



VOKSHI & LATA
LAW FIRM

DATA PROTECTION

LEGAL GUIDE TO INVESTING IN KOSOVO



13. DATA PROTECTION

Data protection is regulated in Kosovo by The Law on Protection of Personal Data No.06/L- 082 (“Law on Data Protection”) entered into force on 13 February 2019. It transposes the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Another law that includes several dispositions related to the protection of personal data is Law No. 04/L-109 on Electronic Communications (“Law on Electronic Communications”).

13.1. LAW ON DATA PROTECTION

The Law on Data Protection applies to the processing of personal data by public and private bodies and the processing of personal data in diplomatic and consular offices, including any representative office of Kosovo abroad.

The overall control over the purpose and means of the data processing is exercised by the data controller (“controller”). The controller can be a natural or legal person, a public authority, an agency or another body.

The competent authority for the supervision of the implementation of the legislation on personal data protection is the Information and Privacy Agency (“AIP”). It also provides advice to public and private bodies and informs the public on issues related to data protection. The law does not require any registration of processing of personal data to AIP. However, AIP is mandated to deliver and withdraw certification to organizations processing data. AIP may also impose fines to the data controller, up to 40,000 euros for minor violations or 2 to 4% of the annual turnover of the previous year for serious or great violations.

The Law on Data Protection sets in particular the main principles and requirements for data processing; the data subjects’ rights, the obligations of the data controllers and processors; and provides rules governing the international transfer of data.

13.1.1. Main Principles and Requirements

The law on Data Protection sets the main principles which apply to personal data processing:

- Lawfulness, fairness and transparency;
- Limitation to data collection to specified, explicit and legitimate purpose;
- Minimisation: collection and process only of adequate and relevant data and within the purposes of collection and process;
- Accuracy: accurate and up-to-date data. If not, data should be erased or rectified;
- Storage limitation of data to the purpose for which they are collected or processed;
- Integrity and confidentiality of data process, in particular, protection against unauthorized or unlawful processing and against accidental loss, destruction or damage;
- Accountability of the controller of the data for all above-mentioned principles.

Processing of personal data is lawful if the data subject has freely given consent to the processing of his or her data for one or more specific purposes. Processing the personal data of a child under 16 is only possible if the holder of parental responsibility over the child has given consent.

Process of personal data without the subject consent may, however, be legal in certain cases defined by the law, such as when necessary for the performance of a contract, or if the processing is necessary to protect vital interests, to perform a task carried out in the public interest, or for legitimate interests (e.g. data are used in an expected way and there is a minimum impact on privacy).

The data subject can withdraw his consent at any time. The Withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Without the subject explicit consent, specifically prohibited is the processing of:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- Data concerning a natural person's sex life or sexual orientation;
- Genetic or biometric data for the sole purpose of identifying a natural person;
- Data concerning health;
- Law on Data Protection however sets several exceptions to these prohibitions

The data subject may however give explicit consent to the processing of the above-mentioned data unless the relevant legislation provides that the prohibition may not be lifted. Law on Data Protection also sets other exceptions to this prohibition, such as:

- When necessary, in the field of employment, social security and social protection;
- To protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- Within certain limitations, for non-profit organizations;
- If processing is necessary for legal claims or courts action,
- For public interest, medical and health reasons,
- For archiving purposes in the public interest, scientific or historical research or statistic purposes.

Even in the above-mentioned exceptions, Law on Data Protection sets limits to the processing, which, in particular, must be performed in compliance with the protection of the rights and fundamental interests of the data subject.



13.1.2. Data Subjects' Rights

• Right to information

Data subjects must be informed whenever their personal data is being processed. This applies both when data is collected directly from the individual and when it is obtained from other sources.

They must be informed of the identity and contact details of the controller, the data protection officer (if applicable), the purpose and legal basis of the processing, the recipients of the data, and whether the data will be transferred outside the country.

In addition, they must be informed of the data retention period, the right to access, rectify, or delete their data, the right to withdraw consent, the existence of automated decision-making including profiling, and the right to file a complaint with the Information and Privacy Agency.

• Right to access:

In any case, the data subject shall have confirmation as to whether or not his or her data are being processed, and if so, access to it and to some information such as:

- the purpose of the processing;
- the identity and contact details of the controller and the contact details of the data protection officer (if applicable);
- the categories of data;
- the recipients or categories of recipients of the personal data;
- the period of storage or, at least, the criteria used to determine it;
- the existence of the right to rectification, deletion, restriction and objection (see below) and of the right to lodge a complaint with AIP;
- In case the controller intends to transfer the data to a third country or international organization, the data subject should be informed of it and of his rights relating to the transfer;
- the right to withdraw consent to process personal data
- the existence of automated decision-making, including profiling, its significance and envisaged consequences.

If there are statutory or contractual requirements to collect data, the *data subject, whose information is collected*, must be informed of such requirements and their consequences.

When data are not collected from the data subject, the controller must inform the subject of the source of personal data, and if applicable, whether it came from publicly accessible sources. In this hypothesis, the right to information does not apply in certain situations, such as when the data subject already has the information; or when the provision of such information proves impossible or would involve a disproportionate effort (especially for archiving purposes in the public interest, scientific, historical or statistical purposes); when there is, regarding the data, an obligation of professional secrecy.

• *Rights to rectification and deletion*

The data subject has the right to obtain from the controller the rectification of inaccurate personal data concerning him or her, and the right to have incomplete data completed including by providing a supplementary statement.

The data subject has the right to obtain deletion of his or her personal data if he or she withdraws consent. Law on Data Protection also sets other grounds for the right to deletion, such as when the personal data are no longer necessary in regards to the purpose of the process; the data subject objects (cf. below, right to object); the personal data has been unlawfully processed; the data must be erased in compliance with a legal obligation, etc.

However, the right to deletion shall not apply in certain situations, including when processing is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation or for public interest, for public health reasons, for archiving purposes in the public interest, for legal claims.

• *Right to restriction*

As an alternative to deletion, the data subject has the right to restrict the processing of their personal data when:

- the accuracy of the personal data is contested by the data subject;
- the data has been unlawfully processed;
- the controller no longer needs the personal data but the data subject requires it to establish, exercise or defend a legal claim;
- the data subject has exercised his or her right to object (see below) pending the verification of whether the legitimate grounds of the controller override those of the data subject.

If data is restricted, except to store it, data can only be processed with the data subject's consent; or for the establishment, exercise or defence of legal claims; or for the protection of the rights of another person (natural or legal); or for reasons of important public interest.

• *Right to Data Portability*

Data subjects have the right to receive the personal data they have provided to a controller and to transmit it to another controller without hindrance, where the processing is based on consent or contract and carried out by automated means.

• *Right to Object*

Individuals may object at any time to the processing of their personal data, especially when it is based on legitimate interests or conducted for direct marketing purposes. If no compelling legitimate grounds exist that override the interests of the data subject, the controller must cease the processing.

• *Automated Decision-Making and Profiling*

Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects them in a similar way.

13.1.3. Obligation of Data Controller and Processor

• Controller

The data controller (“controller”) is any natural or legal person, public authority, agency or other body which, alone or jointly, determines purposes and means of personal data processing.

The controller shall implement measures to ensure compliance of processing with the Law on Data Protection. The controller shall implement appropriate technical and organisational measures, such as pseudonymization, and data minimisation, and integrate the necessary safeguards in order to protect the rights of data subjects.

The controller shall implement appropriate technical and organisation measure to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Personal data should not be made accessible without the individual’s intervention to an indefinite number of persons.

In the case the controller becomes aware of a personal data breach, the controller shall, if possible, within 72 hours, notify the Information and Privacy Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the data breach to the data subject without undue delay, unless:

- ☐ the controller has implemented protection measures, in particular rendering the data unintelligible, such as encryption;
- ☐ the controller has taken measures to ensure that the risk is no longer likely to materialise;
- ☐ it would involve disproportionate effort whereas a public communication would be sufficient to ensure effective information of the data subjects.

If processing is carried out by a processor the controller shall use only processors providing sufficient guarantees to implement measures to ensure compliance of processing to the Law on Data Protection and protection of the rights of the data subject.



• Processor

The data processor (“processor”) is a natural or legal person, from the public or private sector who processes personal data for and on behalf of the data controller.

The processor must be appointed by a binding agreement with the controller, which states that the processor must:

- ☐ only act on the controller’s documented instructions;
- ☐ impose confidentiality obligations to all personnel who process the relevant data;
- ☐ ensure the data safety of the processed personal data;
- ☐ respects rules related to the appointment of sub-processors (see below);
- ☐ implement measures to assist the controller in complying with the rights of data subjects;
- ☐ at the choice of the controller, delete or return all the personal data to the controller at the end of service, and delete existing copies (unless Law on Archives requires data storage);
- ☐ provide the controller with all information necessary to demonstrate compliance with the above-mentioned obligation and allow for and contribute to audits conducted by the controller or another auditor mandated by the controller.

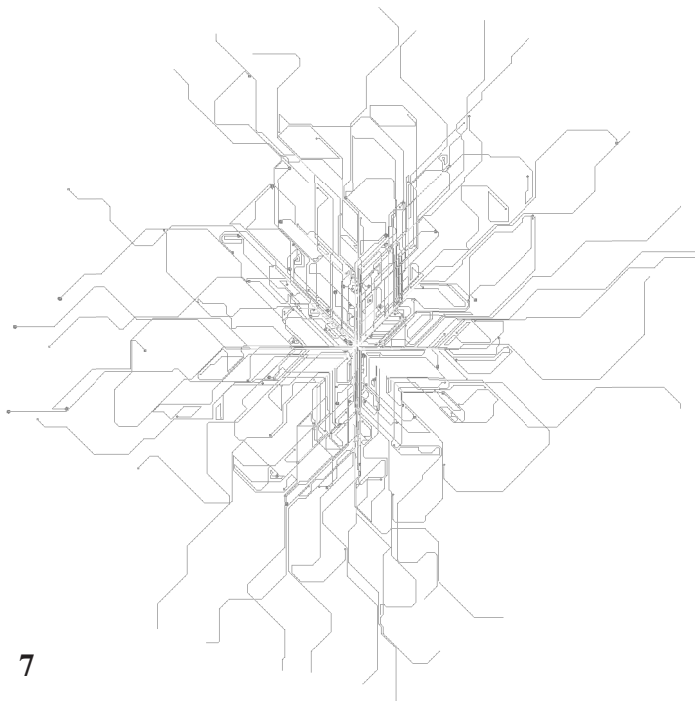
The data processor may act only within the constraints of the controller’s authorizations and is not entitled to process personal data for other purposes.

The processor shall notify the controller without undue delay of any personal data breach.

The processor shall not engage another processor (sub-processor) without prior specific or general written authorisation of the controller. In the case of general authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. In the case of specific authorisation, the obligation applicable to the processor applies to the sub-processor, but the initial processor remains fully liable to the controller.

Processors and if applicable, their representatives, must keep records of their processing activities performed on behalf of the controller

In case of a dispute between the data controller and processor, the processor should, upon the controller’s request, return all the data, without any right to keep copies or any right of further process.



- Data Protection Officer (DPO)

The Data Protection Officer (DPO) is a key figure in the implementation of the Law on Personal Data Protection in Kosovo. The appointment of a DPO does not depend solely on the size of the organization, but on the nature and intensity of the processing of personal data, especially when it involves sensitive or large-scale processing that may have a significant impact on the rights and freedoms of individuals.

According to the Law on Personal Data Protection (LPDP) in Kosovo, the controller and processor must appoint a DPO in every case if:

- The processing is carried out by a public authority (courts acting in their judicial capacity are exempt);
- The core activities of the controller or processor consist of processing operations which, by virtue of their nature, scope, or purposes, require regular and systematic monitoring of data subjects;
- The core activities of the controller or processor consist of large-scale processing of special categories of data and personal data relating to criminal convictions and offenses.

The Data Protection Officer must operate independently within the organization. Their primary responsibilities include:

- Informing and advising the controller or processor and their employees involved in data processing about their obligations concerning data protection;
- Providing advice, as needed, regarding data protection impact assessments and monitoring performance;
- Direct cooperation with the Information and Privacy Agency (IPA), serving as the main point of contact.

A DPO must have deep knowledge in the field of data protection, law, and privacy practices, as well as a good technical understanding of how data is processed within the organization. Key qualifications include:

- Legal expertise in data protection and human rights;
- Technical knowledge of information security and risk management;
- Good communication skills and staff training abilities;
- Practical experience in implementing international privacy standards, e.g., GDPR.

Organizations may choose either an internal employee or an external professional for this role, depending on their size and needs.

The law requires that the appointment of the DPO be notified to the Information and Privacy Agency in Kosovo. This notification:



- Ensures transparency regarding the persons responsible for data protection within organizations;
- Facilitates communication between the IPA and the DPO;
- Contains contact details and other relevant information for the effective functioning of the DPO.

• ***Representatives of controllers or processors not established in Kosovo***

If the controller or processor is not established in Kosovo, the controller must designate in written a representative in Kosovo. There is however some case when this obligation however doesn't apply, to processing on a small scale which does not involve prohibited personal data, and to public authority or body.

The representative must be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor.

• ***Personal data safety***

In order to achieve an appropriate level of security to ensure the protection of the data subject's rights, the controller or the processor may use:

- ☐ pseudonymization and encryption of personal data;
- ☐ ongoing reviews of security of processing systems and services;
- ☐ redundancy and backup abilities;
- ☐ regular security tests, assessments and evaluations.

Should be taken into account, in particular, the risks that may result from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

13.1.4. International Transfer of Data

The transfer to other countries and international organizations of personal data that are processed or are intended to be processed after transfer may take place if the country or the international organization in question ensures an adequate level of data protection. The list of such countries is established by the Information and Privacy Agency.



- ☐ it is so provided by another law or binding international treaty
- ☐ the data subject has given his or her consent;
- ☐ the transfer is necessary for the performance or implementation of a contract between the data subject and the controller or of a contract concluded in the data subject's interest;
- ☐ the transfer is necessary for public interest, for the protection of the vital interest of the data subject, for the establishment, exercise or defence of legal claims;
- ☐ the transfer is made from a public register;
- ☐ the data controller adduces adequate safeguards for the protection of personal data and the fundamental rights and freedoms of individuals as regards the exercise of adduced rights.

13.2. PRACTICAL GUIDE: HOW TO START COMPLYING WITH THE PERSONAL DATA PROTECTION LAW IN YOUR BUSINESS

This chapter provides a practical roadmap for businesses to begin complying with the Law on Personal Data Protection. It outlines clear steps, from assessing current practices to establishing policies and safeguards, that help build a responsible and effective data protection framework.

1. Assess the current state of your data processing and management!

Start by conducting an inventory of the data you collect and process, and determine whether they include personal data, sensitive data, or data used for monitoring and advanced analyses.

This step is essential to understand the level of compliance with the Law and to identify the main risks.

2. Appoint or contract a responsible person for data protection, and, where required, engage a Data Protection Officer (DPO)!

Every organization should have a responsible person within its structure who monitors compliance with the Personal Data Protection Law. This person can be an internal employee or an external professional who ensures that data processing procedures are correctly followed, staff are trained, and processing records are regularly maintained.

If your activities involve sensitive or large-scale processing, or if you are a public institution, it is mandatory to appoint a DPO. The DPO serves as the main point for legal and technical advice and is responsible for communicating with the Information and Privacy Agency (IPA). Make sure the DPO's appointment is notified to the IPA for transparency and effective operation.

3. Create and maintain processing records!

According to Article 39 of the Law on Personal Data Protection, every processing activity must be documented: purpose, data categories, recipients, retention periods, and security measures.

For businesses, it is useful to use a standard form for each activity, keep records in a central location, and update them regularly according to changes in processes or partners handling data.

Such practice helps demonstrate legal compliance, identify risks, and improve personal data management within the organization.

4. Develop internal policies and procedures!

Draft data protection policies, procedures for handling data subject requests, and breach management processes, ensuring that staff are informed and trained on these policies.

5. Conduct a data protection impact assessment!

When your activities process data that pose a high risk to individuals' rights and freedoms, carry out a Data Protection Impact Assessment (DPIA).

For businesses, this means identifying risks, documenting the measures you take to minimize them, and preparing for any inspection or request from the IPA.

This step helps avoid serious breaches and demonstrates commitment to data protection.

6. Take appropriate security measures!

Implement technical and organizational measures to protect data: encryption, pseudonymization, access control, recovery procedures in case of incidents, and regular security system testing.

These measures minimize risks and demonstrate compliance with the Law on Personal Data Protection.

7. Create a plan for data breach incidents!

Develop procedures for notifying breaches, specifying how and when the IPA and, when necessary, the data subject will be informed.

Keep complete documentation of every incident to ensure traceability and accountability.

8. Monitor and continuously improve!

Regularly check compliance, improve processes, and train staff. This ensures data protection, minimizes risks, and builds a culture of privacy respect within the organization.

9. Consult with experts!

In cases of legal or technical uncertainty, seek assistance from a DPO, lawyers, or specialized consultants. Preventing mistakes is always easier and less costly than resolving breaches.

Not all of these measures may be necessary for your specific case. Starting with expert consultation allows you

to avoid unnecessary expenses, prevent fines, and ensure that your operations comply with the Personal Data Protection Law in the most precise and efficient way.

Complying with the Personal Data Protection Law may seem challenging, but a structured approach makes it manageable. Every step you take not only minimizes legal risks but also strengthens trust with clients and business partners.

The first step is always the most important. Start now and build a reliable and sustainable data protection system.

13.3. SANCTIONS AND FINES FOR PERSONAL DATA BREACHES

The Law on Personal Data Protection is a binding legal obligation that imposes direct responsibilities on controllers and processors. Violations can lead to significant financial penalties, reputational damage, and loss of client trust.

13.3.1. Powers of the Information and Privacy Agency (IPA)

The IPA can inspect, audit, and investigate data processing activities, either on its own initiative or based on complaints. During inspections, the Agency may:

10. Review processing records, data security documentation, and filing systems;
11. Inspect premises and technical measures;
12. Seize or examine relevant documentation.

Following inspections, the IPA can:

- Order correction of irregularities (e.g., deletion, anonymization, or blocking of data);
- Temporarily restrict or prohibit data processing;
- Enforce data subject rights;
- Impose fines;
- Issue warnings or advice for minor violations.

13.3.2. Administrative Fines

Fines are determined based on the nature, gravity, and duration of the infringement, whether it was intentional or negligent, prior violations, cooperation with the Agency, and the type of data affected.

- Up to €40,000: unlawful data processing, inadequate protection, breaches involving video surveillance or biometric data, or failure to follow DPO supervision.
- Up to €12,000: violations of video surveillance in apartment buildings.
- Up to €10,000: breaches of direct marketing rules or general video surveillance provisions.
- Up to €8,000: violations related to building access data or DPO supervision.
- Up to €5,000: breaches regarding interconnection of filing systems.

For serious and widespread violations, fines may reach €20,000–€40,000 or 2–4% of a company's annual turnover, aligning with EU GDPR principles.

13.4. LAW ON ELECTRONIC COMMUNICATIONS

The Law No. 04/L-109 on Electronic Communication (“Law on Electronic Communications”) which includes specific dispositions related to the processing of personal data.

For example, regarding the confidentiality of communications, can be highlighted the two following dispositions:

- the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information such as the purposes of the processing, and is offered the right to refuse such processing by the data controller.
- Entrepreneurs should take measures on the electronic communications systems and data processing systems to keep the secret of electronic communications and personal data, as well as to prohibit unauthorized access to the electronic communications systems and data processing systems.

Among other dispositions, the law on Electronic Communications also sets the principles of:

- Deletion of traffic data when no longer needed for the purpose of the transmission of communications;
- information of the types of traffic data processed and duration of such processing;
- Processing for the purpose of marketing electronic communications services only for the duration necessary for this purpose and the possibility of the user or subscriber to withdraw his or her consent at any time;
- Information of the subscriber or user of the types of traffic data processed and duration of the processing;
- Information of the users or subscribers, prior to the consent, of the type of location data processed and whether the data will be transferred to a third party;
- Possibility of the user or subscriber to withdraw his or her consent for the processing of location data at any time.

