ICLG

The International Comparative Legal Guide to:

Data Protection 2018

5th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Anderson Mōri & Tomotsune
Ashurst Hong Kong
BSA Ahmad Bin Hezeem & Associates LLP
Clyde & Co
Cuatrecasas
DQ Advocates Limited
Ecija Abogados
Fırat İzgi Attorney Partnership
GANADO Advocates
GÖRG Partnerschaft von Rechtsanwälten mbB
Herbst Kinsky Rechtsanwälte GmbH
Holding Redlich
Jackson, Etti & Edu
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
KPMG Law Firm
Lee & Ko
Loyens & Loeff Luxembourg S.à r.l.
Loyens & Loeff N.V.
LPS L@w
Lydian
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
OLIVARES
OrionW LLC
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at law
Pillsbury Winthrop Shaw Pittman LLP
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Subramaniam & Associates (SNA)
Trevisan & Cuonzo Avvocati
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg
global legal group

global legal group

Contributing Editors
Tim Hickman & Dr. Detlev Gabel, White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Executive 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
June 2018

Copyright © 2018
Global Legal Group Ltd.
All rights reserved
No photocopying

ISBN 978-1-912509-15-7
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapters:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

Disclaimer
This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice.
Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.
This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Romania

Mihaela Cracea

Pachiu & Associates

Alexandru Lefter

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"). The local data protection authority has also issued several decisions with respect to specific aspects of personal data processing.

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 authority(ies) are responsible for data protection?

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 this 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.

- **"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.

- **"Controller"**

  Any individual or private or public legal entity, including central/local public authorities or institutions, who sets forth the purpose and media for the 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.

- **"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.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- **"Data Subject"**

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

- **"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.

- **"Data Breach"**

  There is no definition of data breach.

- *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.

  - **"Data Record System"**

    Any organised data structure, accessed based on determined criteria, irrespective of whether this structure is organised in a centralised or decentralised way or is assigned based on functional or geographic criteria.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes. The data protection laws apply as well to any processing performed by businesses established in other jurisdictions by using processing means located on Romanian territory, except for in cases where such means are used only for allowing the data to transit the Romanian territory.

4 Key Principles

4.1 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 the 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 – please specify*

  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

© Published and reproduced with kind permission by Global Legal Group Ltd, London

safeguarding 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.

5 Individual Rights

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

- **Right of access to data/copies of 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 the 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.
- **Right to rectification of errors**

  Any data subject is entitled to request to the controller, at no cost, to adjust or update the personal data.
- **Right to deletion/right to be forgotten**

  Any data subject is entitled to request to the controller, at no cost, the following:
  - the 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.
- **Right to object to processing**

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

  Data subjects are entitled to require the blocking of data, at any time, to processing of their personal data, provided that the grounds of such an objection are sound and legitimate.
- **Right to data portability**

  Such right shall be available starting from May 25th 2018 when the GDPR shall become applicable.
- **Right to withdraw consent**

  Under the current legislation, such right is somewhat treated as the right to oppose to processing but starting from May 25th 2018, it shall become a distinct right of the data subjects.
- **Right to object 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.
- **Right to complain to the 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.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its 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;

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- 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.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The registration should be related to each purpose of processing. The businesses are required to provide the ANSPDCP with information as provided under question 6.5 below.

6.3 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.

6.4 Who must register with/notify the data protection authority (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 6.4 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 6.1 are applicable to all cases listed herein.

6.5 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 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.

6.6 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.

6.7 What is the fee per registration/notification (if applicable)?

No fees are required.

6.8 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.

6.9 Is any 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

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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.

6.10 Can the registration/notification be completed online?

Yes. There is only an online notification available.

6.11 Is there a publicly available list of completed registrations/notifications?

Yes. On the ANSPDCP website, any interested person may search for the notifications submitted by a business.

6.12 How long does a typical registration/notification process take?

Filling in the online notification might take about two hours. However, 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).

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Currently, 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.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Currently, this is not applicable.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?

Currently, this is not applicable.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Currently, this is not applicable.

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

Currently, this is not applicable.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best 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.

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

Currently, no registration formalities are needed.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Currently, no registration formalities are needed.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Any processing of personal data through processors should be made based on a contract.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The agreement should be in writing, signed by the parties' representatives and should comprise the obligation of the processor to act in accordance with the controller's instructions, as well as the fact that all obligations with respect to the implementation of appropriate organisational and technical measures will be incumbent to it, as well.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing. (E.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?)

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.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.)

Although not expressly regulated, it is recommended that the data subject is informed, at the beginning of the phone call conversation, of the purpose of such call and the data subject is given the opportunity to stop the conversation.

In what concerns the opt-out register, 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.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Considering that local legal provisions apply to any processing performed by a business located in other jurisdictions, but only when it is using local means for such processing, the Romanian legislation shall apply only in case the way the marketing is addressed to data subjects might be construed as a local means of processing.

9.4 Is/are 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.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Although not very widespread, there is a practice in purchasing marketing lists which are of two categories: lists that comprise contact data of individuals; and lists which contain business contact data which may be found on public registers (e.g. Company House). In the majority of the cases, purchasing is not a lawful practice as there is no consent from the data subjects, as their data is to be provided to third parties for marketing purposes.

9.6 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.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are no legislative restrictions on using cookies.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable in Romania.

10.3 To date, has/have 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 an appropriate information notice. Furthermore, processing activities were suspended or even ceased, and deletion of the processed data was ordered.

10.4 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.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

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.

11.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

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.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Any transfer of personal data to countries outside the 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.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

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

12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies typically address this issue?

The applicable legislation does not contain any specific rules. However, according to the recommendations in Opinion No. 1, anonymous reporting should be discouraged. Anonymous reporting may be permitted in exceptional cases and only under specific terms detailed in Opinion No. 1.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

13 CCTV

13.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

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 equipment of public interest, as well as of the related areas;

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

(v) safeguarding 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.

13.2 Are there limits on the purposes for which CCTV data may be used?

Yes. CCTV data is allowed for the fulfilment of any legal obligations or based on a legal interest which basically is the safety of individuals, assets and areas.

14 Employee Monitoring

14.1 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.

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

Please refer to question 14.1 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.

14.3 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 14.1 above, does not require the notification or consultation of the employees' representatives or trade union.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The security of personal data is an obligation for both the controllers and processors. 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 the training of staff on the rules regarding lawful personal data processing.

15.2 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.

15.3 Is there a legal requirement to report data breaches to affected data subjects? 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.

15.4 What are the maximum penalties for data security breaches?

Failure to comply with the obligations regarding implementation of appropriate personal data security measures and personal

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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.

16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Preliminary investigations: 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*: 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.	N/A	N/A

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes. ANSPDCP has the right to issue a ban in relation to a particular processing without the need of a court order.

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

The main approach of ANSPDCP is to require the businesses to remedy the findings discovered during the investigations and to apply administrative sanctions if the breaches proved to be significant and merely recurrent. We have no information as to whether the ANSPDCP has issued a ban in relation to a specific processing.

16.4 Does the data protection authority ever exercise its powers against companies established in other jurisdictions? If so, how is this enforced?

No, as far as we know.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do companies typically 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 investigations 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.

17.2 What guidance has/have the data protection authority(ies) issued?

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

18 Trends and Developments

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

In the last 12 months, ANSPDCP paid particular attention to the ways the controllers have obtained the data subjects' consent for the processing of personal data for different purposes, both in the online environment as well as offline.

18.2 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 27th 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 ("the GDPR"), ANSPDCP has initiated several campaigns for increasing awareness among the controllers with respect to the new requirements of the 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. Moreover, ANSPDCP has launched a guideline with relevant information regarding the implementation of the GDPR.

Acknowledgment

The authors would like to thank Cosmina Sima, Junior Associate at Pachiu & Associates, for her invaluable assistance in the preparation of the chapter. Email: cosmina.sima@pachiu.com.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Mihaela Cracea
Pachiu & Associates
13 Barbu Delavrancea Street
Bucharest 1
RO-011351
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. She coordinates the IT and data privacy department of the firm as well as the labour and employment sub-practice groups.

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 cybersecurity compliance. She also reviews 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 undertakings 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 an 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 cybersecurity and data privacy.

Alexandru Lefter
Pachiu & Associates
13 Barbu Delavrancea Street
Bucharest 1
RO-011351
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 of 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 Pantheon-Sorbonne, Paris.

PACHIU & ASSOCIATES
ATTORNEYS AT LAW · RECHTSANWÄLTE · ABOGADOS

Our firm's **IT & Data Protection Practice Group** is focused on data privacy, intellectual property and e-commerce related matters featuring a dedicated team of lawyers enthusiastic when faced with the intricate challenges of the digital field, and a dynamic industry undergoing continuous development.

The main legal services we provide:

- Verifying legal compliance of projects aimed at the acquisition of companies active in the online environment.
- Drafting and/or reviewing documents required for notifying the data protection authority in terms of personal data processing.
- Verifying compliance of policies, regulations and agreements used by clients in their online businesses.
- Analysing compliance of personal data transfers to third countries which fail to provide a level of protection similar to the one at European level.
- Verifying compliance of policies, regulations and agreements used by clients in their online businesses.
- Analysing risks in the relationships between companies and employees with a view to secure intellectual property rights in favour of companies.
- Verifying policies, regulations and internal practices to secure compliance with the legal requirements on the processing of the personal data of employees, participants to various promotional campaigns, and webpage users for all intents and purposes.
- Any other data protection and intellectual property related matters encountered by clients in their businesses.

For further reference about us, please visit www.pachiu.com.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- 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
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State 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 Investment Funds
- 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