DATA PROTECTION LAWS OF THE WORLD

Albania

ALBANIA

Last modified 27 December 2022

LAW

The Republic of Albania regulates personal data protection pursuant to Law No. 9887, dated 10 March 2008 "On Protection of Personal Data", as amended ("**Data Protection Law**") (Official Gazette of the Republic of Albania No. 44, dated 1 April 2008). The Data Protection Law was last amended in 2014, thus it is yet to be harmonized with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**").

The complete harmonization of the current Albanian legislation in force on data protection with the GDPR has been one of the main objectives of the Office of Information and Data Protection Commissioner since 2018, however this objective has yet to be achieved (due in part to the Covid-19 pandemic).

In June 2022 the Ministry of Justice of the Republic of Albania launched a public consultation process on a draft law “On Personal Data Protection” which is approximated with the GDPR. As of December 2022 this draft law has yet to be approved by the Albanian Parliament.

Earlier in the year, on 28 January 2022, Albania signed the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which was later ratified by Law No. 49/2022, dated 12 May 2022 “ *On the Ratification of the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*”.

DEFINITIONS

Definition of Personal Data

Data Protection Law defines personal data as any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Definition of Sensitive Personal Data

Data Protection Law defines sensitive data as any information related to a natural person referring to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal prosecution, as well as data concerning his health and sexual life.

NATIONAL DATA PROTECTION AUTHORITY

The Right to Information and Data Protection Commissioner (the "**Commissioner**") is the Albanian independent authority in charge of supervising and monitoring the protection of personal data and the right to information by respecting and guaranteeing

the fundamental human rights and freedoms in compliance with the legal framework.

The Commissioner is a public legal person, elected by the Parliament upon a proposal of the Council of Ministers for a 5-year term, eligible for re-election. The Parliament also designates the organizational structure of the Commissioner’s Office.

The information obtained by the Commissioner while exercising his duties shall be used only for supervisory purposes in compliance with the legislation on the protection of personal data. The Commissioner shall remain under the obligation of confidentiality even after the termination of his functions.

The Commissioner is seated at Rr. "Abdi Toptani", Nd. 5, 1001, Tirana, Albania.

REGISTRATION

Data Protection Law provides for the legal obligation of every controller to notify the Commissioner on the processing of personal data for which it is responsible. The notification shall be made before the controller processes the data for the first time, or when a change of the processing notification status is required.

The notification shall contain the name and address of the controller, the purpose of personal data processing, the categories of data subjects and personal data, the recipients and categories of the recipients of personal data, the proposal on the international transfers that the controller aims to carry out and a general description of the measures for the security of personal data. The notification is done either online, on the website of the Commissioner, or manually, by submitting the completed notification form to the Commissioner's Office.

The information submitted by the data controller through the notification, except for the general description of the measures for the security of personal data, shall be published by the Commissioner’s Office on the Electronic Register of Controllers which is accessible by the public on the official website.

The notification process and the publication of the information it contains is fundamental to ensure transparency for the public and consequently to protect personal data. Through the access to the Electronic Register of Controllers, the public has the means of understanding how personal data are processed by the controlling entities.

The failure of the controlling entities to comply with the obligation to notify the Commissioner constitutes an administrative offence and is punishable by a fine.

However, there are cases when the controllers are exempted from the notification obligation as follows:

- The processing of personal data is performed in order to keep a register, which in accordance with the law or sub-legal acts provides information for the public;
- The processing of personal data is performed in order to protect the constitutional institutions, national security interests, foreign policies, economic or financial interests of the state, or for the prevention or prosecution of criminal offences;
- The processing of data is done pursuant to Decision of the Commissioner No. 4 "On the Determination of the Cases Exempted from the Notification Obligation of the Personal Data which are Processed", dated 27 December 2012.

DATA PROTECTION OFFICERS

In compliance with the responsibility to issue instructions on measures to be undertaken for the activity of specific sectors, the Commissioner has issued two instructions:

- Instruction No. 22 "On the Determination of Rules for Maintaining the Security of Personal Data Processed by Small Processing Entities", dated 24 September 2012, as amended.

Small processing entities shall mean the controllers or processors that process personal data by way of electronic or manual means, by fewer than six processing persons, either directly or through processors.

- Instruction No. 47 "On the Determination of Rules for Maintaining the Security of Personal Data Processed by Large Processing Entities", dated 14 September 2018.

Large processing entities shall mean the controllers or processors that process personal data by way of electronic or manual means, by six or more processing persons, either directly or through processors.

Personal data processing entities are responsible for the internal supervision of the protection of the processed personal data. Each subject that is subject to instruction no. 47, dated 14 September 2018 (i.e., large processing entities), shall authorize in writing at least one Data Protection Officer ("**DPO**") *(Albanian terminology: Contact Person)* who shall be charged to carry out the internal supervision. Small processors contracted by large processors are also advised to appoint a DPO.

Instruction no. 47, dated 14 September 2018 determines the criteria that a person must fulfil in order to be appointed as a DPO, as well as the duties and responsibilities of a DPO, which include, among others:

- the internal supervision of the fulfilment of the obligations for the protection of personal data by the personal data processing entity;
- the implementation of technical, organizational and staff related measures;
- the necessary cooperation with the Commissioner;
- etc.

COLLECTION & PROCESSING

Data Protection Law states that fair and lawful processing is one of the core principles for the protection of personal data. Personal data shall be collected and/or processed for specific, clearly defined and legitimate purposes.

Personal data protection is based on data adequacy, data which are relevant to the purpose of their processing and not excessive in relation to such purpose, as well as data accuracy, data which are updated and complete.

Additionally, the data are to be kept in a form that allows the identification of data subjects for no longer than it is necessary for the purpose for which they were collected or further processed.

Data Protection Law provides for the legal criteria for personal data processing, sensitive data processing and special processing of data.

Personal data may be processed only:

- with the consent of the personal data subject;
- if necessary, for the performance of a contract to which the data subject is a party or in order to negotiate or amend a draft/contract at the request of the data subject;
- to protect the vital interests of the data subject;
- to comply with a legal obligation of the controller;
- for the performance of a legal task of public interest or in exercise of powers of the controller or of a third party to whom the data are disclosed;
- if the processing is necessary for the protection of the legitimate rights and interests of the controller, the recipient or any other interested party. However, in any case, the processing of personal data cannot be in clear contradiction with the data subject's right to protection of personal life and privacy.

The processing of personal data in the field of national security, criminal law and crime prevention, shall be performed by official authorities as stipulated in the law.

The controller or processor that processes personal data for the purpose of offering business opportunities or services may use personal data obtained from a public data list. The controller or processor cannot process these data further, if the data subject has expressed his disagreement or has objected their further processing.

It should be noted that additional personal data cannot be added to the data obtained from the public data list without the consent of the data subject. However, the controller is allowed to keep these personal data in its filing system even after the data subject has objected the processing. Such data can be used only if the data subject gives his content.

Collection of personal data which is related to a data subject solely for reasons of direct marketing is allowed only if the data

subject has given his explicit consent.

Sensitive data may be processed only if:

- the data subject has given his consent, which may be revoked at any given moment making any further processing of data illegal;
- it is in the vital interest of the data subject or another person and the data subject is physically or mentally incapable of giving his consent;
- it is authorized by the responsible authority for an important public interest, under adequate safeguards;
- it is related to data which are widely made known by the data subject or it is necessary, for exercising/protecting a legal right;
- the data are processed for historic, scientific or statistical purposes, under adequate safeguards;
- the data are required for the purposes of preventive medicine, medical diagnosis, the provision of health care, treatment or management of health care services and the data are used by the medical personnel or other persons with the obligation to preserve confidentiality;
- the data are processed by non-profit political, philosophical or religious organizations and trade unions for purposes of their legitimate activity, only for members, sponsors, or other persons related to their activity. These data shall not be disclosed to a third party without the consent of the data subject unless otherwise stipulated by law.
- the data processing is necessary for the purpose of fulfilling the legal obligations and specific rights of the controller in the field of employment in compliance with the Labour Code.

Special processing of data:

- Processing for historical, scientific and statistical purposes:

Personal data collected for any purpose, may be further processed for historic, scientific or statistical purposes, provided that the data is not processed in order to take measures or decisions related to an individual.

The transmission of sensitive data for scientific research shall take place only in case of an important public interest. Personal data shall be used exclusively by individuals who are bound by the obligation of confidentiality. When data processing is made in a manner that allows the identification of the data subject, the data should be encrypted immediately in order for the subjects to be no longer identifiable. Encrypted personal data shall be used exclusively by individuals bound by the obligation of confidentiality.

- Processing of personal data and freedom of expression:

The Commissioner has issued an Instruction No. 31, dated 27 December 2012 "On the Determination of the Conditions and Criteria for the Exemption from the relevant Obligations in Personal Data Processing for Journalism, Literature or Artistic Purposes". The exemptions for these purposes shall be allowed up to the extent that they reconcile the right of personal data protection with the rules governing the right to freedom of expression.

TRANSFER

The international transfer of personal data may be carried out with recipients from states which have an adequate level of personal data protection. The level of personal data protection for a state is established by assessing all circumstances related to the nature, purpose and duration of the processing, the country of origin and final destination, as well as the legal provisions and security standards in force in the recipient state.

Pursuant to the Decision of the Commissioner No. 8, dated 31 October 2016 the following states have an adequate level of data protection:

- European Union member states;
- European Economic Area states;
- Parties to the Convention No. 108 of the Council of Europe "For the Protection of Individuals with regard to Automatic Processing of Personal Data", as well as its 1981 Protocol, which have approved a special law and set up a supervisory authority that operates in complete independence, providing appropriate legal mechanisms, including handling complaints,

investigating and ensuring the transparency of personal data processing;
- States where personal data may be transferred, pursuant to a decision of the European Commission.

International transfer of personal data with a state that does not have an adequate level of personal data protection may be done if:

- it is authorized by international acts ratified by the Republic of Albania which are directly applicable;
- the data subject has given his consent for the international transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken in addressing a request of the data subject, or the transfer is necessary for the conclusion or performance of a contract between the controller and a third party, in the interest of the data subject;
- it is a legal obligation of the controller;
- it is necessary for protecting vital interests of the data subject;
- it is necessary or constitutes a legal requirement over an important public interest or for exercising and protecting a legal right;
- it is done from a register that is open for consultation and provides information to the general public.

Pursuant to the Data Protection Law, the Commissioner issues instructions in order to allow certain categories of personal data to be transferred to a state that does not have an adequate level of personal data protection. In these cases, the controller is exempted from the authorization request. Accordingly, the Commissioner has issued the Instruction No. 41, dated 13 June 2014 "On allowing some categories of international transfers of personal data in a country that does not have an adequate level of personal data protection".

Controllers wishing to transfer personal data to other countries lacking adequate personal data protection, may fill in an application form "*For the approval of the transfer of personal data to a state that does not have an adequate level of data protection, through the authorization of the Commissioner*".

In 2014, the Commissioner has also issued a Manual on the International Transfer of Personal Data which provides guidelines to the international transfer of personal data.

The exchange of personal data with the diplomatic representations of foreign governments or international institutions in the Republic of Albania shall be considered an international transfer of data.

SECURITY

Data Protection Law introduces the obligation of the data controller or processor to undertake appropriate organizational and technical measures to protect personal data from unlawful or accidental destruction, accidental loss, or from being accessed or disclosed by unauthorized persons, as well as from any kind of unlawful processing.

The controller is under the obligation to document the measures it has undertaken to ensure protection of personal data, in compliance with the law and other legal regulations.

The data controller undertakes the following special security measures:

- defines the functions among the organizational units and the operators for the use of data;
- the use of data shall be done by order of authorized organizational units or operators;
- instructs all operators on their obligations arising from the data protection legal framework;
- prohibits access of unauthorized persons to the working facilities of the data controller or processor;
- data and programs shall be accessed only by authorized persons;
- prohibits access to and use of the filing system by unauthorized persons;
- data processing equipment shall be operated only with an authorization and every device shall be secured with preventive measures against unauthorized operation;
- records and documents data alteration, rectification, erasure, transfer etc.

The level of security shall be in compliance with the nature of personal data processing. The Commissioner has established the detailed rules for personal data security by means of Decision No. 6, dated 05 August 2013 "On the Determination of Detailed Rules for the Security of Personal Data".

The recorded data may only be used in accordance with their collection purpose, unless they are used to guarantee national security, public security, for the prevention or investigation of a criminal offence, or prosecution of the author thereof, or of any infringement of ethics of the regulated professions.

The data documentation shall be kept for as long as it is necessary for their collection purpose.

The obligation of confidentiality and integrity of the controllers, processors and any other persons that come to know the content of the processed data while exercising their duty shall survive the termination of their functions. The processed data shall not be disclosed unless provided otherwise by law. Anyone acting under the authority of the controller or the processor shall not process the personal data to which they have access, without the authorization of the controller, unless obliged by law.

BREACH NOTIFICATION

Data Protection Law does not provide for a general obligation of the data controller or data processor to notify the Commissioner in case of personal data breach.

However, pursuant to Instruction No. 47, dated 14 September 2018 "On the Determination of Rules for Maintaining the Security of Personal Data Processed by Large Processing Entities", which, as mentioned above applies only to large data processing entities, the DPO shall promptly notify the large data processing entity in writing of any risk of violation of the data subjects' rights, including in case of the violation of personal data protection legislation.

In the event that, following the notification of the DPO, the large data processing entity fails to take appropriate measures to address the problem in a timely manner, the DPO notifies the Commissioner without delay. Therefore, in case of breach of data handled by a large data processing entity, resulting from the violation of violation of the data subjects' rights, or from the violation of personal data protection legislation, which has not been addressed effectively, the DPO has the obligation to notify the Commissioner.

It should also be noted, that pursuant to an opinion of the Commissioner on the protection of personal data on the websites of public and private controllers, data subjects have the right to be notified by the data controller if their personal data have been compromised (data has been lost or stolen, or if their online privacy is likely to be negatively affected). To the best of our understanding the opinion expressed by the Commissioner in this opinion, merely serves as a guideline and has not a binding effect.

On the other hand, Law No. 9918, dated 19 May 2008 "On Electronic Communications in the Republic of Albania", as amended ("**Electronic Communications Law**"), (Official Gazette of the Republic of Albania No. 84, dated 10 June 2008) provides for another breach notification procedure.

The Electronic Communications Law defines personal data breach as *any breach of security leading to the destruction, loss, alteration or unauthorized distribution, accidental or unlawful, or access to personal data transmitted, stored or processed, in connection with the provision of an electronic communications service available to the public.*

Pursuant to article 122 of the Electronic Communications Law, entrepreneurs of public electronic communications networks and services are under the obligation to, individually or when necessary, in cooperation with each-other, implement technical and organizational measures, to ensure the security of networks and/or services, provided by them.

These measures are meant to ensure an adequate level of protection and security of personal data against potential, foreseeable risks. With respect to the personal data of the users, entrepreneurs of public electronic communications networks and services are under the obligation to inform their users about any specific risk, how the risk can be reduced by the users, as well as the possible costs, which must be covered by the user, if the risk that happens is beyond the measures that the entrepreneur can take.

In addition, in case of personal data breach, the entrepreneur who provides electronic communications services available to the

public promptly notifies the Authority of Electronic and Postal Communications ("**AEPC**"). When the breach of personal data may adversely affect the personal data and privacy of the subscriber or individual, the entrepreneur shall also promptly notify the said subscriber or individual.

However, if the entrepreneur has proved to the AEPC that it has implemented the necessary technological protection measures and these measures have been applied to the relevant data, then the entrepreneur is not required to notify the subscriber or the individual of the violation of personal data. These technological safeguards ensure that the personal data become illegible to any person who does not have authorized access to the data.

ENFORCEMENT

The Commissioner is the competent authority for the supervision and enforcement of Data Protection Law. The Commissioner has the right to:

- conduct administrative investigations, have access to personal data processing and collect all the necessary information in order to fulfil his supervisory obligations;
- order the blocking, erasure, destruction or suspension of the unlawful processing of personal data;
- give instructions prior to the processing of data and ensure their publication.

In cases of recurring or intentional serious infringement of the Data Protection Law by a controller or processor, the Commissioner acts in compliance with article 39 of Data Protection Law and reports the case publicly or reports it to the Parliament and the Council of Ministers.

Article 39 (1) of Data Protection Law specifies that data processing in violation of the Data Protection Law constitutes administrative offences and may be subject to administrative fines which vary from 10,000 ALL (approx. 83 EUR) to 1,000,000 ALL (approx. 8300 EUR), with legal persons being subject to double the amount specified herein.

Data Protection Law also states that the fine is doubled when the following provisions are breached:

- When the data subject has filed a complaint, the controller shall have no right to make any changes to the personal data until a final decision is reached.
- The Commissioner is responsible for authorizing, in special cases, the use of personal data for purposes not designated during the phase of their collection in compliance with the principles of the Data Protection Law.

The sanctioned subject may appeal the fine in court within the deadlines and according to the procedures that regulate the administrative trials.

Fines shall be paid no later than 30 days from their issuing. When the deadline expires, the decision becomes an executive title and is executed in a mandatory manner by the bailiff's office, upon request of the Commissioner. Fines are cashed in the state budget.

In case the offence consists in a crime, the Commissioner files the relevant criminal charges with the competent law enforcement authorities.

ELECTRONIC MARKETING

Data Protection Law provides that the collection of personal data related to a data subject, solely for reasons of direct marketing is allowed only if the data subject has given his explicit consent.

Data Protection Law defines direct marketing as *the communication of the promotional material, by every means and way, using personal data of legal or natural persons, agencies or other entities with or without interference.*

Moreover, the data subject has the right to demand the controller not to start processing, or in case the processing has started, to stop processing personal data related to him for the purposes of direct marketing and to be informed in advance before personal data are disclosed for the first time for such purpose.

The Commissioner has issued an Instruction no. 06, dated 28 May 2010 "On the correct use of SMSs for promotional purposes,

advertising, information, direct sales, via mobile phone". This instruction emphasizes the importance of the prior consent given by the data subject.

In addition, pursuant to article 124 of the Electronic Communications Law, electronic communications service providers may process traffic data for marketing purposes only after prior approval by the subscriber. Subscribers should be informed on the type of traffic data being processed, before give approval for their processing. Subscribers and users have the right to withdraw to any time from the approval they have made.

ONLINE PRIVACY

The Data Protection Law does not provide for regulatory measures targeting cookies. Accordingly, the general data protection rules, as provided for by the Data Protection Law apply to online privacy as well.

Although there are no specific regulatory measures under the data protection regulatory framework, the Commissioner has tried to provide some clarifications on the notion of cookies and on their use, albeit in a minimalist way.

The Commissioner has defined the cookies in an online dictionary as *some data stored on the computer, which contain specific information.* This rudimentary definition is further complemented by a short explanation which states that cookies *allow any server to know what pages have been visited recently, just by reading them.*

In addition, the Commissioner has issued an opinion (which is slightly dated and as mentioned above does not have a binding effect on the data controllers) on the protection of personal data on the websites of public and private controllers. In this opinion the Commissioner reminds the data controllers on their obligations per the Data Protection Law and on the rights of data subjects, which apply to online personal data collection:

- The right to be fully informed and to give their approval if a website (or an application) processes their data;
- The right to keep their online communications secret (including email, the computer's IP or modem No.);
- The right to be notified if their personal data are compromised (data has been lost or stolen, or if their online privacy is likely to be negatively affected);
- The right to request that their personal data to be excluded from data processing for direct marketing if they have not given their consent.

Furthermore, in this opinion the Commissioner emphasizes the importance for data controllers to adopt privacy policies, which should include, *inter alia:*

- The identity of the controller;
- The information collected from the users, specifying the category of personal data;
- Specific policies regarding cookies and other technologies that allow data controllers to gather information on the users that use the website and to notify the latter about their use.

In addition to the above, it should be noted that the Electronic Communication Law (articles 124 -126), introduces rules on the processing of location data.

Under these rules, electronic communication providers may process traffic data only as long as such data is necessary for the purpose of the transmission of the communication’s transmission and thereafter must delete such data or render them anonymous.

Electronic communications service providers must provide in the contract entered into with the user details on the storage, the duration and the manner of processing of the traffic data. The Electronic Communication Law provides that these traffic data can be processed only by the relevant persons which are authorized by the electronic communications service providers, namely those who are responsible for billing or traffic management, customer service, marketing, fraud detection, or the provision of added value services, provided that the processing of traffic data should be limited only to the scope of their respective activity.

In addition, the Electronic Communication Law provides that the processing of location data can be carried out for the duration value added services and only if the data is rendered anonymous or if the user has granted their prior consent, which consent may be revoked at any time.

Prior to obtaining the consent of the users, the electronic communications service providers must provide information on:

- the type of location data to be processed;
- the purposes and duration of processing;
- the possibility that the location data be shared with third parties, for value-added service purposes.

The location data can be processed only by the relevant persons which are authorized by the electronic communications service providers, namely those who are responsible for the provision of the service or by third parties which are responsible for the provision of added value services, provided that the processing of traffic data should be limited only to the scope of their respective activity.

KEY CONTACTS

Tashko Pustina
tashkopustina.com/

Flonia Tashko
Partner
T +355423891 90
flonia.tashko@tashkopustina.com

Alban Shanaj
Partner
T +355423891 90
alban.shanaj@tashkopustina.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.