into force.

Officials responsible for access to public documents are responsible for implementing the law, subject to all provisions and obligations deriving from it, and may be subject to individual fines in case of failure to comply (art. 32.1 and 33.2).

Mayors have an important role to play in raising the awareness of municipal officials on their obligation to provide access to public documents, and to balance such open sharing of

[26] LAW NO. 06/L-082 ON PROTECTION OF PERSONAL DATA (rks-gov.net)
[27] LAW NO. 06/L-081 ON ACCESS TO PUBLIC DOCUMENTS (rks-gov.net)

information with each individual's right to personal data privacy. Moreover, officials responsible for providing information from various municipal directorates (e.g., cadastre, education, health, or public services) can, thorough understanding their responsibilities regarding access to public documents and data protection, can enhance transparency while safeguarding residents' rights.

Considerations on data protection and access to public documents

- The Law on Protection of Personal Data is applicable to the entirety of Kosovo and includes both private and public institutions.
- The Law on Access to Public Documents only applies to public institutions.
- The Law on Protection of Personal Data protects all data of natural persons, but not legal persons.[28]
- The deceased persons do not fall under the purview of the Law on Protection of Personal Data and, therefore, any applications dealing with access to such data should be dealt with under the Law on Access to Public Documents.
- Data on legal entities – for example, a business, NGO, public institution, etc. – are deemed accessible and not protected by the requirements of the Law on Protection of Personal Data, especially when such entities are involved in the spending of public funds.
- In the processing of personal data for purposes of discharge of official duties and responsibilities (these include civil status offices, personnel offices, etc.), data controllers should exercise caution and prohibit use not sanctioned by the Law on Protection of Personal Data (art. 5–10). Cases would involve, for example, an application for civil status documents of a sibling, by a sibling, without due authorization.
- Personal data processing includes access, transmission and disposal. Lawful processing of data should follow these criteria set out in the Law on Protection of Personal Data (art. 5):

    1. The data subject should give personal consent to the processing of his or her personal data for one or more specific purposes;
    2. The processing is necessary for the performance of a contract to which the data subject is a contracting party or in order to take steps at the request of the data subject prior to entering into a contract;
    3. The processing is necessary for compliance with a legal obligation to which the controller is subjected;
    4. The processing is necessary in order to protect the vital interests of the data subject or of another natural person;

[28] In jurisprudence, a *natural person* (sometimes also referred as *physical person*) is an individual human being, while a *legal person* is a public (i.e., government) or private (i.e., business or non-governmental organization) entity.

5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

a. The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to the processing carried out by public authorities in the performance of their tasks.

↳ In addition, municipalities are not only required to harmonize their by-laws with the legislation above, but also issue their own internal acts related to the processing of personal data, including regulations on personal data protection, data processing, or privacy policies, to name a few. The IPA is ready to work with municipalities to ensure that local regulations are fully aligned with the law.