BACK TO DATAGUIDANCE

DataGuidance GUIDANCE NOTES

About The Authors

Ciprian Timofte is a Managing Associate at Ţuca Zbârcea & Asociaţii, drawing upon 11 years of experience in corporate/commercial law, mergers and acquisitions, capital markets and insurance law. Ciprian has extensive experience in the field of personal data protection (from various analyses of implementation solutions for projects regarding/involving processing of personal data, to representing clients to ANSPDCP), direct marketing and advertising, consumer protection and online trade.
Throughout his professional activity, he has provided assistance on a wide range of personal data protection issues. He is an editor of dataprivacyblog.tuca.ro, Ţuca Zbârcea & Asociaţii's blog dedicated to the protection of personal data and the right to privacy.
Email: ciprian.timofte@tuca.ro

Sergiu Cretu is a Senior Associate at Ţuca Zbârcea & Asociaţii, with eight years of experience in areas such as commercial and corporate law, intellectual property law, environmental law. Also, since the beginning of his professional activity, he has focused on projects that involved legal advice on niche areas such as personal data protection, direct marketing and advertising operations, online trade, consumer protection and gambling.
He is an editor of dataprivacyblog.tuca.ro, Ţuca Zbârcea & Asociaţii's blog dedicated to the protection of personal data and the right to privacy.
Email: sergiu.cretu@tuca.ro

Scroll to Top

Romania - Data Protection Overview

Ciprian Timofte and Sergiu Cretu

17 April 2017

1. The Law

1.1. Primary legislation

The main legal enactment in data privacy field is Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data ('the Privacy Act'), published in the Official Gazette of Romania No. 790 dated 12 December 2001, as subsequently amended and supplemented. The Privacy Act fully implements the Data Protection Directive (95/46/EC), having substantially similar provisions.

There are also a series of laws regulating the processing of personal data in particular sectors, such as:

- Law No. 506/2004 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, published in the Official Gazette of Romania No. 1101 dated 25 November 2004 ('the ePrivacy Law'). The ePrivacy Law implements the European Directive on privacy and electronic communications (2002/58/EC).
- Law No. 365/2002 on Electronic Commerce, published in the Official Gazette of Romania No. 959 dated 29 November 2006, as subsequently amended and supplemented ('the E-Commerce Law') (only available in Romanian here). The E-Commerce Law implements the European Directive on Electronic Commerce (2000/31/EC).

1.2. Secondary legislation

There are also secondary norms regulating various data privacy matters, most of which consist in administrative regulations (decisions) passed by the National Supervisory Authority for Personal Data Processing ('ANSPDCP') with regard to matters such as transfer abroad of personal data, video monitoring, processing of personal data performed in an evidence system of credit bureau type systems (unofficial translations of the ANSPDCP's decisions may be found here).

1.3. Guidelines

- ANSPDCP Notification Guidelines (only available in Romanian here);
- Opinions/other deeds alike issued by Article 29 Working Party ('WP29') as regards various data privacy matters, which while not legally binding, could still be viewed as soft-law/guidance with regard to the matters they are dealing with.

1.4. Case Law

To our knowledge, as at date there is quite scarce available national case law in data privacy field. There is however quite rich case law at EU level, mostly rulings of the Court of Justice of the European Union ('CJEU'), out of which the most important are:

- CJEU decision of 1 October 2015 in *Smaranda Bara et al. v. Presedintele Casei Nationale de Asigurari de Sanatate (CNAS) et al.*, C-201/14;
- European Court of Human Rights decision of 12 January 2016 in *Barbulescu vs. Romania* on employer's breach of right to respect for his private life and correspondence and that the domestic courts had failed to protect his right;
- CJEU decision of 1 October 2015 in *Weltimmo s.r.o. v. Nemzeti Adatvedelmi es Informacioszabadsag Hatosag*, C-230/14;
- CJEU decision of 6 October 2015 in *Maximilian Schrems v. Data Protection Commissioner*, C-362/14;
- CJEU decision of 13 May 2014 in *Google Spain SL v. AEPD & Mario Costeja Gonzalez,* C-131/12;
- CJEU decision in *Minister voor Immigratie v. M,* C-141/12 and C-372/12;
- CJEU (Third Chamber) decision of 24 November 2011 in *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* C-70/10;
- CJEU decision of 29 June 2010 in *European Commission v. Bavarian Lager Co. Ltd.*, C-28/08;
- CJEU decision of 7 May 2009 in *College van burgemeester en wethouders van Rotterdam v. Rijkeboer*, C-553/07;
- CJEU decision of 6 November 2003 in C-101/01, *Criminal proceedings against Bodil Lindqvist*.

2. GDPR

The primary aim of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') was to ensure a harmonisation of the data protection rules (and particularly on the way of application of such) amongst EU Member States. To this end, the GDPR has restated and developed to some extent the general rules and principles set forth by the Data Protection Directive.

Still, the GDPR has also introduced a series of substantial changes in data privacy legal regime, out of which we note the following:

a. Territorial scope: As outlined in the Section 4 below, generally the Privacy Act applies to data controllers established on the Romanian territory. By exception, Privacy Act also applies to foreign data controllers which make use of equipment located on the Romanian territory. By contrast, the GDPR envisages a broader scope, namely:

1. it will apply to the data processing carried out by a data controller or data processor established in the UE, regardless whether the processing is carried out inside or outside EU;
2. it will also apply to processing of personal data of data subjects located in the EU performed by data controllers and/or data processors not located in the EU, where the processing relates to offering of goods or services (irrespective of whether payment is required) and to the monitoring of behaviour that takes place within the EU.

b. Elimination of the ANSPDCP's notification formalities: Starting with entry into force of the GDPR, the national provisions requiring the notification of the ANSPDCP will be replaced by one or more of the following obligations: (i) keeping records of data processing activities and enabling the access thereto to the representatives of the ANSPDCP; (ii) appointing a data protection officer (mandatory in certain cases); (iii) performing a data privacy impact assessment and/or prior consultation of the ANSPDCP.

c. Data breach notifications: Currently, the data breach notification obligations are limited to the cases provided by the ePrivacy Law for the electronic communication service providers (for details see Section 12). Under the GDPR, the notification of the data breaches will become mandatory in all cases where it is likely to result in a risk for the rights and freedoms of individuals.

d. Right to information: The GDPR specifically provides that the data controllers shall provide any information related to the data processing 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'. Therefore, the data controllers shall have to make sure that the information notices not only contain minimum information required under the GDPR, but also that those are drafted in intelligible manner (e.g. terms and conditions full of legalese will be not be suitable anymore);

e. Consent requirements:The GDPR contains additional requirements for the validity of the consent of the data subject for the data processing, such as:

1. the consent should be unambiguous: this means that the consent should entail a statement or a clear affirmative action in order to be valid (e.g. ticking a box, choosing technical settings for a website)
2. The consent must be specific (granular): a general broad consent to unspecified processing operations will be invalid; at the same time, where data processing will entail multiple purposes, a consent to those processing activities should cover all those purposes;
3. The consent must be easily revocable: the GDPR not only restates the data subject's right to withdraw the consent, but it also states that the consent must be as easy to withdraw as it is to give it;

f. Facilitation of data transfers to third countries: under the GDPR, the transfer of personal data to unsafe third countries will not require a special authorisation from the ANSPDCP if those ensure adequate safeguards (e.g. Binding Corporate Rules, standard data protection clauses adopted by the EU Commission, approved codes of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights, etc.);

g. Sanctioning regime: Under the Privacy Act, the administrative sanctions range from RON 500 to RON 25,000 (approx. 120 to 5,500 euros). As an exception, the ePrivacy Law contains stricter sanctioning rules (please see Section 10). In stark contrast to the current sanctioning system, under the GDPR the fines for the breach of data privacy rules may be of up to 4% of annual global turnover or €20 million (whichever is greater). The GDPR allows the Member States to lay down rules on other penalties applicable to infringements of the GDPR provisions, in particular for infringements which are not subject to administrative fines pursuant to Article 83 of the GDPR. In this regard, GDPR states that any such national sanctions should be effective, proportionate and dissuasive.

3. Key Definitions | Basic Concepts

- **Personal Data:** Under the Privacy Act, personal data means any information relating to an identified or identifiable natural person [data subject]; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or

Scroll to Top

social identity.

- **Sensitive Data:** Under the Privacy Act, sensitive data means personal data revealing racial or ethnic origin, political opinions, religious, philosophical or other similar beliefs, trade-union membership, and the processing of data concerning health or sex life.
- **Data Controller:** Under the Privacy Act, controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; if the purpose and means of the personal data processing is set out or based on a legal provision, the data controller shall be the natural or legal person assigned as data controller by that specific legal provision;
- **Data Processor:** Under the Privacy Act, data processor means a natural or legal person, of private or public law including public authorities, institutions and their legal bodies, which processes personal data on the data controller's behalf.

4. Scope of Application

4.1. Subjects whom the laws/regulations apply to

The Privacy Act applies to:

a. the processing carried out in the context of the activities of an establishment of the controller on the territory of Romania;
b. the processing carried out in the context of the activities of the diplomatic missions and consular offices of Romania;
c. the processing of personal data, undertaken within the framework of data processing activities of data controllers not established on the territory of Romania and, for purposes of processing personal data, such controllers make use of equipment, automated or otherwise, situated on the territory of Romania, unless such equipment is used only for purposes of transit through the territory of Romania.

Also, ANSPDCP deems that the processing of personal data carried out by the data controllers established in another Member State shall be governed by the law of that Member State, even though the processing shall be carried out by means located on the territory of Romania (provided that such means do not qualify as an establishment). Such approach is in line with the basic principle laid down under Article 4(1)(a) of the Data Protection Directive, which gives prevalence to the law of the EU state where the data controller has an establishment (for details on the concept of applicable law, please refer to the analysis included in the Opinion 8/2010 on Applicable Law issued by the WP29).

4.2. Types of processing covered/exempted

The Privacy Act provides that it applies to any processing performed by any individual or legal entities, irrespectively whether such processing is carried-out in public or private sector.

The following processing of personal data do no fall within the scope of the Privacy Act:

a. processing carried out by individuals exclusively for private use, provided the processed data are not supposed to be disclosed to third parties; and
b. processing and data transfers, performed in the context of activities pertaining to national defense and national security, carried within the limits and restrictions provided by the law.

5. DPA | Regulatory Authority

The ANSPDCP is an independent public authority legally entrusted with overseeing and controlling the legality of personal data processing falling under the scope of the Privacy Act. The ANSPDCP is the authority receiving notifications of personal data processing, issuing authorisations for processing where such authorisations are required, and also investigating and sanctioning controllers and processors which fail to comply with the Privacy Act. The ANSPDCP also issues administrative regulations in the field of personal data processing and has also the power to act in justice and to stand as claimant before courts with regard to various data privacy matters.

6. Notification | Registration

Following the issuance of ANSPDCP's Decision No. 200/2015, the rule is that processing of personal data do not need to be notified/ registered with the ANSPDCP (prior to such, only expressly excepted cases were not subject to notification).

The same Decision No. 200/2015 enumerates a series of limitative cases where notification is still required, which include:

- processing of personal data related to racial or ethnic origin, political, religious, philosophical or similar beliefs, personal data related to trade union membership, as well as health data and data related to sex life (e.g. market research);
- processing of genetic and biometric data (e.g. clinical study);
- processing of personal data which directly or indirectly allows the geographical localisation of natural persons through electronic means (e.g. monitoring or security of persons and / or public or private goods via GPS);
- transfer of personal data towards non-EEA states for which the Commission has not recognised by decision an adequate level of protection of personal data.

Submitting a notification with the ANSPDCP involves the completion of the standard

notification form (only available in Romanian here) in accordance with the instructions comprised in ANSPDCP's Guidance on Notifications (only available in Romanian here). The notification is free of charge.