



INTERNATIONAL
LAWYERS
NETWORK

2024

ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com



ILN Cybersecurity & Data Privacy Group and ILN
Technology Media & Telecommunications Group



Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

Each contributing law firm is the owner of the copyright in its contribution. All rights reserved.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was

honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. **Cybersecurity & Data Privacy Group**

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. **Technology, Media & Telecom (TMT)**

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.



Romania

Introduction

PETERKA & PARTNERS is a modern, independent and integrated CEE full-service law firm with worldwide activities and a leader on the regional market. The law firm benefits from a unique coverage across the CEE region, operating 100% fully-owned offices in the Czech Republic, Slovakia, Poland, Hungary, Bulgaria, Romania, Ukraine and Croatia.

PETERKA & PARTNERS opened its Romanian office in 2010 and strengthened the position of the firm in the CEE region, helping companies towards the expansion of their business in a key market like Romania.

The Romanian team of PETERKA & PARTNERS consists of experienced and business-oriented lawyers with extensive knowledge of Romanian law and industry insight and

provides domestic and international clients with complex legal services in all business law areas, from day-to-day assistance to sophisticated transactions, with a focus on Corporate and M&A, Labour Law, Real Estate, General Commercial and Distribution, Litigation and Insolvency, Compliance and Regulatory, Banking and Finance, E-commerce and Tax.

The Bucharest office assists clients active in a wide range of industries, including Automotive, Aviation, Retail and Luxury, Energy, IT&C and Technology, Pharma and Life Sciences and Transportation and Logistics.

All our lawyers are registered with the Romanian Bar Association and are fluent in English, while part of the team may assist in French as well.

Governing Data Protection Legislation

2.1. Overview of principal legislation

The General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), as implemented

Contact Us

☎ +40 21 310 48 82

🌐 www.peterkapartners.com/en/local/bucharest/

✉ ciupala@peterkapartners.ro

📍 33 Aviatorilor Boulevard, 2nd floor, 1st District
Bucharest, 011853 Romania

by Law 190/2018 is the principal data protection legislation in Romania. The collective citation of these pieces of legislation used hereafter will be “Romanian Data Protection Acts”.

Law 129/2018 completing Law No 102/005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing repealed the previous laws, Law 667/2001 for the protection of individuals in regards to Personal Data Processing and the free circulation of such data which regulated the data protection in Romania before the enactment of the GDPR.

In Romania, the following pieces of sectoral-specific legislation impact data protection:

- Law No 146/2021 on electronic monitoring in judicial and executive criminal proceedings
- Law No 363/2018 on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of preventing, detecting, investigating, prosecuting and combating criminal offences or the execution of penalties, educational and security measures, and on the free movement of such data.
- Law No 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector

However, this Guide does not cover these laws, but instead focuses on the general rules applicable to Data Protection in Romania, highlighting, whenever applicable, the derogations as contained in Law 190/2018 which are permitted under the GDPR.

2.2. Additional or ancillary regulation, directives or norms

The National Authority for the Supervision of Data Processing (ANSPDCP) is the Romanian supervisory authority that is responsible for monitoring the application of the GDPR, and has functions and powers related to the regulation of data processing, monitoring the fulfilment of legal obligations by personal data controllers, and investigation of violations of data subjects' rights, ex officio or upon the receipt of a complaint or referral.

In the exercise of its powers, the ANSPDCP shall issue binding decisions and instructions to public authorities and institutions, legal entities governed by private law, and any other bodies, as well as to natural persons whose activities fall within the scope of the legislation on the protection of individuals with regard to the processing of personal data, hereinafter referred to as entities. Decisions and instructions of a regulatory nature are published in the Official Gazette of Romania.

The applicable decisions are:

- Decision No 133 of 3 July 2018 approving the Procedure for the receipt and settlement of complaints
- Decision No 161 of 9 October 2018 approving the Procedure for conducting investigations
- Decision No 174 of 18 October 2018 on the list of operations for which it is obligatory to carry out a personal data protection impact assessment

There are also soft law documents of importance for the interpretation of applicable law from the European Data Protection Board (former Article 29 Working Party), namely:

- Opinion No 2/2017 on data processing in the workplace;
- Working document on the supervision of electronic communications in the workplace;
- Opinion No. 8/2001 on the processing of personal data in the context of employment;
- Opinion No 6/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC;
- Guidelines 9/2022 on personal data breach notification under the GDPR;
- Guidelines 01/2022 on data subject rights – Right of access;

2.3. Upcoming or proposed legislation (if applicable)

There is no upcoming or proposed legislation in Romania.

Scope of Application

3.1. Legislative Scope

As per GDPR.

3.1.1. Definition of personal data

As per GDPR.

3.1.2. Definition of different categories of personal data

As per GDPR.

3.1.3. Treatment of data and its different categories

- Regulation of personal and non-personal data: As per GDPR.
- Regulation of electronic and non-electronic data: As per GDPR.

Specific Romanian regulations

Three situations of data processing are regulated separately from the provisions of the GDPR, namely:

- **Processing a national identification number**

The processing of a national identification number, along with the collection or disclosure of documents containing it, must

adhere to specific safeguards implemented by the controller. These safeguards include:

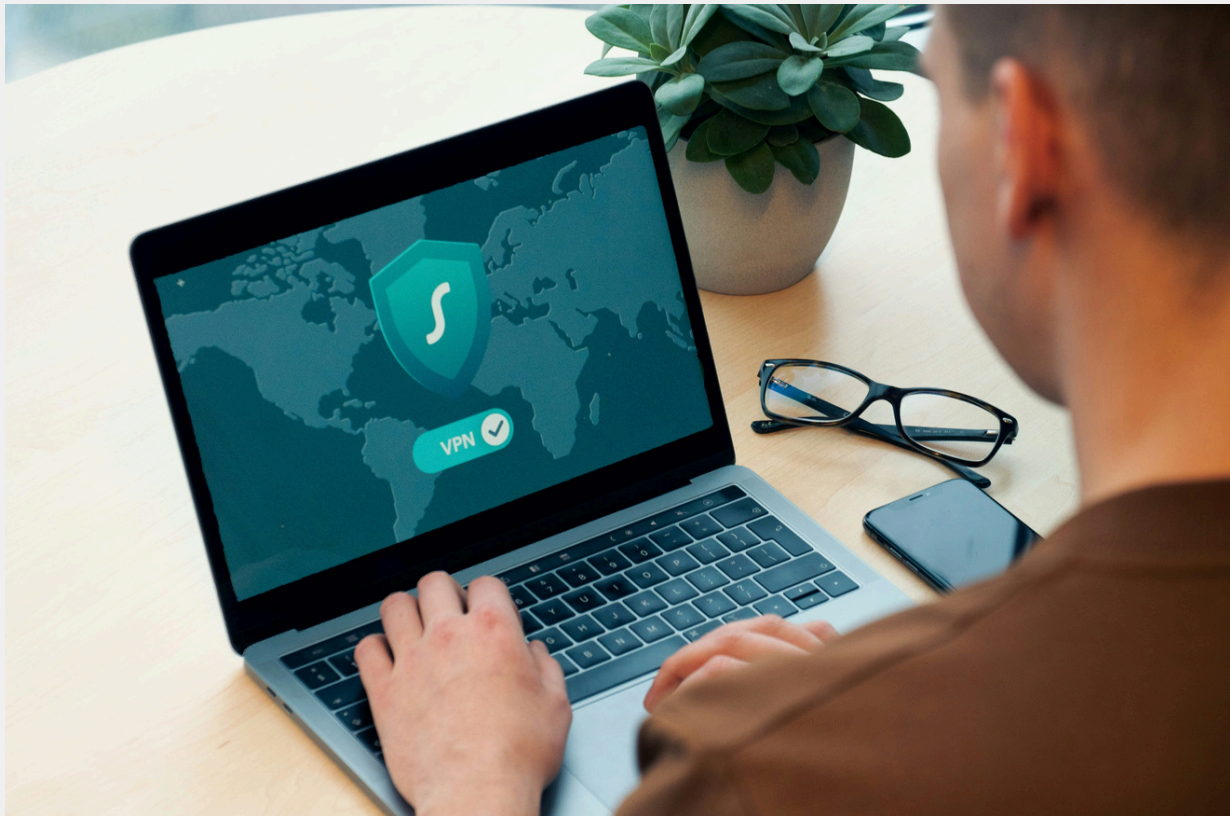
a) Implementation of Appropriate Technical and Organizational Measures: The controller must establish and apply suitable technical and organizational measures. These measures serve to ensure compliance with the principle of data minimization, as well as to guarantee the security and confidentiality of the personal data processing.

b) Appointment of a Data Protection Officer (DPO): The controller is

required to appoint a Data Protection Officer, responsible for overseeing and advising on compliance with data protection regulations.

c) Establishment of Storage Periods: The controller should define storage periods based on the nature of the data and the purpose of processing. Additionally, specific timeframes must be set for the deletion, or review for deletion, of personal data.

d) Regular Training: Persons involved in processing personal data under the direct authority of the controller or processor must undergo regular training. This training aims to ensure a comprehensive understanding of



the obligations related to the processing of personal data.

- **Processing of personal data in the context of employment relationships**

Where monitoring systems by means of electronic communications and/or video surveillance are used at the workplace, the processing of personal data of employees for the purpose of the legitimate interests pursued by the employer is only permitted if the following conditions are met:

a) Balancing of Interests: The legitimate interests pursued by the employer must be duly justified, and these interests must outweigh the interests, rights, and freedoms of the data subjects (employees).

b) Full and Explicit Prior Information: The employer is required to provide employees with comprehensive and explicit information before initiating the monitoring systems. This ensures transparency regarding the purpose and scope of the data processing.

c) Consultation with Trade Union or Representatives: Prior to implementing monitoring systems, the employer must consult with the trade union or, where applicable, employees' representatives. This consultation is a crucial step in obtaining input and feedback from the workforce.

d) Exploration of Less Intrusive Alternatives: The employer must demonstrate that other, less intrusive methods of achieving the intended purpose have been considered and

proven ineffective. This underscores the importance of exploring alternatives before resorting to more invasive monitoring systems.

e) Proportionate Duration of Data Storage:

The duration for which personal data is stored must be proportionate to the purpose of processing. Generally, this should not exceed 30 days, unless specific situations provided for by law or duly justified cases necessitate a longer storage period.



- **Processing of personal data and special categories of personal data in the context of a task carried out in the public interest**

The processing of personal and special data necessary for the performance of a task carried out in the public interest shall be carried out with the establishment of the following safeguards by the controller or the third party:

a) implementation of appropriate technical and organizational measures to comply with the principles of the GDPR, in particular data minimization and the principle of integrity and confidentiality;

b) the appointment of a data protection officer;

c) the establishment of storage periods depending on the nature of the data and the purpose of the processing, as well as specific periods within which personal data must be deleted or reviewed for deletion;

3.1.4. Other key definitions pertaining to data and its processing

As per GDPR.

Specific Romanian regulations

The following are also defined:

- **“Authorities and public bodies”** – the Chamber of Deputies and the Senate, the Presidential Administration, the Government, ministries, other specialized bodies of central public administration, authorities and

- autonomous public institutions, authorities of local and county public administration, other public authorities, as well as institutions under their subordination/coordination. For the purposes of the law, religious entities and associations and foundations of public utility are assimilated to public authorities/organizations;

- **“National identification number”** – the number by which an individual is identified in certain record systems and which has general applicability, such as: personal identification number, series and number of the identity document, passport number, driver's license number, social security number;

- **“Remediation plan”** – annex to the finding and sanctioning minutes of the offence, by which the National Supervisory Authority for Personal Data Processing establishes measures and a remediation deadline;

- **“Remediation measure”** – a solution ordered by the national supervisory authority in the remediation plan for the fulfilment by the public authority/organization of the obligations provided by law;

- **“Remediation deadline”** – a period of up to 90 days from the date of communication of the finding and sanctioning minutes

- of the offence, during which the public authority/organization has the opportunity to remedy the identified irregularities and fulfil legal obligations;
- **“Performing a task serving a public interest”** – includes activities of political parties or organizations of citizens belonging to national minorities, non-governmental organizations, serving the achievement of objectives provided by constitutional law or international public law or the functioning of the democratic system, including encouraging citizen participation in the decision-making process and policy preparation, respectively promoting the principles and values of democracy.

3.2. Statutory exemptions

As per GDPR.

Specific Romanian regulations

There are two exemptions from the GDPR rules, namely ***in the processing of personal data for journalistic purposes or for purposes of academic, artistic, or literary expression*** when the processing relates to personal data which have been manifestly made public by the data subject or which are closely linked to the public status of the data subject or to the public nature of the facts in which it is involved ***and in the processing of personal data for scientific or historical research purposes, for statistical purposes or for archiving purposes in the public interest*** when

the derogation is necessary to achieve those purposes.

3.3. Territorial and extra-territorial application

As per GDPR.

Legislative Framework

4.1. Key stakeholders

As per GDPR.

4.2. Role and responsibilities of key stakeholders

As per GDPR.

Requirements for Data Processing

5.1. Grounds for collection and processing

As per GDPR.

5.2. Data storage and retention timelines

As per GDPR.

5.3. Data correction, completion, data updating or erasure of data

As per GDPR.

5.4. Data protection and security practices and procedures

As per GDPR.

Specific Romanian regulations

In order to ensure an increased level of security in employer-employee relations, Romanian legislation has also introduced the obligation that where monitoring systems are used by means of electronic communications and/or by means of video surveillance at the workplace, the processing of employees' personal data, for the purpose of achieving the legitimate interests pursued by the employer, is allowed only if the duration of storage of personal data is proportionate to the purpose of the processing, but not for more than 30 days, except in situations expressly regulated by law or in duly justified cases. So, if the employer wants to carry out surveillance by video or electronic means it must delete the stored data after a maximum of 30 days from the date of storage.

5.5. Disclosure, sharing and transfer of data

As per GDPR.

5.6. Cross border transfer of data

As per GDPR.

5.7. Redressal of grievances

As per GDPR.

Specific Romanian regulations

Any data subject who believes that the processing of their personal data violates the applicable legal provisions has the right to lodge a complaint. This applies particularly if the alleged breach occurs within

Romania or affects the data subject's habitual residence or place of work. Complaints must be submitted in writing, either in Romanian or English, and sent to the supervisory authority. The supervisory authority shall inform the data subject of the admissibility of the complaint within 45 days of registration at the latest. If the authority finds that the information in the complaint is incomplete or insufficient, it may request the data subject to provide additional details for the complaint to be considered admissible for investigation. The National Supervisory Authority is then obligated to update the data subject on the progress or outcome of the investigation within 3 months from the date of informing the complainant that the complaint is admissible.

In addition to filing a complaint with the supervisory authority, data subjects also have the right to address their complaint directly to the competent court to defend their rights as guaranteed by applicable law. Where a legal claim has been brought with the same subject matter and same parties, the supervisory authority may order the suspension of, and/or close, the complaint, as appropriate. The data subject will have to inform the Authority, via a complaint form, of the lodging of such a complaint with the court.

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

As per GDPR.

6.2. Duties

As per GDPR.

Processing of the data of Children or Minors

As per GDPR.

Specific Romanian regulations

The processing of the personal data of a child carried out on the basis of consent, is lawful only when the child is at least 16 years of age. If the child is under the age of 16, such processing is lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

Regulatory Authorities

8.1. Overview of relevant statutory authorities

As per GDPR.

Specific Romanian regulations

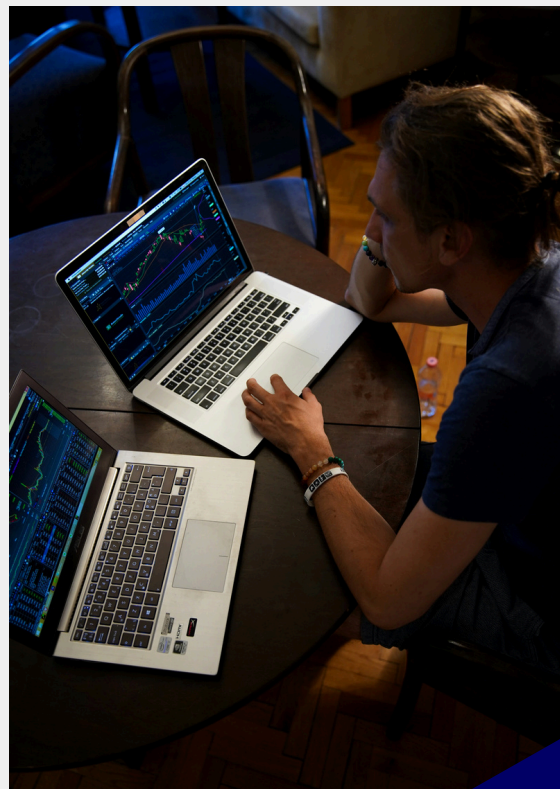
The National Supervisory Authority for Personal Data Processing, hereinafter referred to as the National Supervisory Authority, is a public authority with legal personality, autonomous and

independent from any other authority of the public administration, as well as from any natural person or legal entity in the private sector, which exercises the powers conferred to it by the legal provisions on the processing of personal data and the free movement of such data.

8.2. Role, functions and powers of authorities

- **Role functions and powers of principal data regulation authority**

In Romania, the data regulation authority is the National Supervisory Authority for Personal Data Processing.



Romania

The objective of the National Supervisory Authority is to protect the fundamental rights and freedoms of natural persons, and in particular their right to private, family and private life, in relation to the processing of personal data and the free movement of such data.

Among the main tasks of the National Supervisory Authority for Personal Data Processing and its President, established in accordance with the GDPR, are:

- monitoring the uniform application of personal data protection legislation by all entities acting as data controllers;
 - regulation, through the drafting of binding decisions and instructions, which are published in the Official Gazette of Romania;
 - endorsement of draft legislation on personal data protection;
 - guidance, through advisory activity, including to Parliament, the Government and other public authorities or institutions and to entities acting as data controllers, and informing data subjects and the public of their obligations under the legislation on personal data protection and the rights guaranteed by law;
 - monitoring the fulfilment of legal obligations by personal data controllers, through powers to investigate violations of data subjects' rights, ex officio or upon receipt of a complaint or referral;
- applying corrective measures in cases where breaches of the relevant legislation are found;
 - cooperation and mutual assistance with the supervisory authorities of the other Member States, as well as cooperation with the European Commission and the European Data Protection Board, in the framework of the mechanism to ensure consistency in the application of the General Data Protection Regulation throughout the EU;
 - informing the Parliament, the Government, the European Commission, and the European Data Protection Board on its activities by means of an annual activity report.

In addition to the national authority, there is the European Data Protection Board (EDPB) acting at both the European and national level. The EDPB is an independent European body. It is the umbrella organization which brings together the national data protection authorities (National Supervisory Authorities) of the countries in the European Economic Area, as well as the European Data Protection Supervisor (EDPS) for ensuring a consistent application and enforcement of data protection law across the EEA, and providing general guidance (including guidelines, recommendations and best practices).

8.3 Role, functions and powers of civil/criminal courts in the field of data regulation

As per GDPR.

Specific Romanian regulations

If, in the exercise of its legal powers, the national supervisory authority considers that any of the rights of data subjects guaranteed by the legal regulations on the protection of personal data have been infringed, it may bring the matter before the competent court, in accordance with the law.

In this situation, the data subject shall automatically acquire the status of complainant and shall be summoned as such. If the data subject accepts the action, the National Supervisory Authority's capacity to bring proceedings shall cease. If the person concerned does not accept the action brought by the national supervisory authority, the court shall cancel the application in accordance with the Code of Civil Procedure.

Actions and applications, including those for ordinary or extraordinary legal remedies, brought by the National Supervisory Authority shall be exempt from the payment of stamp duty.

On the other hand, courts intervene directly when data protection crimes are being committed. Such crimes are: illegal access to a computer system, illegal interception of a computer data transmission, altering the integrity of computer data, disrupting the operation of computer

systems, unauthorized transfer of computer data, and illegal operations with computer devices or software.

Consequences of non-compliance

As per GDPR.

Specific Romanian regulations

The violation of the followings constitutes an infringement and is punishable by administrative fines of up to EUR 20,000,000 or, in the case of a company, up to 4% of the turnover:

- Processing of genetic data, biometric data or health data
- Processing of a national identification number
- Processing of personal data in the context of employment relationships
- Processing of personal data and special categories of personal data in the context of the performance of a task carried out in the public interest
- Processing of personal data for journalistic purposes or for purposes of academic, artistic, or literary expression
- Processing of personal data for scientific or historical research purposes, for statistical purposes or for archiving purposes in the public interest

Romania

- Processing of personal data by political parties and organizations of citizens belonging to national minorities, non-governmental organizations

Conclusion

As can be observed throughout this guide, Romania focuses mainly on the GDPR for the protection of personal data, with additions being made by Law No. 190/2018 which regulates the situation of special categories of data, the authority in charge of data protection at the national level, and the way of sanctioning and the penalties applicable in case of non-compliance with the legal provisions applicable to data protection.

Contact Us

☎ +40 21 310 48 82

🌐 www.peterkapartners.com/en/local/bucharest/

✉ ciupala@peterkapartners.ro

📍 33 Aviatorilor Boulevard, 2nd floor, 1st District
Bucharest, 011853 Romania