ICLG

The International Comparative Legal Guide to:

# Data Protection 2017

## 4th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bae, Kim & Lee LLC
Bagus Enrico & Partners
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Cuatrecasas
Dittmar & Indrenius
Drew & Napier LLC
Ecija Abogados
ErsoyBilgehan
Eversheds Sutherland
GANADO Advocates
Gilbert + Tobin
GRATA International
Hacohen & Co.
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
LPS L@w
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at Law Ltd.
Portolano Cavallo
Rato, Ling, Lei & Cortés Lawyers
Rossi Asociados
Subramaniam & Associates (SNA)
Wikborg Rein Advokatfirma AS

global legal group

global legal group

**Contributing Editors**
Anita Bapat and Aaron P. Simpson, Hunton & Williams

**Sales Director**
Florjan Osmani

**Account Director**
Oliver Smith

**Sales Support Manager**
Paul Mochalski

**Sub Editor**
Hollie Parker

**Senior Editors**
Suzie Levy, Rachel Williams

**Chief Operating Officer**
Dror Levy

**Group Consulting Editor**
Alan Falach

**Publisher**
Rory Smith

**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
May 2017



**ISBN** 978-1-911367-50-5
**ISSN** 2054-3786

**Strategic Partners**

MIX
Paper from responsible sources
FSC® C011748

## General Chapter:



## Country Question and Answer Chapters:

Chapter 25

# Romania



Mihaela Cracea


Alexandru Lefter

Pachiu & Associates


## 1 Relevant Legislation and Competent Authorities

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

In Romania, the core legal framework for the protection of personal data is set forth by Law No. 677/2001 on the protection of individuals with regard to the processing of personal data and on free movement of such data ("Personal Data Law").

The Personal Data Law implements into the national legal system the provisions of the Directive of the European Parliament and Council No. 95/46 on the protection of individuals with regard to the processing of personal data and on free movement of such data ("Personal Data Directive").

The scope of the Personal Data Law is to secure and protect the fundamental rights of individuals, mainly the right to intimate family and private life, in connection with the processing of personal data.

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

The minimum security requirements for the processing of personal data are set forth in the Order of the Romanian Ombudsman No. 52/2002 ("Order 52/2002").

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

Law No. 506/2004 on personal data processing in the field of electronic communications sets forth the general conditions for processing of personal data in the electronic communications field ("**Law 506/2004**") and applies to providers of public communication networks and electronic communication services, as well as to providers of subscriber records which, within their economic activities, are processing personal data.

Law No. 238/2009 on the regulation of personal data processing undertaken by the structures/units of the Ministry of Internal Affairs pertaining to activities for prevention, investigation and the fight against criminal activities, as well as for maintenance and assurance of public order, as subsequently republished, sets forth a set of rules for automatic and non-automatic personal data processing in connection to such activities. This law is not applicable to personal data processing and transfers in the field of national defence and security.

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

Romania has set forth a special and independent supervisory and regulatory institution in the field of personal data protection, i.e., the National Supervisory Authority for Personal Data Processing ("**ANSPDCP**").

ANSPDCP supervises and controls the lawfulness of personal data processing in Romania. For such purpose, ANSPDCP has attributes, such as the ability to receive and assess notifications on data processing, to authorise personal data processing when required by law, to investigate and sanction unlawful processing, and to keep a record of personal data processing, etc.

## 2 Definitions

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

- "**Personal Data**"

  Any information regarding an identified or identifiable individual. An indefinable individual is deemed to be an individual who can be identified, directly or indirectly, particularly with reference to an identification number or by one or more features pertaining to his physical, physiological, psychical, economic, cultural or social identity.

- "**Sensitive Personal Data**"

  Under the Personal Data Law, the concept of "sensitive personal data" is not expressly defined. However, specific categories of personal data, namely those pertaining to racial or ethnic origin, health condition, sexual life, identification details, criminal convictions and minor offences are granted a special legal regime. Furthermore, for the application of such legal provisions, in the standard notification form approved by the decision of the Romanian Personal Data Authority, the following data are qualified as "special personal data": data denoting the racial origin of data subjects; data denoting the ethnic origin of data subjects; data on the political, philosophical and religious beliefs of data subjects; data on memberships of trade unions, political parties and religious organisations of data subjects; personal identification number; series and number of identification documents; health status; genetic data; biometric data; data regarding sexual life; data regarding perpetration of criminal offences; data on criminal convictions/security measures; data on disciplinary sanctions; data on contraventions; and data in criminal records.

- "**Processing**"

  Any operations or set of operations with personal data, by automatic or non-automatic media, such as collecting, registration, classification, storage, adaptation or alteration, extraction, consultation, use, disclosure to third parties by transmission, dissemination or in any other way, annexation or combination, blocking, erasure or destruction.

- "**Data Controller**"

  Any individual or private or public legal entity, including central/local public authorities or institutions, who sets forth the purpose and media for processing of personal data; if the purpose and media of personal data processing are set forth by law, the "controller" shall be deemed as the individual or private or public entity so qualified by the respective law or based on such a law.

- "**Data Processor**"

  Any public or private, natural or legal person, including public authorities, agencies and local structures of such, which process personal data on behalf of the controller.

- "**Data Subject**"

  The individual whose personal data are subject to processing by the controller or the processor.

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

  - "**Data Recipient**"

    Any public or private, natural or legal person, including central/local public authorities and agencies, to whom data are disclosed, irrespective of whether such a person is a third party or not. Public authorities to which data are disclosed in connection to their special investigation attributions are not deemed as "data recipients" under the Personal Data Law.

  - "**Third Party**"

    Any public or private, natural or legal person, including public authorities, agencies and local structures of such, other than the data subject, the controller, the processor or persons under the direct control of the controller or the processor, who is authorised to process data.

  - "**Anonymous Data**"

    Data which, due to their origin or specific processing modality, cannot be associated with an identified or identifiable person.

## 3 Key Principles

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

- **Transparency**

  If personal data are obtained directly from the data subject, the controller must disclose at least the following information: the controller's identity; the purpose of processing; recipients; whether disclosure of all requested data is mandatory; the consequences if the data subject refuses to provide such data; the rights of the data subjects in connection to the proposed processing and effective modalities for exercise of such rights; and any other information imposed by ANSPDCP depending on the nature of the processing.

  If personal data are not obtained directly from data subjects, the controller should provide the information above either before processing or, at the latest, when personal data are disclosed to third parties.

- **Lawful basis for processing**

  Under the Personal Data Law, personal data shall be processed fairly and lawfully. This is another term that the Personal Data Law does not define. However, "lawful" refers not only to compliance with the Personal Data Law, but also to all other provisions in the Romanian legal system, whether criminal or civil.

- **Purpose limitation**

  Under the Personal Data Law, personal data can only be collected for specific, precise and legitimate purposes. Subsequent processing of personal data for statistical, historical or scientific research shall not be deemed a breach of the initial purpose if made in accordance to the law, including with the legal provisions of the obligation to notify ANSPDCP.

- **Data minimisation**

  Under the Personal Data Law, personal data should be adequate, relevant and not excessive in relation to the purpose for which they are processed.

  In practice, controllers must ensure that personal data are sufficient for the purpose of processing and that they do not hold more information than they actually need for that purpose.

- **Proportionality**

  The measure adopted, i.e., the interference with the fundamental right to personal data protection, must also be proportionate to the purpose of processing. This principle is, essentially, about reaching an acceptable compromise between two constitutional values: the fundamental right to personal data protection, which will be restricted, and the legitimate purpose it is aiming to achieve. Interference is in compliance with the principle of proportionality when the processing is balanced, and results in more benefits and advantages to general interest than harm to other conflicting values.

- **Retention**

  Under the Personal Data Law, personal data, processed for any purpose, cannot be kept for longer than actually necessary for the purpose of processing.

- *Other key principles*

  As a general rule, any personal data processing can be made only upon manifest and unequivocal consent of the data subject, save when otherwise provided by law. The consent of the data subject is not required if processing is necessary, *inter alia*: for the execution of an agreement to which the data subject is a party; for taking appropriate actions for the safeguard of the life, physical integrity or health of the data subject or another individual; for compliance by the controller with a legal obligation; or for a legitimate interest of the controller or of the third party.

  Moreover, for special categories of personal data, processing can be made only upon manifest consent of the data subject, or if absolutely necessary for compliance with a legal obligation of the controller/safeguard of a public interest or of the rights and freedoms of the data subject or other individuals, or if expressly provided by law.

## 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**

  Under the Personal Data Law, any data subject is entitled to request and obtain from the controller confirmation on whether his personal data are subject to processing. The controller must disclose to the applicant, at least, the following information:

- the purpose of processing, categories of processed data and data recipients;
- any information regarding the origin of the processed data;
- the mechanism by which any automatic processing of data is made;
- information on the conditions for exercise of the right of intervention over the data and of the right to object to processing; and
- the possibility to verify the processing in the ANSPDCP Record, to file a complaint against the decisions of the controller with ANSPDCP or with the competent courts of law.

- **Correction and deletion**

  Any data subject is entitled to request to the controller, at no cost, the following:
  - the adjustment, update, blocking, erasure or transformation of anonymous data of the personal data subject to unlawful processing; and
  - the notification to third parties to which personal data have been disclosed of any of the operations above, provided that such notification is not impossible and does not entail a disproportionate effort with respect to the legitimate interest that might be violated.

- **Objection to processing**

  Data subjects are entitled to object, at any time, to processing of their personal data, provided that the grounds of such an objection are sound and legitimate.

- **Objection to marketing**

  Data subjects are entitled to object, at any time, with no cost and without motivation, to any processing of their personal data for direct marketing purposes, as well as to any disclosure to third parties for such purposes.

- **Complaint to relevant data protection authority(ies)**

  Data subjects can file complaints to ANSPDCP in connection with alleged violations of their rights, as granted by the Personal Data Law. A complaint to ANSPDCP can be filed only upon a lapse of 15 days from the date of registration of a similar complaint with the controller.

  If the complaint is found to be grounded, ANSPDCP can decide to temporarily suspend or cease personal data processing, as well as to erase, totally or partially, the personal data which are subject to such unlawful processing. Moreover, ANSPDCP can inform the criminal investigation bodies and file a lawsuit with the relevant courts of law.

- *Other key rights – please specify*

  **The right of not being subject to an individual decision**

  Data subjects have the right to request and to obtain: (i) the withdrawal or annulment of any decision exclusively taken in consideration of personal data processing by automatic means and which is aimed at assessing features of the data subjects' personality, such as professional capabilities, credibility and behaviour; and (ii) the reassessment of any decision taken in the above-mentioned conditions.

  Provided that all the other guarantees are observed, the data subjects can be subject to an individual decision, as mentioned above, if the decision is taken in relation to the execution of an agreement or the decision is authorised by a legal provision.

## 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.)

Notification is not required, except for the following cases when notification to ANSPDCP is mandatory:

- processing of personal data related to the racial or ethnic origin of data subjects, data on the political, philosophical and religious beliefs of data subjects, data on memberships of trade unions, and data regarding health status and sexual life;
- genetic and biometric personal data processing;
- processing of data which allows, directly or indirectly, the geographical localisation of natural persons through electronic communication devices;
- processing of data regarding perpetration of criminal offences by the data subject or data regarding criminal convictions, preventive measures, administrative penalties or data on minor offences applicable to the person, performed by private entities;
- personal data processing via electronic devices within an evidence system, aiming to monitor and/or evaluate aspects such as personality, professional competence, credibility, behaviour and other similar aspects;
- processing of personal data by electronic means within evidence systems aiming to take automatic individual decisions relating to the evaluation of solvability, financial and economic situations, actions which may imply disciplinary, minor offences or criminal liability of natural persons by private law entities;
- processing personal data related to ethnic or racial origins, political, religious, philosophical or other similar beliefs, union affiliation, data regarding health status or sexual life performed by associations, foundations or any other non-profit organisations with regard to their members, if the personal data are disclosed to third parties without the prior consent of the data subject;
- processing infants' personal data, if such activity was performed during direct marketing activities, via the internet or electronic messages; and
- personal data processing via video surveillance systems, including the transfer of such data to a non-EU state; such notification shall not be required for cases in which the personal data processing is performed by an individual on his own personal interest, even if the images saved also comprise public domain pictures.

Furthermore, for international transfers of personal data, notification to ANSPDCP is also required, save for cases when such transfers are made based on a special law or international treaty ratified by Romania, or they are implemented exclusively for literary or journalistic purposes when data were already manifestly made available to the public by the data subject, or the data are strictly linked to the data subject being a public person, or taking into account the public nature of that particular person.

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

Under the Romanian Data Protection Law, notifications are made based on the purpose of processing.

**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 data protection authority must be notified by the following: (i) local legal entities; (ii) Romanian subsidiaries of foreign entities (exemptions under question 5.3 are also applicable); and (iii) foreign legal entities, if they are processing personal data by means of any nature located in Romania, save when such means are used exclusively as data transit facilities.

Processing by Romanian representative offices or branches of foreign entities is subject to notification in Romania.

The aspects mentioned under question 5.1 are applicable to all cases listed herein.

**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.)**

Under the Personal Data Law, the notification must include at least the following:

a. identification of the controller;
b. purpose/related purposes of processing;
c. categories of data subjects;
d. categories of data recipients;
e. guarantees pertaining to third-party disclosure;
f. means by which data subjects are informed of the processing and their rights in connection thereof; estimated date for termination of the processing and subsequent destination of the processed data;
g. intended transfers abroad (if applicable);
h. description of the measures implemented for security of the personal data; and
i. description of any record of personal data related to the processing, as well as on potential links with other personal data processing or records, irrespective of whether such are made/located in Romania.

In the case of the international transfer of personal data, the notification will also list the transferred personal data, as well as the destination country for each category of transferred data.

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

Failure to notify ANSPDCP when mandatory under the Personal Data Law is sanctioned with an administrative fine amounting to between approximately EUR 1,000 and EUR 5,000 (in national currency equivalent), save when incriminated as a criminal offence. Additionally, ANSPDCP may order the temporary or permanent ceasing of the unlawful processing, as well as deletion of the processed data.

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

No fees are required.

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

There is no general requirement with respect to the notifications renewal. The notifications should be updated each time changes occur as per the processed personal data, the data subjects, the data recipients, and the means and modalities of processing. In cases where personal data are processed for a different purpose, a separate notification must be filed.

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

The transfer of personal data to countries which are not deemed to grant an adequate level of protection cannot be made unless authorised by ANSPDCP. The authorisation is not required: if the transfer is made exclusively for journalism, or a literary or artistic purpose; if data have been already disclosed to the public by the data subject; or if the data are strictly related to the public nature of the activities of the data subject.

In all cases, transfer of personal data to entities located outside Romania can be made only upon prior notification to ANSPDCP.

International transfer is always allowed, among other circumstances, when the data subject has expressly consented to such transfer.

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

Where applicable, authorisations of personal data processing may be awarded only upon prior notification to ANSPDCP. The notification will include the information mentioned under question 5.4. In 30 days as of the online filing, the first page of the notification, in hard copy, signed and stamped by the legal representative of the controller, must be registered with ANSPDCP. Failure to register this first page shall result in the refusal of ANSPDCP to consider the notification filed online.

As a general rule, the authorisation must be issued in 30 days as of the registration of the relevant notification with ANSPDCP (final version, including all amendments, supplementation and clarifications required by ANSPDCP).

## 6 Appointment of a Data Protection Officer

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

The Personal Data Law does not require the appointment of a Data Protection Officer ("**DPO**"). Romanian companies do not usually appoint DPOs. However, there is a practice for multinational companies with subsidiaries in Romania to appoint, at parent company level, an employee with duties related to the processing of personal data performed by Romanian subsidiaries.

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

This is not applicable.

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

Although not mandatory, the appointment of a DPO has turned out to be advantageous for the monitoring of implementation of the statutory provisions of companies' internal policies with respect to data privacy for keeping in contact with ANSPDCP representatives during investigations, and for relevant training of the employees. Therefore, DPOs play an important role in the compliance of companies with data protection rules.

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

This is not applicable.

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

In practice, the responsibilities of DPOs focus mainly on advising companies on data protection rights and obligations, and supervising activities related to processing, appropriate notification, management and avoidance of breaches.

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

No registration formalities are needed.

## 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.)

**Opt-in requirements**

Unless the subscriber has given his express prior consent, the following deeds are forbidden:

- marketing communications sent by email; and
- commercial communications made through automatic systems that do not require the intervention of a human operator − by fax, email, SMS or any other method using electronic communication systems destined for the public.

  Commercial e-communications should observe the following requirements:
  - clear identification of their commercial nature;
  - clear identification of the individual or legal entity on behalf of which the communications are made;
  - clear identification of promotional offers and of all relevant conditions in connection therewith; and
  - clear identification of competitions and promotional games, and the relevant participation conditions must be clearly identifiable.

An exemption from the opt-in mechanism requirement applies when the controller has obtained the consumer's email address on entering a contractual relationship for the trade of specific products or services. Nevertheless, it is only permitted to send emails for the purposes of direct marketing for similar products and services, and in compliance with the opt-out requirements.

**Opt-out requirements**

All commercial communications must inform consumers, in a manifest and accurate manner, of the possibility to opt-out from receiving these communications through a simple and free-of-charge procedure.

Opt-out must also be possible in cases where the consumer has not initially objected, but later changes his mind.

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

ANSPDCP is one of the authorities with jurisdiction to enforce breaches of marketing restrictions. Additionally, under Law No. 506/2004, the National Authority for Management and Regulation in Communications ("**ANCOM**") has specific attributes regarding the activity of electronic communication services and communication networks providers.

ANSPDCP has performed a significant number of investigations concerning the processing of personal data and privacy in the field of e-commerce.

Subject to findings regarding unsolicited commercial communications, most of the collectors were sanctioned for lack of expressed prior consent of the subscribers and for failing to tell subscribers that they may reject marketing communications in the future.

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

There is no legal requirement for companies to screen against a "do not contact" list or registry. However, companies have to obtain the express prior consent of the subscriber in order to send commercial communications, and the consumer has the possibility to opt-out from receiving these communications in cases where he has not initially objected, but later changes his mind. In such cases, companies should draft a "do not contact" list, including consumers who have exercised their right to opt-out. The list should be considered by the company upon every commercial communication sent to consumers.

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

Breach of the legal requirements for marketing communications is sanctioned with administrative fines ranging between approximately EUR 1,100 and approximately EUR 22,000 (in national currency equivalent). Furthermore, for companies with a turnover exceeding the national currency equivalent of EUR 1.11 million, fines can reach up to 2% of the turnover.

Moreover, ANSPDCP may order the temporary or permanent cessation of the unlawful processing, or deletion of processed data.

### 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)?

Storing cookies or gaining access to such data is allowed upon prior and manifest consent of the data subject, obtained subject to easily accessible and accurate information on the processing and its purpose.

If the provider of electronic communication services allows third parties to store cookies on the terminals of the data subjects, the information notice will also have to include the purpose of the processing by third parties, as well as the manner in which data subjects may adjust their web browser settings.

**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)?**

The consent for using cookies may be given implicitly through the settings in the internet browser or similar technology.

Prior consent is not required when the processing is done exclusively for the purpose of transmitting a communication through an electronic communication network, or is strictly necessary for providing an information society service expressly requested by the respective data subject.

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

Controllers were mainly sanctioned for failure to obtain the prior consent of data subjects and for failure to provide appropriate information notice. Furthermore, processing activities were suspended or even ceased, and deletion of the processed data was ordered.

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

Failure to comply with the legal restrictions is sanctioned with administrative fines ranging between approximately EUR 1,100 and approximately EUR 22,000 (in national currency equivalent). For companies with a turnover exceeding the national currency equivalent of approximately EUR 1.11 million, the amount of the fines can reach up to 2% of turnover.

In addition, ANSPDCP may order the temporary or permanent cessation of the unlawful processing.

## 8 Restrictions on International Data Transfers

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

The Personal Data Law sets forth a different set of rules depending on whether the data importer is located in states which are offering an adequate data protection level or not:

a. **International transfer to states that offer an adequate level of personal data protection**

Importers in EU and EEA Member States or other states mentioned in the relevant decisions of the European Commission are deemed as granting an adequate level of personal data protection. Consequently, in these cases, authorisation by ANSPDCP is not necessary.

b. **International transfer to states that do not offer an adequate level of personal data protection**

Such transfers can only be implemented upon prior authorisation by ANSPDCP, which is awarded only when appropriate guarantees for the protection of individuals' fundamental rights are stipulated in contracts compliant with the standard contractual clauses set forth by the European Commission Decision No. 2001/497/EC ("**Data Transfer Contracts**").

Data Transfer Contracts are not required when:

- data subjects have expressly consented to the transfer;
- the transfer is necessary for the execution of a contract between the data subject and the controller or between the controller and third parties, but for the benefit of the data subject;
- the transfer is necessary for a major public interest or the protection of the life, the physical integrity and health condition of the data subjects; or
- the transfer pertains to public data.

Data Transfer Contracts are also not required in the case of intra-group international data transfers when the group has implemented an internal code of conduct for international data transfers between group entities ("**Binding Corporate Rules**") that were previously approved by ANSPDCP. In such cases, notification of the transfer and authorisation by ANSPDCP are still required; however, the proceedings are more simplified and authorisation of the transfer is likely to be granted in a shorter term than in the case of transfers implemented based on Data Transfer Contracts.

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

In practice, transfers to countries granting an adequate level of protection do not raise major issues for the controller.

As for transfers to countries not granting an adequate level of protection, the companies commonly transfer the personal data either based on a Standard Data Transfer Agreement, or upon consent of the data subjects.

In relation to both mechanisms, ANSPDCP generally assesses the equivalence between the information in the Standard Data Transfer Contract/consent notice and the information in the notification.

Recently, more and more companies are implementing Binding Corporate Rules for international transfers of data between group entities in order to hasten proceedings for authorisation of the transfer.

**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.**

Any transfer of personal data to countries outside EU/EEA and not granting an adequate level of protection can be made only upon notification to ANSPDCP. Transfer to countries not granting an adequate level of protection, based on a Standard Data Transfer Contract and Binding Corporate Rules, requires authorisation by ANSPDCP. For the authorisation procedure and timeframe, please refer to question 5.9.

## 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.)**

ANSPDCP has not issued any binding regulations on the implementation of corporate whistle-blower hotlines; however, the guidelines in the Opinion No. 1/2006 of the European Commission's

Data Protection Working Party (the "**Opinion No. 1**") should be observed.

Implementation of whistle-blowing schemes is possible only if necessary:

- ***for compliance with a legal obligation of the controller*** – implementation of whistle-blowing schemes is mandatory by law in specific fields. Government Emergency Ordinance No. 99/2006 on credit institutions and capital adequacy sets forth the obligation of credit institutions to implement appropriate schemes for reporting breaches of banking regulations, providing, however, for an adequate standard of personal data protection, both for the whistle-blower and for the incriminated person, in accordance with the rules under the Personal Data Law; or
- ***to pursue a legitimate interest of the controller or of a third party to whom data are disclosed*** – corporate concern to prevent fraud and internal misconduct might be deemed as a legitimate interest justifying the implementation of whistle-blowing schemes. Nevertheless, implementations of such schemes can be done only if the relevant principles in the Personal Data Law are observed, in particular the proportionality, data minimisation and retention rules. Furthermore, reported employees should be informed about the purpose of the whistle-blowing scheme, the alleged accusations, the recipients of the data collected through the whistle-blowing scheme, and how to exercise their rights of access and ratification. However, in cases where there is a significant risk that the information of the incriminated person would jeopardise the effectiveness of the investigation, this may be delayed for as long as the risk exists.

### 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 contain any specific rules. However, according to the recommendations in the Opinion No. 1, anonymous reporting should be discouraged. Anonymous reporting may be permitted in exceptional cases and only under specific terms detailed in the Opinion No. 1.

### 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.

Under ANSPDCP Decision No. 200/2015, prior notification is required by private entities for the processing of personal data regarding criminal offences committed by the data subjects or criminal convictions, security measures or contraventional/administrative penalties applied to the data subject.

If the implementation of whistle-blower hotlines triggers the transfer abroad of personal data to countries which do not offer an adequate level of protection (e.g., transfer in the United States in connection to Sarbanes-Oxley whistle-blower schemes), the transfer shall be subject to authorisation by ANSPDCP under the terms and conditions in sections 5 and 8.

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

A separate privacy notice is not required only when the implementation of the whistle-blowing scheme is expressly provided by the law. Furthermore, processors may be exempted from the obligation to inform data subjects about the implementation of a whistle-blower hotline if such information proves itself impossible or would apply a disproportionate effort reported to the legitimate interest it aims at safeguarding.

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

The Romanian legislation does not set forth a statutory obligation to notify or consult with works councils/trade unions/employee representatives when implementing whistle-blower hotlines. However, such notification/consultation should be observed if stipulated by the company's internal regulation.

## 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 processing of personal data by video surveillance may be performed for the following purposes:

(i) criminal prevention and control;

(ii) traffic surveillance;

(iii) protection of individuals, assets, values, locations and equipments of public interest, as well as of the related areas;

(iv) implementation of public interest measures or the exercise of public authority; and

(v) safeguard of legitimate interests, provided that the fundamental rights and freedoms or interests of the data subject are not prejudiced.

Prior notification to ANSPDCP is required.

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

The processing of personal data of employees by video surveillance means is allowed for the fulfilment of any legal obligations or based on a legal interest, with the observance of the employees' rights, especially regarding the prior notification of such.

If the above circumstances are not met, the processing of employees' personal data cannot be performed without the express and freely given prior consent of the employees.

The use of hidden video cameras or in locations which require the protection of individuals' intimacy is forbidden.

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

Please refer to question 10.2 above. The consent of employees is usually obtained in writing. The notification of the employees is also made in writing, usually by posting a relevant notice at the places where video cameras are located.

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

The processing of personal data by video surveillance means, for

the legitimate purposes under question 10.1 above, does not require the notification or consultation of the employees' representatives or trade union.

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

The processing of employees' personal data by video surveillance means is not allowed in offices where employees are working, except in circumstances expressly provided by the law or when the prior approval of ANSPDCP has been obtained.

## 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)?**

Although there are some practical issues, the processing of personal data in the cloud is not forbidden by the legal provisions.

Depending on the nature of the services performed by the cloud computing providers, the latter may be qualified either as data controllers, or as data processors.

As data processors, they should act based on the instructions received from the controllers.

When accessing a cloud computing service, controllers should assess the facilities and the infrastructure for securing data privacy offered by the processors, and the technical and organisational measures for the protection of personal data which they are implementing. The major concerns regarding cloud computing are the following: transparency regarding subcontractors and the location of data centres; the risk that data are processed for other purposes than were initially agreed by the parties; granting permanent access to data; securing data integrity; confidentiality; and the ability of the providers to support the controller in facilitating the exercise of the rights of the data subjects.

**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)?**

ANSPDCP did not issue a binding guidance in this respect. However, the guidelines in the Opinion No. 5/2012 of the European Commission's Data Protection Working Party on cloud computing (the "**Opinion No. 5**") should be observed.

In the light of the Opinion No. 5, the contractual clauses should precisely clarify, among others, at least the following aspects: the object of the contract; the technical and organisational security measures to be taken by the services provider; the persons who will have access to the personal data; the recipients of the personal data; the rights of the controller to perform audits; the obligation of the processor to facilitate the exercise of the rights by the data subjects; and the conditions under which the international transfer is allowed.

## 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)?**

The law guarantees confidentiality of communications by means of public networks and of publicly available electronic communications services, as well as the related traffic data.

The provider of a publicly available electronic communications service may process the traffic data related to subscribers and users for the purpose of marketing electronic communications services or for the provision of value-added services, only to the extent and for the term needed for such services or marketing, if the subscriber or user to whom the data relate has given his consent. Users or subscribers shall have the right to withdraw their consent for the processing of traffic data at any time.

In cases where the big data analytics are performed on anonymous or publicly available data, the consent of data subjects is not generally required.

Relevant binding guidance has not been issued by national authorities so far. However, the general legal principles on personal data protection should also be observed when it comes to big data analytics.

## 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)?**

Order 52/2002 sets forth the minimum security standards for the processing of personal data, which aim mainly at: the implementation of appropriate measures for the identification and login of authorised users; access by each user only to the data necessary for their professional attributions; collection of personal data only by authorised persons and on authorised terminals; execution of security copies; implementation of access logs and encryption systems; secure deletion of unnecessary or outdated data; as well as training of staff on the rules regarding lawful personal data processing.

**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.**

There is no statutory obligation of controllers to report data breaches to ANSPDCP except for the providers of publicly available electronic communication services who must promptly notify ANSPDCP about data breaches.

The notification shall include at least a description of the data breach and the contact details where more information can be obtained, as well as recommended measures to mitigate the possible negative effects of the breach. The notification will include a description of the consequences of the data breach and of the actions already implemented or proposed by the provider to address them.

### 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.

There are no statutory rules compelling the operator to report data breaches to individuals.

However, in the electronic communications field, when the breach could affect the personal data or privacy of a subscriber or any other individual, the supplier must immediately notify the concerned subscriber or individual about such a breach. Notification is not required if the provider can attest that it has applied to the data affected by the security breach appropriate and effective security measures. The same obligation of information subsists in the case of a potential risk of data. If the risk exceeds the scope of the measures that providers can take, they must inform the subscribers about possible remedies and the relevant costs.

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

Failure to comply with the obligations regarding implementation of appropriate personal data security measures and personal data confidentiality is incriminated as a contravention under the Personal Data Law and is sanctioned with a fine amounting between approximately EUR 330 and approximately EUR 11,100 (in national currency equivalent).

Furthermore, under Law No. 506/2004, failure to comply with the obligations regarding confidentiality and securing of the personal data processed in the field of electronic communications is sanctioned with a fine amounting between approximately EUR 1,100 and approximately EUR 22,200 (in national currency equivalent). For companies with an annual turnover exceeding the national currency equivalent of approximately EUR 1,100,000, such fines may reach 2% of the turnover.

## 14 Enforcement and Sanctions

### 14.1 Describe the enforcement powers of the data protection authority(ies).

| Investigatory Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| Preliminary investigations<br>■ upon notification and before processing, in connection with processing operations which may trigger special risks to the individuals' fundamental rights and freedoms. | ANSPDCP has the right to apply administrative fines ranging between approximately EUR 1,100 and approximately EUR 11,000 (in national currency equivalent), and to order temporary suspension or complete cessation of unlawful processing activities. | Whenever there is a reasonable assumption that a criminal offence might have been committed by means of unlawful personal data processing, ANSPDCP shall notify the competent criminal investigation authorities. |
| Ordinary investigations upon complaint or *ex officio*<br>■ ANSPDCP may request from the controller any information related to the processing (including professional and state secrecy) and may verify any relevant document or registration. | | |

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

Recently, ANSPDCP has undertaken a series of investigations in order to assess compliance by local controllers in the banking industry with the legal requirements of data protection. The most significant sanctions were applied for breaches related to the failure to observe the data subjects' right of intervention, and for informing the Credit Bureau without prior notification of the targeted data subjects.

## 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?

In Romania, e-discovery requests are dealt with in different ways depending on the nature of the request.

In civil matters, the legal framework is set forth by Law No. 175/2003 on Romania's accession to the 1970 Hague Convention on the taking of evidence abroad in civil or commercial matters (the "Hague Convention"). Under the Hague Convention, a judicial authority of a signatory state can request Romanian authorities to take evidence, intended only for use in ongoing or contemplated judicial proceedings. Moreover, diplomatic officers or consular agents of a signatory state can take evidence from Romania in aid of judicial proceedings commenced in the state which they represent. Nonetheless, in order for the pre-trial discovery procedure to be lawful, the processing of personal data needs to be legitimate and to satisfy one of the grounds set forth in the Personal Data Law.

In criminal matters, e-discovery by national companies in connection with trans-national criminal investigation can only be requested by national authorities who are entitled to take evidence based on letters rogatory. Consequently, companies cannot disclose personal data directly to foreign law enforcement agencies.

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

In relation to this topic, ANSPDCP has not issued any guidance.

## 16 Trends and Developments

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

ANSPDCP has recently launched some investigations regarding processing of personal data by the bank industry and has applied significant fines for not observing the data subjects' rights and for providing negative information about the financial status of the customers to the Credit Bureau without the prior notification of such customers with respect to the transfer of their personal data to such Bureau.

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

Following the enactment of 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 and repealing Directive 95/46/EC ("GDPR"), ANSPDCP has initiated several campaigns for increasing awareness among the controllers with respect to the new requirements of GDPR. In this respect, the authority has organised seminars, workshops and roundtables having as attendees and speakers stakeholders from the private, as well as the public, sector.

**Mihaela Cracea**
Pachiu & Associates
75–77 Buzesti Street, 5th floor
Bucharest 1
RO-011013
Romania

*Tel:* *+40 21 312 1008*
*Fax:* *+40 21 312 1009*
*Email:* *mihaela.cracea@pachiu.com*
*URL:* *www.pachiu.com*

Mihaela is a lawyer with over 14 years of professional experience, being part of the firm's **Corporate and M&A Department** and coordinating the IT and data privacy, as well as the labour and employment practice areas in this department.

Mihaela has built solid expertise and legal competence in the IT, data protection and intellectual property fields and manages data privacy projects in the digital field, information security and cross-border data flow matters.

Other highlights of Mihaela's practice involve holding seminars on the measures to be implemented so as to ensure data privacy and cyber security compliance and reviewing IT and data privacy policies and other related documentation in terms of local and European statutory provisions in the field.

As a labour and employment lawyer, she has been involved in projects on staff restructuring and transfer of undertaking by providing guidelines, drafting the required documentation, assisting the clients during the negotiations and following up on the post-acquisition issues.

She is a graduate of the Faculty of Law of the Ovidius University in Constanta and holds a LL.M. degree in Business Law and is an intellectual property counsel on trademarks. She is fluent in English and conversant in French and co-authored several *International Comparative Legal Guides* focusing on data protection matters and digital environment and attended, as a speaker, several local conferences on cyber security and data privacy.

**Alexandru Lefter**
Pachiu & Associates
75–77 Buzesti Street, 5th floor
Bucharest 1
RO-011013
Romania

*Tel:* *+40 21 312 1008*
*Fax:* *+40 21 312 1009*
*Email:* *alexandru.lefter@pachiu.com*
*URL:* *www.pachiu.com*

A lawyer with over 12 years of professional experience, Alexandru is a Partner coordinating the firm's **Corporate and M&A Department**.

As head of the Corporate Practice Group (including the Labour Law, Competition, Insolvency and IP sub-practice areas), his practice covers corporate governance and restructuring (mergers, spin-offs, capital restructuring, etc.), intricate joint venture deals and takeover/divestment procedures, as well as private equity funds in complex transactions, including greenfield and brownfield developments. Alexandru has also been involved in financing and insurance matters and constantly advises on competition, insolvency, labour law and recently on several IT deals.

Alexandru plays a key role in the core management team, being in charge with the smooth delivery of all projects in the Corporate Practice Group, supervising and coordinating client and internal practice development.

Alexandru is a graduate of the Faculty of Law of the University of Bucharest and holds an LL.M. awarded by Suffolk University Law School in Boston. He also holds a degree from the Institute of Business Law and International Cooperation "Henri Capitant" – a partnership of the Faculties of Law of the University of Bucharest and the University of Paris I Pantheon Sorbonne.

PACHIU & ASSOCIATES
ATTORNEYS AT LAW · RECHTSANWÄLTE · ABOGADOS

Pachiu & Associates is a leading business law firm based in Bucharest. The firm was established in 2002, developing a sound practice covering all areas of law. There are currently five partners, each heading a department and a practice area in the firm.

Due to our well-established network of clients and partners, we have constantly been involved in a variety of cross-border transactions.

We provide first-class legal skills and market knowledge, combining exceptional legal skills with innovative and lateral thinking, and we believe we have the expertise in guiding you through each key milestone of your project.

Pachiu & Associates has been always noted for the commitment to client service and ability to assist clients with their most demanding legal and business challenges.

**We deliver** our services in **English**, **German**, **French**, **Italian** and **Spanish** with the same ease as we do in **Romanian**.

**We may be of assistance worldwide** through our membership of certain regional and global legal networks and many other reputable law firms located in business centres around the world.

www.pachiu.com

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 Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- 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
- Vertical Agreements and Dominant Firms

glg global legal group

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

www.iclg.com