ICLG

The International Comparative Legal Guide to:

# Data Protection 2016

## 3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bagus Enrico & Partners
Cuatrecasas, Gonçalves Pereira
Deloitte Albania Sh.p.k.
Dittmar & Indrenius
ECIJA ABOGADOS
Eversheds SA
Gilbert + Tobin
GRATA International Law Firm
Hamdan AlShamsi Lawyers & Legal Consultants
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Rossi Asociados
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

global legal group

global legal group

**Contributing Editor**
Bridget Treacy,
Hunton & Williams

**Sales Director**
Florjan Osmani

**Account Directors**
Oliver Smith, Rory Smith

**Sales Support Manager**
Toni Hayward

**Sub Editor**
Hannah Yip

**Senior Editor**
Rachel Williams

**Chief Operating Officer**
Dror Levy

**Group Consulting Editor**
Alan Falach

**Group Publisher**
Richard Firth

**Published by**
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

**GLG Cover Design**
F&F Studio Design

**GLG Cover Image Source**
iStockphoto

**Printed by**
Ashford Colour Press Ltd.
April 2016



**ISBN** 978-1-910083-93-2
**ISSN** 2054-3786

**Strategic Partners**

MIX
Paper from responsible sources
FSC® C011748

## General Chapter:



## Country Question and Answer Chapters:

# Albania

Sabina Lalaj

Ened Topi

Deloitte Albania Sh.p.k.

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

- Constitution of the Republic of Albania.
- Law no. 9887, dated 10.03.2008 "On personal data protection" as amended.
- Decision of the Parliament no. 211, dated 11.09.2008 "On the appointment of the Commissioner for the protection of personal data".
- Decision of the Parliament no. 225, dated 13.11.2008 "On approving of the structure, staff and classification of the working positions in the office of the Commissioner for the protection of personal data".
- Decision of the Commissioner for the protection of personal data no. 3, dated 20.11.2012 "On the countries with an adequate level of protection for personal data" as amended.
- Decision of the Commissioner for the protection of personal data no. 4, dated 27.12.2012 "On exceptions to the obligation to notify the processing of personal data".
- Decision of the Commissioner for the protection of personal data no. 2, dated 10.03.2010 "On determination of procedures for registration administration of data and their recording, procession and extraction".

### 1.2 Is there any other general legislation that impacts data protection?

The Republic of Albania has also ratified the following international acts:

- Convention on the Protection of Individuals regarding the automatic processing of personal data (Law no. 9288/2004) ("the Convention").
- Additional Protocol to the Convention regarding supervisory authorities and trans-border flows of personal data (Law no. 9287/2004).

### 1.3 Is there any sector specific legislation that impacts data protection?

The competent authority on personal data protection, with the purpose to further regulate the processing of personal data and ensure the correct implementation of the law provisions, has issued several instructions, guidelines and orders.

### 1.4 What is the relevant data protection regulatory authority(ies)?

The competent authority is the Information and Data Protection Commissioner ("the Commissioner").

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  "Personal Data" refer to 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.
- **"Sensitive Personal Data"**

  "Sensitive Personal Data" mean any information related to the natural person in referring to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal record, as well as with data concerning his health and sexual life.
- **"Processing"**

  "Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, transmission, dissemination or otherwise making available, alignment or combination, photographing, reflection, entering, filling in, selection, blocking, erasure or destruction, even though they are not recorded in a database.
- **"Data Controller"**

  "Data Controller" means the natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of processing of personal data, in compliance with the laws and applicable secondary legislation, responsible for the fulfilment of obligations defined by the law provisions.
- **"Data Processor"**

  "Data Processor" means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the data controller.
- **"Data Subject"**

  "Data Subject" means any natural person whose personal data are being processed.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Anonymous Data"**

    "Anonymous Data" means any data, which in its origin or during its processing, may not be associated to any identified or identifiable individual.

## 3 Key Principles

### 3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  The transparency principle is not expressly provided in the applicable legislation, although the same can be carved out by reading the other law provisions, such as the duty to inform the data subject, processing for a specific purpose and limited in time, etc.
- **Lawful basis for processing**

  Based on the provisions of the Law no. 9887, dated 10.03.2008 "On personal data protection" as amended ("the Law"), one of the guiding principles is the fair and lawful processing of personal data.
- **Purpose limitation**

  Furthermore, the legislator stipulates that personal data are collected for specific, clearly defined and legitimate purposes and shall be processed in a way that is compatible with these purposes.
- **Data minimisation**

  The principle of data minimisation is not addressed separately in the Law but is applied as a combination of the principles of proportionality and retention.
- **Proportionality**

  Based on the Law provisions, personal data must be proportionate and correlated with the scope of processing, and not excessive in relation to the purposes for which they are collected and processed.
- **Retention**

  The legislator provides that personal data cannot be kept for longer than is necessary for the purpose for which they were collected or further processed. The Law does not contain a specific provision determining the minimum or maximum time for the retention of personal data. However, there exist time limits applicable to specific sectors, as determined by the decision of the Commissioner.
- *Other key principles – please specify*
  - **Data accuracy**

    In addition to the above, protection of personal data is based on accurate data and, where necessary, updated. For such a purpose, the law provides that every reasonable step must be taken to ensure that data, which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

## 4 Individual Rights

### 4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  Data subjects are entitled to obtain, free of charge, from the data controller upon written request: a) confirmation of whether or not his personal data are being processed, information on the purposes of processing, the categories of processed data and the recipients or categories of recipients to whom personal data are disclosed; b) communication to him/her in a comprehensible form of the data undergoing processing and of any available information as to their source; and c) in the case of automated decisions, information about the logic applied in the decision-making.
- **Correction and deletion**

  The data subject has the right to request blocking, rectification or deletion of his data, free of charge whenever he/she becomes aware that data relating to him/her are irregular, false, and incomplete, or have been processed in violation of the law provisions.
- **Objection to processing**

  The data subject has the right to object, at any time, free of charge the processing of data related to him/her carried out by the data controller: i) in the ambit of the performance of a legal task of public interest or in exercise of powers of the data controller or of a third party to whom the data are disclosed; or ii) in cases where the processing is necessary for the protection of the legitimate rights and interests of the data controller, the recipient or any other interested party.
- **Objection to marketing**

  The data subject has the right to demand the data controller not to start processing, or if processing has started, to stop processing of personal data related to him/her for the purposes of direct marketing and to be informed in advance before personal data are disclosed for the first time and for such a purpose.
- **Complaint to relevant data protection authority(ies)**

  Any person who claims that the rights, freedoms and legal interests concerning his/her personal data have been violated shall have the right to complain or to notify the Commissioner and to request its intervention to remedy the infringed right.
- *Other key rights – please specify*

  Data subjects can address the court and seek damage relief in cases of unlawful processing of personal data.

## 5 Registration Formalities and Prior Approval

### 5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

Data controllers should notify the Commissioner in advance for any processing of personal data. To this end, the Law provides that data controllers before starting the processing should notify the Commissioner on the intended activity and categories of personal

data and any changes to the status of notification. The notification to the Commissioner should also contain the intention of the data controller to undertake the transferring of personal data to third countries. Deviation from the rule is made where personal data are processed by non-profit organisations of political, religious, or philosophical character, trade unions, etc., and the process refers to their members, sponsors, etc.

The Decision of the Commissioner no. 4, dated 27.12.2012, provides for another exemption to the notification rule relating to personal data used for employment purposes. The exemption applying to both the public and private sector refers to activities such as employment, dismissal, qualifications of employees and other working related matters.

### 5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

The notification is performed by the data controller being the same defined by the Law as the natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of processing of personal data, in compliance with the laws and applicable secondary legislation, responsible for the fulfilment of obligations defined by the Law.

### 5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

The obligation to notify applies to:

- data controllers established in the Republic of Albania;
- diplomatic missions or consular offices of the Albanian state;
- data controllers who are not established in the Republic of Albania, making use of any equipment situated in the Republic of Albania; and
- public authorities processing data in the framework of crime prevention and prosecution activities, in cases of a criminal offence against the public order and other violations in the field of criminal law, defence and national security.

### 5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

The notification form can filled in and filed online with the Commissioner or printed, filled in and delivered in person near the Commissioner's office. The notification contains information on the data controller and processor, categories of individuals and data to be processed, purpose of the processing, information on whether international transfer to third countries will occur, measures adopted to secure data (i.e., policy and/or regulation documents can be enclosed to the notification form), etc.

### 5.5 What are the sanctions for failure to register/notify where required?

The administrative sanctions provided by the Law are applicable by the Commissioner and consist in fines that vary from a minimum of ALL 10,000 up to a maximum of ALL 500,000.

The aforementioned fines applying to natural persons double in cases where the violations are attributed to legal persons. The maximum of the fine also doubles in the case of processing of personal data without the prior authorisation of the Commissioner.

### 5.6 What is the fee per registration (if applicable)?

The notification to the Commissioner is free of charge.

### 5.7 How frequently must registrations/notifications be renewed (if applicable)?

The notification needs to be renewed should changes occur to the information provided to the Commissioner.

### 5.8 For what types of processing activities is prior approval required from the data protection regulator?

Authorisation by the Commissioner is required for processing of sensitive data for an important public interest and under adequate safeguards. Additionally, prior approval is required in the ambit of the international data transfer to countries without an adequate level of protection for personal data. However, in the latter case, prior approval is not required when:

a. it is authorised by international acts ratified by the Republic of Albania, which are directly applicable;

b. the data subject has given his/her consent for the international transfer;

c. the transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures addressing the data subject's request, or the transfer is necessary for the conclusion or performance of a contract between the data controller and a third party, in the interest of the data subject;

d. it is a legal obligation of the data controller;

e. it is necessary for protecting vital interests of the data subject;

f. it is necessary or constitutes a legal requirement over an important public interest or for exercising and protecting a legal right; and

g. transfer is done from a register that is open for consultation and provides information to the general public.

### 5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

The Law does not set a specific term for obtaining prior approval.

## 6 Appointment of a Data Protection Officer

### 6.1 Is the appointment of a Data Protection Officer mandatory or optional?

Based on the Instruction of the Commissioner no. 21, dated 24.09.2012 "On determination of rules on the safety of personal data processed by large data controllers" as amended, large processing data entities being considered those controllers or processors, which process data by automatic or manual means, by employing six or more persons, directly or by virtue of the processors, are required to appoint a Data Protection Officer, defined as "Contact Person" in the Law.

**6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?**

Failing to appoint the Contact Person is sanctioned by fines ranging from a minimum of ALL 10,000 up to a maximum of ALL 1,000,000.

The aforementioned fines applying to natural persons double in cases where the violations are attributed to legal persons.

**6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?**

As indicated above, it is mandatory for large processing data entities to appoint a Contact Person. There are no advantages granted to other processing entities which voluntarily appoint a Contact Person.

**6.4 Please describe any specific qualifications for the Data Protection Officer required by law.**

Based on the above-indicated Instruction no. 21, the Contact Person should:

a) have full legal capacity to act;

b) have integrity;

c) possess a Bachelor's degree in computer science law;

d) have professional skills and ethics;

e) have at least five years of work experience as a jurist or IT expert, or more than three years of work experience at the Commissioner's office in the capacity of jurist or IT expert; and

f) have not been convicted for any criminal offence.

**6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?**

The Contact Person:

a) is responsible for the internal surveillance of fulfilment by the processing entity of the obligations for the protection of personal data;

b) advises the responsible persons on personal data protection;

c) is responsible for the implementation of technical, organisational measures in relation to the personnel and oversees their practical implementation;

d) in the case of engagement of a processor, is responsible for the internal surveillance of its activity, the content and preparation of the contract with the processor. During the implementation period of the contract or authorisation, the Contact Person will verify the fulfilment of the agreed terms and conditions including the engagement or changes of processors, if any;

e) is responsible for the internal surveillance of the international personal data transfer;

f) is responsible for the handover of the documentation on the archiving systems for the special registration and for the announcing of the changes and de-registration of the archiving systems from the special register and keeps data on the archiving systems which are not subject to registration and make them available to any person which by law has the right to access them;

g) is responsible for the necessary collaboration with the Commissioner; and

h) upon request of the Commissioner, is obliged to submit the written authorisation by means of which he or she operates, as well as proof of the skills gained during the professional training.

**6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

The Contact Person(s) should be notified to the Commissioner. In the case of the replacement of the Contact Person, the Commissioner should be notified within 14 days from the date of the replacement.

## 7 Marketing and Cookies

**7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)**

By letter of law, collection of personal data for direct marketing purposes requires the explicit consent of the data subject.

The concept and rules applicable to the direct marketing are further developed by the Commissioner, *inter alia*, in: the Instruction no. 16, dated 26.12.2011 "On protection of personal data in the direct marketing and the safety measures" as amended; Instruction no. 6, dated 28.05.2010 "On correct use of SMS for promotional, advertising, information, direct sales, by means of mobile telephony"; and Instruction no. 14, dated 22.12.2011 "On processing, protection and safety of personal data in the public electronic communication sector".

**7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The Commissioner is active in promoting and raising awareness on the obligations and rights attached to both data controllers and data subjects. Based on information publicly available on the website of the Commissioner, different data controllers have received recommendations and/or were subject to decisions (administrative sanctions) of the Commissioner.

**7.3 Are companies required to screen against any "do not contact" list or registry?**

The applicable Law and the above-mentioned instructions provide for the right of the data subject to withdraw its consent at any moment.

**7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Generally, the applicable fines range from a minimum of ALL 10,000 up to a maximum of ALL 500,000.

**7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?**

The applicable legislation does not address the matter.

**7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?**

This is not applicable.

**7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

This is not applicable.

**7.8 What are the maximum penalties for breaches of applicable cookie restrictions?**

This is not applicable.

## 8 Restrictions on International Data Transfers

**8.1 Please describe any restrictions on the transfer of personal data abroad?**

International transfer of personal data to third countries not having an adequate level of protection might be undertaken upon prior authorisation of the Commissioner. In cases where the Commissioner, after assessing the situation, permits the international transfer of personal data to a third country lacking in adequate levels of protection, a set of proper safety measures shall apply to the case. The Commissioner might exempt data controllers to require authorisation for special categories of personal data. The categories of data, falling under the said exemption, shall be the object of instruction by the Commissioner.

However, the Law provides for exceptions to the obtaining of the prior authorisation in cases of international transfer to a third country having an inadequate level of protection, which are:

- Made based on international treaties ratified by the Republic of Albania, being the same directly applicable.
- Consented to by the data subject.
- Necessary for the implementation of the contract between the data subject and data controller or for the implementation of the pre-contractual measures, in response to the request of the data subject, or the transfer is necessary for the fulfilment or implementation of the contract between the data controller and a third party, in the interest of the data subject.
- Necessary for completion of a contract between the data controller and the data subject or a third party in the interest of the data subject.
- Necessary for the vital interest of the data subject.
- Done through a register open to consultation, which provides information to the public in general.
- Necessary or legally required by an important public interest or for the exercise/defence of a legal right.

**8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.**

Based on the Law provisions, for cases falling outside the above exceptions, companies are required to obtain the prior authorisation of the Commissioner.

**8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.**

Based on the applicable legislation, international transfer of personal data in countries deemed to have an adequate level of protection are not restricted if the Commissioner has been duly notified. The Decision of the Commissioner for the protection of personal data no. 3, dated 20.11.2012 "On the countries with adequate level of protection for personal data" as amended, provides that countries with an adequate level of protection for international transfer of personal data are, namely, the EU countries and countries part of the European Economic Area. The same consideration is made for members that have ratified the Convention for the Protection of Individuals regarding the automatic processing of personal data and related protocol, as well as countries designated by a decision of the EU Commission.

As for the international transfer of data to countries deemed not to have adequate protection, the prior authorisation of the Commissioner is required, provided that none of the requirements as indicated in question 8.2 are met.

Notwithstanding the fact that the letter of law is clear in that respect, the Commissioner's standing is that every international transfer to third countries having an inadequate level of protection of personal data should undergo a prior check by the same.

## 9 Whistle-blower Hotlines

**9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)**

The applicable legislation does not address the matter.

**9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?**

The applicable legislation does not address the matter.

**9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.**

This is not applicable.

**9.4 Do corporate whistle-blower hotlines require a separate privacy notice?**

This is not applicable.

**9.5 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?**

This is not applicable.

## 10 CCTV and Employee Monitoring

**10.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies)?**

The use of CCTV is subject to notification with the Commissioner, with exceptions in cases of processing of personal data which, based on the applicable legislation, the sole purpose is to keep records for providing information for the public in general. Also exempted from the notification are personal data processed for the purpose of protection of the constitutional institutions, national security interests, foreign policy, economic or financial interests of the state, prevention or prosecution of the criminal offences.

**10.2 What types of employee monitoring are permitted (if any), and in what circumstances?**

The applicable legislation stipulates that use of video surveillance is allowed only for security reasons. Under no circumstances should video surveillance be used to monitor private areas such as lavatories, changing rooms, etc.

**10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Video surveillance should be carried out in accordance with the requirements set by the applicable legislation. Additionally, the video surveillance process should be duly notified by the employer by affixing notices in the workplace.

**10.4 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?**

The applicable legislation does not explicitly address the matter; however, the Commissioner with the Instruction no. 11 dated 08.09.2011 "On processing personal data in the private sector" provides that in cases where, due to the size and organisational structure of the enterprise, it is not possible for employees to exercise personally their rights as stipulated by the Law, the latter can appoint a representative vested with the respective powers.

**10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?**

No specific registration/notification or prior approval is required.

## 11 Processing Data in the Cloud

**11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

There are no restrictions on the processing of personal data in the cloud. To this end, in 2014, the Commissioner issued a non-binding guideline named "On protection of personal data in the cloud computing services". The guidance is of a non-binding nature; therefore, it only incorporates recommendations on rights and obligations applicable to the cloud service provider and the cloud client (data controller).

**11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

As indicated in question 11.1 above, the Commissioner has issued a non-binding guideline which, *inter alia*, includes some recommendations on the clauses of the contract to be entered by the cloud service provider and the cloud client. To this effect, it is recommended that the contract address matters such as the possibility to process personal data only in accordance with the instructions of the cloud client (data controller), as well as the necessity for security measures clauses applicable on the part of the cloud service provider.

## 12 Big Data and Analytics

**12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

There are no restrictions on utilisation of big data. The applicable legislation does not address the matter.

## 13 Data Security and Data Breach

**13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

The Commissioner has issued two instructions; namely, Instruction no. 6, dated 05.08.2013 "On determination of detailed rules on the security of personal data" and Instruction no. 2, dated 10.03.2010 "On determination of administration procedures on registration of data, insertion, processing and extraction of personal data" as amended. Additionally, the Commissioner has drafted a Standard Template Regulation "On protection, processing, storage and safety of personal data".

All of the above acts further develop the provisions of the Law on the security measures to be adopted by data controller and processors, including, *inter alia*, security measures applicable to computer systems and apps, which should be protected by strong passwords (i.e., password is recommended to be changed every three or six months).

**13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.**

Although there is no specific duty to report data breaches, the legislator sanctions the unauthorised disclosure of confidential information. The Law provides for a fine ranging from ALL 10,000 up to ALL 150,000.

Moreover, in some specific cases, the confidential information breach may constitute a criminal offence punishable by a fine or imprisonment of up to two years.

**13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.**

Please refer to the above answer.

**13.4 What are the maximum penalties for security breaches?**

Please refer to the answer to question 12.2.

## 14 Enforcement and Sanctions

**14.1 Describe the enforcement powers of the data protection authority(ies):**

| Investigatory Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| The Commissioner may start investigations on an *ex officio* or *ex parte* basis in order to verify compliance with the law provisions. | Pecuniary sanctions vary from a minimum of ALL 10,000 up to a maximum of ALL 1,000,000. | - |
| State Prosecutor. | - | Fine or imprisonment for up to two years. |

**14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

During the investigation process, the Commissioner issues recommendations, orders to comply with, and administrative sanctions should data controllers and processors fail to meet/comply with the law provisions. According to the data obtained from the official website, during the year 2015, the Commissioner issued 37 recommendations, two orders and 46 administrative sanctions.

The State Prosecutor may start investigation upon *ex parte* or Commissioner's referral of a committed criminal contravention.

## 15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

This is not applicable.

**15.2 What guidance has the data protection authority(ies) issued?**

This is not applicable.

## 16 Trends and Developments

**16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

As indicated above, during the last year, the Commissioner has been very proactive in issuing various recommendations, orders and administrative sanctions to data controllers and processors.

**16.2 What "hot topics" are currently a focus for the data protection regulator?**

The Commissioner continues to focus its attention on raising awareness with respect to the rights and obligations deriving from the provisions of the applicable legislation.

**Sabina Lalaj**
Deloitte Albania Sh.p.k.
Rr. Elbasanit
Pallati Poshte F. Gjeologji
Miniera
Tirana, 1001
Albania

*Tel: +355 4 45 17 927*
*Email: slalaj@deloittece.com*
*URL: www2.deloitte.com/al/en*

Sabina is the Senior Legal Manager in the Tax & Legal Department of Deloitte Albania. She joined our practice in 2015 from a leading law firm in Albania. She specialises in commercial companies, project finance, real estate, public procurement, mergers and acquisitions, concessions, employment, privatisations, energy, banking and construction law. Sabina is continuously involved in providing legal advice both in Albania and Kosovo. She is an author of several papers and chapters in international legal publications such as the *International Comparative Legal Guide* series and *International Law Office*. Sabina graduated in Law from Tirana University in Albania (2000), and obtained a Master of Art degree in South East European Studies at the National & Kapodistrian University of Athens, Greece (2001). Sabina has been a member of the Albanian Bar Association since 2003.

**Ened Topi**
Deloitte Albania Sh.p.k.
Rr. Elbasanit
Pallati Poshte F. Gjeologji
Miniera
Tirana, 1001
Albania

*Tel: +355 4 45 17 906*
*Email: etopi@deloittece.com*
*URL: www2.deloitte.com/al/en*

Ened is a Senior Associate in the Tax & Legal Department of Deloitte Albania. He joined our practice in 2015 from a leading law firm in Albania. Ened has more than eight years of experience in corporate law, project and corporate finance, mergers and acquisitions, competition, construction, employment, concessions, intellectual property, consumer and data protection law, etc. He is an author of several papers and chapters in international legal publications such as the *International Comparative Legal Guide* series and *International Law Office*. Ened graduated in Law from the University of Macerata, Italy (2006), and holds a Master's degree in Euro-Mediterranean Studies in Commerce and Social-cultural Cooperation from the University of Macerata, Italy (2007). He is a member of the Albanian Bar Association and an Authorised Trademark & Industrial Design Representative.

Deloitte.

Deloitte Albania Sh.p.k. is an affiliate of Deloitte Central Europe Holdings Limited, the member firm in Central Europe of Deloitte Touche Tohmatsu Limited. Deloitte Albania Sh.p.k., founded in 1996, has extensive knowledge of the local market and of best practices from around the world. With almost 20 years of operations in Albania, Deloitte Albania Sh.p.k. is a reputable firm and enjoys the distinction of being the leading professional services organisation in the country, delivering world-class assurance, tax, legal, consulting, financial advisory and technology services. The practice serves many of the country's largest companies, public institutions, and successful fast-growing companies.

In 2011, Deloitte Albania and Deloitte in Kosovo agreed on a closer cooperation by forming the Deloitte Albania & Kosovo cluster. Comprising over 290 people in the two offices, this collaboration enables Deloitte Albania & Kosovo professionals to use their combined size, scale and expertise to offer greater breadth and depth of service to our clients where and when they are needed.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk