COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Romania

DATA PROTECTION & CYBERSECURITY

Contributor

Bondoc si Asociatii SCA

Lucian Bondoc

Managing Partner | lbondoc@bondoc-asociatii.ro

Monica Iancu

Partner | miancu@bondoc-asociatii.ro

Diana Savu

Managing Associate | dsavu@bondoc-asociatii.ro

Andra Gheorghe

Managing Associate | agheorghe@bondoc-asociatii.ro

Alexandru Daniliuc

Senior Associate | adaniliuc@bondoc-asociatii.ro

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Romania.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

ROMANIA
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

As of 25 May 2018, the main piece of legislation governing **privacy related matters** in Romania, irrespective of the sector or activity field, is *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)* ("**GDPR**").

The national legal framework also includes other pieces of legislation, namely:

i. Law no. 190/2018 on the measures for the application of GDPR ("**Romanian Data Privacy Law**"), which sets forth specific rules for the cases where the GDPR allows Member States to further tailor certain measures;
ii. Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector ("**Romanian e-Privacy Law**"), which transposes the e-Privacy Directive[1] in the Romanian legislation and regulates, among others, the use of cookies and the data processing for direct marketing purposes;
iii. Law no. 363/2018 on the protection of natural persons with regards to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, which transposes the Law Enforcement Directive[2] in the Romanian legislation ("**Law 363/2018**").

The competent authority in Romania for data privacy matters is the National Supervisory Authority for Personal Data Processing ("**NSAPDP**"), which is an autonomous central public authority with general competences in the field of personal data protection and acts as a guarantor of fundamental rights to private life and personal data protection. The privacy related legal framework is supplemented by the decisions adopted by NSAPDP with respect to investigations, settlement of complaints, data breach notifications *etc.*

As for **cybersecurity matters**, one of the main pieces of the relevant national legal framework is represented by Law no. 362/2018 on measures to secure a high common level of security of networks and information systems ("**Romanian Cybersecurity Law**"), which transposes the NIS Directive[3] in the Romanian legislation. The Romanian Cybersecurity Law benefits from a series of subsequent regulatory acts that ensure its effective application, and which include, among others, regulatory acts for the approval of the list of essential services, methodological norms for the organization and functioning of the Registry of operators of essential services ("**OES**"), various technical norms and regulations *etc.* At European level, the NIS2 Directive[4] entered into force on January 16th, 2023, and Romania must adopt and publish the measures necessary to comply with the NIS 2 Directive by October 17th, 2024. The NIS2 Directive affects all entities that provide essential or important services to the European economy and society, including digital providers (*e.g.* social networks, search engines, online marketplaces) and digital infrastructure (*e.g.* cloud computing service providers and ICT management).

Additionally, a novelty in the cybersecurity framework was brought by *Law no. 58/2023 on the cybersecurity and cyber defence of Romania, as well as for amending and supplementing some normative acts* ("**Cyber-defence Law**"), which entered into force on March 18th, 2023, and sets forth the obligations of various types of

entities and the corresponding prerogatives of public authorities and institutions that have specific responsibilities and capabilities in preventing and countering cyber threats, vulnerabilities, and risks. With respect to private entities, the Cyber-defence Law applies to individuals and legal persons that own, organize, manage, or use informational networks or systems and provide public services or services of public interests. The Cyber-defence Law was followed by a series of subsequent regulatory acts aimed at ensuring its enforcement, including methodological norms on the request and communication of incident data and information and rules establishing cyber alert levels and ways of action in cyber alert situations *etc.*

As regards the competent authority in the cybersecurity field, the National Cyber Security Directorate ("**NCSD**") is the Romanian national cybersecurity and incident response body, that aims to create a coherent and resilient cybersecurity architecture at national level. The main responsibility of NCSD is to ensure the cybersecurity of the national civilian cyberspace, in collaboration with the competent institutions and authorities.

Of further relevance for the data protection and cybersecurity areas are the regulatory acts adopted for the effective implementation of the National Interoperability Framework[5].

One of these implementation acts is *Law 242/2022 on the exchange of data between information systems and the creation of the National Interoperability Platform* ("**Interoperability Law**"), which aims to increase the quality of public services by facilitating the exchange of data between information systems, reducing the bureaucratic and administrative burden on individuals and legal entities, and increasing the transparency of data use by public authorities and institutions. The Interoperability Law provides for the establishment of the National Interoperability Platform with the control, monitoring and evaluation function being the responsibility of the Authority for the Digitization of Romania ("**ADR**")[6]. On November 3rd, 2023, the regulatory framework has been extended with the *Reference Standards for achieving interoperability in the field of information and communication technology*[7], establishing technical rules and standards as a basis for interoperability and compatibility of existing or to be developed platforms, applications, IT systems, as well as process and data standardization. Furthermore, in the last year, Romania took further steps for the creation and operation of the Government Cloud, which is operationally managed by the ADR and will consist of a set of IT, communications and cyber security resources owned by the Romanian state, interconnected at service level with public clouds and/or private clouds.

Last but not least, the Romanian entities are also subject to the European regulations, which are directly applicable, and which have influence in the data privacy and cybersecurity sectors, including, but not limited to the following:

i. The Digital Services Act ("**DSA**")[8] which became directly applicable across the EU on February 17th, 2024, to a broad category of online services, from intermediary and hosting services to large online platforms, whether established in the EU or outside, as long as the services are offered in the EU single market. The purpose of DSA is to minimise harms and counter risks online, while also introducing a new framework that prioritizes transparency and accountability. Correlatively, the Romanian legislator adopted Law No. 50/2024 on the establishment of measures for the implementation of the DSA[9], which established the National Authority for Administration and Regulation in Communications ("**ANCOM**") as the competent authority, the sanctioning regime, as well as other measures necessary for the application of the DSA.
ii. The Digital Markets Act ("**DMA**")[10] became fully applicable across the EU on May 2nd, 2023, in relation to large, core online platforms (including search engines, online marketplaces, social networking and video sharing platforms) which qualify as "gatekeepers". The DMA places several restrictions on gatekeepers, including limiting the legal bases for processing personal data, prohibiting the processing of certain data for the purpose of competing with other businesses (unless that data is publicly available), requiring the sharing of end users' data with other businesses and advertising companies, and facilitating end users' data portability requests. These measures aim to create a more competitive and transparent digital market, along with a safer internet, to protect the privacy and data rights of end users, and to increase accountability among gatekeepers.
iii. Data Governance Act ("**DGA**")[11] became fully applicable across the EU on September 24th, 2023, and regulates the secondary use of personal and non-personal data held by public sector bodies and the creation of new business models and applicable rules for data intermediaries (such as data marketplaces). It

also promotes the concept of data altruism and provides a voluntary registration framework for entities that collect and process data for altruistic purposes. Finally, the DGA sets out appropriate safeguards regarding transfers of non-personal data from third countries, ensuring that a data re-user in a non-EU country provides a level of protection that is essentially equivalent to that provided by Union law.

Footnote(s):

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[5] The National Interoperability Framework was approved under Government Decision no. 908/2017, based on the provisions of the European Interoperability Framework.

[6] According to the law, central and local public authorities and institutions holding a basic register are obliged to integrate with the National Interoperability Platform within a maximum of 18 months after the platform becomes operational and to provide access to such data through the platform. It should be mentioned that this law is also applicable by voluntary participation, on the basis of a data exchange contract, to private legal entities, i.e. persons exercising regulated liberal professions, those who own IT systems and have data of interest to public authorities and institutions.

[7] Order No. 21286/2023 approving the Reference Standards for achieving interoperability in the field of information and communication technology.

[8] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[9] Law No 50/2024 on the establishment of measures for the implementation of Regulation (EU) 2022/2.065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (the Digital Services Regulation), as well as amending and supplementing Law No 365/2002 on electronic commerce, effective from 22 March 2024.

[10] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[11] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

The main piece of legislation that will bring significant amendments to the current legislative framework is the e-Privacy Regulation[12], which is still undergoing legislative processes and has not been officially adopted by the European Union, and will be directly applicable in Romania once completed and entered into force. In addition to the e-Privacy Regulation, there also are various expected pieces of legislation which, if eventually implemented, will also have consequences in terms of personal data processing and the protection of individuals' privacy, including the adoption of rules regarding the responsible use of technology in the context of the deepfake phenomenon[13] (*please also see Question 14*).

Also, the Romanian legislative framework will continue to be impacted by the legal framework pending adoption and/or implementation of legislative acts at European level on artificial intelligence, cybersecurity, data and

digital markets, that will affect businesses in a wide range of sectors, namely:

i. The AI Act[14] which was adopted on March 13th, 2024, by the European Parliament and is expected to be finally adopted through the so-called corrigendum procedure. The AI Act is a regulation on artificial intelligence ("**AI**"), one of the first of its kind proposed around the world, introducing a new risk-based approach that will be uniformly applied across all Member States.
ii. The Data Act[15] entered into force on January 11th, 2024, and is set to be applicable from September 12th, 2025, bringing clarity to data access by defining who can access data and under what conditions, thereby facilitating increased data sharing among private and public entities and contributing to the development of new services (particularly in AI, where vast amounts of data are required for algorithm training).
iii. The Cyber Resilience Act ("**CRA**")[16] (proposal), which imposes cybersecurity assessments and requirements on products with digital features, was approved by the European Parliament on March 12th, 2024, and awaits formal adoption by the Council to be enacted into law.
iv. The Cyber Solidarity Act[17] ("**CSA**") (proposal), on which a political agreement was reached recently between the European Parliament and the Council (on March 6th, 2024) and is now subject to formal approval. It introduces vital measures to bolster cybersecurity resilience and response capabilities across Member States, including Romania.

Footnote(s):

[12] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

[13] Draft law on the responsible use of technology in the context of the deepfake phenomenon.

[14] Proposal for a Regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts. The adopted text of the AI Act is available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

[15] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

[16] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

[17] Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

There are no registration or licensing requirements under the Romanian data privacy legislation. Nonetheless, if a data protection officer ("**DPO**") has been appointed as per the legal provisions, the data controller or the data processor shall communicate the contact details of the DPO to the NSAPDP using a template notification form. There are other forms of interactions with NSAPDP (e.g., in connection with any residual risks resulting from data protection impact assessments) but these are generally in line with the GDPR rules.

According to the Romanian Cybersecurity Law, all OES (providing a wide array of essential services from several economic sectors, including healthcare, energy, transport, supply and distribution of drinking water, digital infrastructure, banking, and financial market infrastructures, as defined therein) are required to comply with various obligations, including the obligation to notify the NCSD in order to be registered within the Registry of OES. Additionally, there is an obligation for private entities to analyse and notify the applicability of the Cyber-defence Law to NCSD. Based on such analysis, NCSD shall confirm or infirm the applicability of Cyber-defence Law to that entity.

Nevertheless, we mention that *Law No. 50/2024 on the establishment of measures for the implementation of the DSA* requires any provider of intermediate services in Romania to submit to ANCOM, within no more than 45 days from the date of starting the provision of services, an information in this regard.

4. How do these data protection laws define “personal data,” “personal information,” “personally identifiable information” or any equivalent term in such legislation (collectively, “personal data”) versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

In Romania, the definition of „*personal data*” is the one provided under Article 4 para. (1) of the GDPR[18]. Also, the definition of „*special categories of personal data”* is the one provided under Article 9 para (1) of the GDPR[19].

However, the Romanian Data Privacy Law further defines the concept of national identification number the processing of which is subject to particular requirements if it is based on the controller’s legitimate interest. The national identification number is defined as the number according to which a natural person is identified in certain record keeping systems and which has a general applicability, such as: personal numeric code, number of the identity document, passport number, driving license number, social health insurance number *etc.*

The cybersecurity framework does not amend these definitions and the general rule is that any processing of personal data shall be carried out in compliance with the legal provisions on the protection of personal data.

Footnote(s):

[18] any information relating to an identified or identifiable natural person („data subject„), in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[19] data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or “fair information practice principles” in detail.

Given the direct applicability of the GDPR in Romania, all its mandatory requirements must be duly implemented and observed, including the principles relating to processing of personal data (provided in Article 5 of the GDPR). These principles have the meaning and scope assigned under the GDPR:

i. The lawfulness, fairness and transparency principle;
ii. The purpose limitation principle;
iii. The data minimization principle;
iv. The accuracy principle;
v. The storage limitation principle;
vi. The integrity and confidentiality principle;
vii. The accountability principle.

As regards storage, as an exception provided by GDPR, personal data may be kept for a longer period for archiving purposes in the public interest or for scientific or historical research purposes, provided that appropriate technical and organisational measures (such as anonymisation, encryption, etc.) are implemented.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

There are certain specific situations for which the Romanian legislation requires that personal data should only be processed after obtaining a data subject’s consent. Notably, under the Romanian e-Privacy Law, a data subject’s consent is mandatory for the processing of personal data for direct marketing purposes by electronic means. Article 12 thereof states that “*the performance of commercial communications by using automated calling systems that do not require human intervention, by fax, electronic mail, or by means of any other method employing publicly available electronic communications services, is forbidden, except where the concerned subscriber has previously given his/her express consent to receive such communications*”. The law also establishes an exception from obtaining consent, by implementing a soft opt in mechanism if there was a previous commercial agreement between the data controller and the data subject.

Furthermore, the Romanian Data Privacy Law further

establishes particularities with regard to the processing of genetic data, biometric data and data concerning health for the purpose of automated decision-making or profiling, *i.e.* the processing thereof is only permitted based on two legal grounds, namely the explicit consent of the data subject or the existence of legal obligations in this regard.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

With regard to how consent must be given by data subjects and further managed by data controllers, the Romanian legislation does not provide for certain particularities and thus, the conditions provided in the GDPR definition of "consent" ("*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*"), as well as the requirements set forth under Article 7 (Conditions for consent) of the GDPR apply.

Additionally, in relation with the minimum requirements that must be met in order for the consent to be considered informed, the European Data Protection Board ("**EDPB**") issued specific guidelines[20] in this respect.

Footnote(s):

[20] Guidelines 05/2020 on consent under Regulation 2016/679, adopted by EDPB on 4 May 2020

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

As a general rule, the GDPR prohibits the processing of special categories of data, unless one of the circumstances under Article 9 paragraph (2) of the GDPR is met (along with a legal basis as per Article 6).

In addition, the Romanian Data Privacy Law stipulates some particular requirements for processing special categories of data or sensitive data, as follows:

i. the processing of genetic data, biometric data and data concerning health for the purpose of automated decision-making or profiling is only permitted based on two legal grounds, namely the explicit consent of the data subject or the existence of legal obligations in this regard, with appropriate measures in place for the protection of the rights, freedoms and legitimate interests of the data subject;
ii. the processing of the national identification number based on legitimate interest is only allowed if the following safeguards are implemented: (i) adequate technical and organizational measures to observe the data minimization principle and to ensure the security and confidentiality of personal data processing; (ii) appointment of a DPO; (iii) setting storage times according to the nature of the data and the purpose of processing, as well as specific deadlines by which personal data must be deleted; (iv) regular training of the persons who process personal data;
iii. processing of special categories of data (and generally of personal data) that is necessary for the performance of a task carried out in the public interest (in accordance with Article 6 para. (1) letter e)[21] and Article 9 para. (2) letter g)[22] of the GDPR) must be carried out provided that certain safeguards are applied, namely: (i) the implementation of adequate technical and organizational measures for the observance of the principles mentioned in Article 5 of the GDPR, in particular the data minimization principle and the integrity and confidentiality principle; (ii) the appointment of a DPO, if necessary; (iii) the establishment of retention periods according to the nature of the data and the purposes of processing, as well as specific deadlines by which personal data must be erased or revised for deletion;
iv. processing of special categories of data (and generally of personal data) by political parties, organizations of citizens belonging to national minorities and non-governmental organizations for achieving their objectives can be made without the express consent of the data subject, only if the following safeguards are implemented: (i) ensuring the proper information of data subjects about the processing, (ii) ensuring the transparency of the information, communications and ways of exercising the rights of the data subjects, (iii) guaranteeing the right to rectification and erasure.

In addition, once entered into force, the AI Act prohibits the use of specific AI tools, such as those designed for social scoring or real-time remote biometric identification in publicly accessible spaces. This anticipated prohibition on such tools will lead to additional limitations on the processing of sensitive personal data.

Footnote(s):

[21] processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

[22] processing is necessary for reasons of substantial public interest, pursuant to the Union or Member State law which shall be proportionate to the aim pursued, observe the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

9. How do the data protection laws in your jurisdiction address health data?

The Romanian Privacy Law includes specific provisions that address the processing of health data. Hence, the processing of data concerning health (alongside genetic data and biometric data) for the purpose of automated decision-making or profiling is only permitted based on two legal grounds, namely the explicit consent of the data subject or the existence of legal obligations in this regard, with appropriate measures in place for the protection of the rights, freedoms, and legitimate interests of the data subject. It should also be noted that the processing of health data carried out for the purpose of ensuring public health, as well as health and safety at work, cannot be carried out later, for other purposes, by third parties.

Additionally, patient confidentiality is a vital aspect of healthcare, and it is protected by the Patients' Rights Law no. 46/2003. All information related to a patient's condition, diagnosis, prognosis, treatment, and personal data is considered confidential, even after the patient's death. Disclosure of such health data requires either the patient's explicit consent or compliance with legal obligations. However, accredited healthcare providers involved in the patient's treatment may access this information without explicit consent.

Other provisions relating to health data are included in *Law no. 95/2006 on healthcare reform*, according to which healthcare units have the obligation to ensure the conditions for using medical information in electronic format through the patient's electronic health record system. Medical professionals can only access the information and data with the patient's explicit consent. However, there is an exception for the "Emergency Summary" module, which can be accessed without consent by healthcare professionals working in emergency structures or primary medical care, but only for the purpose of performing the medical act.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Other than the particularities already described, the Romanian Data Privacy Law also regulates the following:

i. Where electronic monitoring and/or video surveillance systems are used in the workplace, the processing of employees' personal data based on legitimate interest is only permitted if: (i) the legitimate interest is duly justified and prevails over the interests or rights and freedoms of the persons concerned, (ii) the employer has made a prior, complete and explicit notification to the employees, (iii) the employer has consulted the trade union or, as the case may be, the employees' representatives before the introduction of the monitoring systems, (iv) other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proved their effectiveness, (v) the storage period of personal data is proportional to the purpose of processing, but not more than 30 days, except for situations expressly regulated by the law or duly justified cases.
ii. Derogations from various chapters of the GDPR are also provided for the processing of personal data for journalistic purposes or the purposes of academic, artistic, or literary expression.
iii. Derogations from some provisions of the GDPR are provided for the processing of personal data for archiving purposes in the public interest, for scientific, historical research or statistical purposes.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please

describe how.

According to Article 8 of the GDPR, when consent is the legal basis for the processing of personal data in relation to the offer of information society services directly to a child, the processing of the child 's personal data shall be lawful where the child is at least 16 years old. Otherwise, if the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility.

Although it had the possibility to do so, Romania did not establish a lower age for these purposes, therefore the same requirements provided in Article 8 of the GDPR apply.

However, the requirement for a valid consent for the provision of information society services directly to a child are part of a legal framework that must be considered separately from the national contract law. In that respect, please note that the Romanian contract law provides that children below the age of 14 do not have legal capacity to contract (very limited exceptions are available) while children between 14 and 18 years have a limited legal capacity to contract. The data privacy age limitation provided under the GDPR must be applied so as to be consistent with the capacity to contract limitation provided under the civil rules.

Additionally, according to *Law No. 272/2004 on the protection and promotion of the rights of the child* ("**Law No. 272/2004**"), certain information concerning the child shall respect the principle of confidentiality and the provisions related to the disclosure of personal information. This includes: (i) information concerning the parent or other person(s) entitled to maintain personal relations with the child, and (ii) information relating to the child when transmitted by the person with whom the child lives, including photographs, medical assessments, school assessments, to the parent or other person(s) entitled to maintain personal contact with the child.

There are also specific provisions regulated by the *Audiovisual Law No. 504/2002*, according to which minors' personal data collected or generated by providers of video-sharing platforms, by whatever means, may not be processed for commercial purposes, such as direct marketing, profiling, and behavioural advertising.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

Although not data privacy laws per se, we note as follows:

Amendments have recently been made to the *Audiovisual Law No. 504/2002* introducing several rules to regulate legal issues arising from the technical progress in the field of audiovisual media services. For example, providers of video sharing platforms are required to safeguard minors and the general public by taking appropriate measures against harmful content, including pornography, violence, and materials inciting violence or hatred based on factors like race or religion. Additionally, they must inform users about commercial content and implement controls to restrict access to harmful material, such as age verification systems and parental controls.

If these requirements are not complied with, the National Audiovisual Council (which is the competent authority in the field of audiovisual communication) may request:

i. video sharing platform providers to remove or restrict access to illegal content or display a warning to users when accessing such content or disable the user's account for up to 12 months.
ii. service providers who provide storage space for video sharing platforms to remove, disable or restrict access to a video sharing platform.
iii. registry operators, which allocate domain names for video sharing platforms, to remove the domain name of the video sharing platform.

Romanian consumer legislation also sanctions manipulative practices used in the online environment that can influence consumers to take transactional decisions that may go against their best interests (i.e. false countdowns with deadlines for the purchase of specific products, concealment of information and misleading interfaces). More information on such practices have been addressed on the "*Behavioural study on unfair commercial practices in the digital environment*"[23] released by the European Commission in 2022.

Finally, *Law No. 217/2003 on preventing and combating domestic violence* ("**Law No. 217/2003**") regulates the concept of "cyber violence" into the sphere of "domestic violence" and defines the phenomenon by listing the acts that may fall under its scope[24]. However, it should be noted that this cyber violence will be punished only if it meets the criteria for domestic violence, occurring

within the family or domestic environment, or between spouses, former spouses, current, or former partners. If the cyber violence happens outside these contexts, the provisions of this specific law will not apply.

Footnote(s):

[23] Available at https://op.europa.eu/en/publication-detail/.

[24] "cyber violence" means online harassment, online messages inciting gender-based hatred, online stalking, online threats, non-consensual publication of intimate information and graphic content, unlawful access to intercept private communications and data, and any other form of misuse of information and communication technology through computers, smart mobile phones or other similar devices that use telecommunications or can connect to the internet and transmit and use social or email platforms, with the purpose of shaming, humiliating, frightening, threatening, silencing the victim.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

There is no special regulator with oversight of children's and teenagers' personal data, or online safety in general. However, according to Law No. 272/2004, parents bear primary responsibility for their child's upbringing and development, prioritizing the child's best interests. Local communities are also responsible for generally supporting parents and providing diverse, accessible, and quality services for children. State intervention complements this, ensuring child protection and upholding their rights through relevant institutions and authorities.

In consumer matters, the National Authority for Consumer Protection monitors compliance with the legal provisions on consumer protection, relating to products and services intended for the population in its area of competence, as well as the protection of their legitimate rights and economic interests, including in relation to consumers' online safety.

Last, but not least, the National Audiovisual Council has powers in what regards the providers of video sharing platforms, as further detailed above at Question 12.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

Once the AI Act is adopted and enters into force across the EU, deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated. This transparency obligation shall not apply where the use is authorized by law to detect, prevent, investigate, or prosecute criminal offence.

Furthermore, at national level, there is also a *Draft Law on the responsible use of technology in the context of the deepfake phenomenon* (the "**Deepfake Law Draft**" – as first pointed out in Question 2), which defines "deepfake" as any forged image, audio and/or video content made, usually using AI, virtual reality (VR), augmented reality (AR) or other means, so as to create the appearance that a person has said or done things to which that person has not consented, which in reality were not said or done by that person.

However, the Deepfake Law Draft currently in discussion does not prohibit the creation or distribution of artificial intelligence material but requires that deepfake material be accompanied by the message "*This material contains imaginary poses*".

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

There are no particular requirements imposed by the Romanian legislation regarding the implementation of "*data protection by design*" or "*data protection by default*" principles. However, in its *Guidelines on the application of the GDPR by controllers*[25], the NSAPDP drew attention to the importance of such a principle being addressed under the internal procedures of a data controller.

Footnote(s):

[25] https://www.dataprotection.ro/servlet/ViewDocument?id=1425

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

According to Article 30 of the GDPR, each data controller shall maintain a record of processing activities under its responsibility and each data processor shall maintain a record of all categories of processing activities carried out on behalf of a controller. The record must be kept in writing, including in electronic format (which is usually how the businesses keep it).

This obligation is applicable to data controllers and data processors employing more than 250 people, as well as in those cases in which fewer people are employed, but the processing is either (i) likely to result in a risk to the rights and freedoms of data subjects, (ii) not occasional (which presumably covers most of the entities considering that, generally, when conducting business, data processing is rarely occasional), or (iii) includes special categories of data, as referred to in Article 9 para. (1) of the GDPR or personal data relating to criminal convictions and offences, as referred to in Article 10 of the GDPR.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

As a matter of principle, there are no express requirements for data controllers to implement data retention and data disposal policies under the current Romanian legislative framework, but such an approach is strongly recommended, being necessary for ensuring that the data storage limitation principle is complied with, as well as for ensuring compliance with other obligations laid down in the GDPR[26].

As regards data retention, there are certain regulatory acts regulating specific areas of activity (such as archiving, tax, accounting, anti-money laundering, health, gambling) that impose a certain retention period. For example, the annual financial statements must be kept for 10 years, whereas the mandatory accounting records and the related supporting documents, including the employees' salary statements, must be kept for 5 years. Furthermore, the data permitting the identification of the donor and the beneficiary in case of collection and transplantation of organs, tissues and cells of human origin should be kept for 30 years *etc.*

The Romanian Privacy Law also provides for a 30-day maximum retention period in the case of employees' personal data where electronic monitoring and/or video surveillance systems are used in the workplace.

Footnote(s):

[26] This may include ensuring compliance with the accountability principle, providing information to data subjects under Article 13 or maintaining records of processing activities under Article 30 of the GDPR (which should in principle contain the deadlines for deleting different categories of data).

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

The consultation of NSAPDP is not binding under any national legal provision. The prior consultation obligations provided under article 36 GDPR apply.

On the other hand, the Cybersecurity Law regulates the possibility for entities to request assistance from NCSD in their identification process as OES, as well as regarding the documentation necessary for de-registration from the Registry of OES.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

Under the NSAPDP`s Decision no. 174/2018 regarding the list of processing operations that are subject to the requirement of data protection impact assessment ("**DPIA**") ("**Decision no. 174/2018**"), a DPIA is necessary in the following cases (the list being exemplificative):

a. processing of personal data in order to carry out a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly

affect the natural person;
b. large-scale processing of special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or personal data relating to criminal convictions and offenses;
c. processing of personal data for the purpose of systematic and large-scale monitoring of publicly accessible area, such as video surveillance in shopping centres, stadiums, markets, parks, or other such spaces.
d. large-scale processing of personal data of vulnerable persons, especially minors and employees, by automatic means of monitoring and/or systematic recording of people's behaviour, including for advertising, marketing, and publicity purposes.
e. large-scale processing of personal data by using innovative or by applying new technological solutions, particularly where such operations limit the ability of data subjects to exercise their rights, such as the use of facial recognition techniques to facilitate access to different spaces;
f. large-scale processing of personal data generated by sensing devices transmitting data through the Internet or by other means (the "Internet of Things" applications, such as smart TV, connected vehicles, smart metering, intelligent toys, intelligent cities or other such applications);
g. large-scale and/or systematic processing of traffic and/or location data of individuals (such as Wi-Fi monitoring, processing the geo-location of passengers in public transportation or other similar situations), when processing is not necessary in order to provide a service requested by the data subject.

As mentioned, the list of processing activities proposed by NSAPDP is not comprehensive. Therefore, even if certain processing activities are not included in this list, data controllers still need to make a case-by-case analysis of whether DPIAs are required for their processing operations.

This decision does not include any specific provisions on how the risk assessment should be conducted. Thus, the risk assessment should follow the DPIA Guidelines[27] adopted by Article 29 Working Party.

On the other hand, the Cybersecurity Law implements a risk assessment process for OSE, who must consider at least: (i) the new threats in the field of cybersecurity; (ii) recently discovered weaknesses; (iii) loss of effectiveness of security measures; (iv) changes in the risk situation caused by changes in the architecture of networks and IT systems; (v) any other changes in the risk situation. However, the risk assessment process for OSE does not directly relate to data processing activities, but to security of networks and IT systems.

Footnote(s):

[27] Guidelines on Data Protection Impact Assessment (DPIA) and for determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 adopted by Article 29 Working Party

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

The Romanian Data Privacy Law provides for the mandatory appointment of a DPO as per Articles 37-39 of the GDPR. In addition, the appointment of a DPO is mandatory (i) where national identification numbers are processed based on the data controller's legitimate interest (alongside other safeguards – *please see Question 8 point (ii) above*) and (ii) where the processing of personal data or special categories of personal data is conducted for the performance of a task carried out in the public interest (alongside other safeguards – *please see Question 8 point (iii) above*). The DPO's legal responsibilities are laid down in Article 39 of the GDPR.

The Romanian Cybersecurity Law requires OES and digital service providers ("**DSP**") to appoint a Chief Information Security Officer ("**CISO**") responsible for monitoring the permanent means of contact established by these entities. This obligation is based on the NIS Directive, which places a large part of the responsibility for the network and information systems security on OES and DSP.

Similar, the Cyber-defence Law established that the CISO appointed by the entities regulated by this law is responsible for:

a. establishing the policies, strategies and processes of cyber security risk management specific to the supply chain;
b. including in the content of existing policies,

strategies and processes of new and emerging requirements regarding the management of cyber risks specific to the supply chain;
c. establishing mandatory cyber security risk management standards for contracting authorities within procurement procedures;
d. establishing measures to stimulate potential suppliers within the procurement processes, relative to the level of implementation of their cyber security practices;
e. establishing the methodologies and applications used in the assessment of cyber security risks, specific to the supply chain;
f. exchanging information with other institutions regarding threats, risks and vulnerabilities of a cyber nature specific to the supply chain;
g. developing a methodology for evaluating the level of maturity and the capacity of supply chain operators to perform cyber security risk management;
h. collecting and updating data on the efficiency of suppliers in eliminating or reducing cyber security risks.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

Even though the GDPR does not expressly impose a separate obligation on controllers and processors to conduct internal training sessions concerning data protection rules for their employees, such training sessions are considered as an intrinsic part of the technical and organizational measures that controllers and processors are actually obliged to implement to ensure a level of security appropriate to the risk posed by the data processing activities, in accordance with Article 32 of the GDPR.

In view of the above, employee training can be considered, as a general rule, mandatory under the GDPR and the NSAPDP implemented this approach in practice and have already imposed sanctions on controllers and processors for lack or inefficiency of internal employee training. Furthermore, employee training is one of the corrective measures usually imposed by the NSAPDP after investigating security breaches or other irregularities in complying with the data protection requirements.

Moreover, Article 4 of the Romanian Data Privacy Law expressly provides for the need to conduct employee training where a national identification number is processed for the purpose of fulfilling the legitimate interests pursued by the controller or by a third party – *please see Question 8 point (ii) above*.

In addition, the Cyber-defence Law provides, *inter alia,* the obligation incumbent upon concerned entities to ensure the setting up and training of response teams to cyber security incidents and to ensure the training of personnel through regular performance of information, awareness raising and cyber hygiene campaigns at organization level.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

In addition to the requirements of properly informing data subjects as per Articles 12-14 of the GDPR,

i. the Romanian Data Privacy Law requires employers to inform their employees in a mandatory, complete, and explicit manner about the processing activities at the workplace involving monitoring systems, conducted on the basis of the employer`s legitimate interest;
ii. the Romanian e-Privacy Law requires providers of publicly available electronic communications services to inform the subscribers / users on the processing of traffic data and the duration of this processing where such processing (i) is pursued for subscribers' / users` invoicing or for setting out payment obligations or (ii) is carried out for the purpose of providing marketing services or higher-added-value services.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

The laws in Romania do not draw this type of distinction. Nevertheless, the general regime of data controllers and data processors set out under the GDPR applies entirely.

24. Do the data protection laws in your jurisdiction place obligations on processors

by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

The laws in Romania do not place obligations on processors by operation of law, nor do they require minimum terms with processors, except the mandatory contractual clauses set forth in Article 28 of the GDPR.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

The Romanian legislation does not impose additional restrictions regarding the appointment of a data processor, as long as the concerned data processor complies with the contractual requirements provided in Article 28 of the GDPR.

26. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these terms defined, and what restrictions on their use are imposed, if any?

The Romanian Data Privacy Law stipulates particular restrictions in what regards (i) processing of genetic, biometric or health data, for the purpose of automated decision-making or profiling – *please see Question 8 point (i) above*; (ii) monitoring systems at the workplace – *please see Question 10 point (i) above*.

Regarding tracking technologies (*i.e.* cookies), according to the Romanian e-Privacy Law, in order to store or access information that is being stored in the user`s terminal equipment, the following requirements must be met: (i) the user has expressly consented to such processing – the consent may also be given through the browsing application`s settings or by means of other similar technologies and (ii) prior to the consent, the user has been clearly and comprehensively informed, according to the data privacy legislation, in an easy and accessible manner, about the purpose of such processing.

In addition, if the electronic communication service provider allows third parties to store or access the information stored in a user`s terminal equipment, the user must be informed about the general purpose of the processing by third parties and about how to use the browsing application`s settings or other similar technology settings to erase such information or to deny access from third parties. EDPB issued specific guidelines[28] on the matter, conducting a technical analysis on the scope of application of Article 5(3) of the e-Privacy Directive, namely clarifying what is covered by the phrase "*to store information or to gain access to information stored in the terminal equipment of a subscriber or user*".

Footnote(s):

[28] Guidelines 2/2023 on Technical Scope of Art. 5(3) of e-Privacy Directive, adopted on 14 November 2023 by the EDPB.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

There are no definitions established in the relevant Romanian legislation for the specific concepts of "*targeted advertising*" and "*cross-contextual behavioural advertising*". Definitions of related concepts, together with more detailed views on behavioural advertising are provided in Opinion 2/2010 on online behavioural advertising[29], whereas the specifics of targeting are analysed in Guidelines 8/2020 on the targeting of social media users issued by the European Data Protection Board ("**EDPB**").

According to the latter, social media users may be targeted on the basis of *(i)* provided data – when the information is provided by the data subject (i.e., data subject indicate his/her age or e-mail in the description of the profile), *(ii)* observed data – when the data is provided by the data subject by virtue of using a service or device (i.e., the content shared by the data subject) or *(iii)* inferred data – when the data is created by the data controller on the basis of the data provided by the data subject or as observed by the controller (i.e., a social media provider might infer that an individual is likely to be interested in a certain activity or product on the basis of his/her web browsing behaviour). Furthermore, all these alternatives may be used individually, as well as in any combination.

Nevertheless, according to the newly enacted DSA, providers of online platforms shall not present advertisements to recipients of the service based on profiling, using special categories of personal data. Furthermore, providers of online platform shall not present advertisements on their interface based on

profiling, using personal data of the recipient of the service, when they are aware with reasonable certainty that the recipient of the service is a minor.

Finally, we refer to the provisions regulated by the *Audiovisual Law No. 504/2002*, related to minors' personal data, which may not be processed for commercial purposes, such as direct marketing, profiling, and behavioural advertising (please see Question 11).

Footnote(s):

[29] According to the Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010 by Article 29 Working Party, (i) "behavioural advertising" means advertising that is based on the observation of the behaviour of individuals over time, that seeks to study the characteristics of this behaviour through their actions in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests; (ii) "contextual advertising" means advertising that is selected based on the content currently being viewed by the data subject. The opinions also refers in several places to the concept of "targeted advertising" in correlation with cookie mechanisms.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

There are no specific rules addressing the sale of personal data under the Romanian privacy related legislation. General principles, requirements, and restrictions relevant to personal data processing are however correspondingly applicable[30].

As such, among others, the seller will need to have a legal basis to sell personal data and must ensure that the data subjects in question were properly informed about their data being collected for selling purposes (for example by including in their privacy notices the names of the organizations to which the data will be sold).

On another hand, if the selling was not one of the purposes for which the personal data was initially collected, then selling may be a possibility if *(i)* the seller obtains the consent from the data subjects for selling their personal data, *(ii)* the sale of personal data represents a legal obligation of the seller or *(iii)* the purpose compatibility test (as per Article 6 para. (4) of the GDPR) is conducted and concludes that the sale of personal data is compatible with the purpose(s) for which the personal data were initially collected.

At the same time the buyer, in all cases, after purchasing the personal data, as data controller, must also provide its own information notice to data subjects, in accordance with Article 14 of the GDPR.

Footnote(s):

[30] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-common-issues-might-come-up-in-practice/

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

The Romanian e-Privacy Law defines "*communications*" as "*any exchange or transmission of information between a determined number of participants, by the means of an electronic communication service for the public, without including the information transmitted to the public through an electronic communication network as part of an audio-visual program service, to the extent that no link can be established between that information and the identifiable subscriber or recipient user*".

While a specific definition for direct marketing does not exist, the definition given to "*commercial communication*" is considered applicable, as provided under Law no. 365/2002 on electronic commerce, namely "*any type of communication with the purpose to promote, directly or indirectly, the products, services, image, name, trademark or logo of a merchant or of a member of a regulated profession [...]*".

Article 12 of the Romanian e-Privacy Law forbids commercial communications by automated calling systems without human intervention, fax, electronic mail, except where the data subject gives his/her prior express consent. The law also establishes an exception from obtaining consent, by implementing a soft opt in mechanism if there was a previous commercial agreement between the data controller and the data subject.

In addition, any commercial communication that hides the identity of the person on behalf of whom such communication is made, or that prevents the user /

subscriber from requesting termination of such communications is forbidden.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

In addition to the GDPR provisions referring to "*biometric data*", the Romanian Data Privacy Law allows processing of biometric data for automated decision-making or profiling purposes if certain conditions are met – *please see Question 8 point (i) above*. In addition, as per NSAPDP's Decision no. 174/2018, large-scale processing of biometric data, as well as using facial recognition techniques to facilitate access to different spaces must be subject to a DPIA – *please see Question 19 points b) and e) above.*

On the other hand, the *Norms on the regulation, recognition, approval, or acceptance of the remote person identification procedure using video means*, approved by ADR Decision 564/2021, establish the minimum technical and security requirements for the remote person identification process using video means, as a form of "electronic identification", defined in the eIDAS Regulation[31].

In brief, prior to the development of a remote person identification procedure using video means, the identification service provider shall conduct a risk analysis, which shall cover risks related to the presentation of false identity documents, communication channels, and incorrect conservation of evidence. Also, prior to the start of the procedure, the individual who is subject to identification must expressly consent to the identification process, the purpose of the identification, the taking of photographs and/or images of himself/herself and of the identity document.

Separate, specifically in relation with law enforcement authorities, EDPB issued guidelines[32] on their use of facial recognition technology, also providing practical examples. Finally, it should also be noted that AI Act prohibits the use of real-time facial recognition (also known as "remote biometric identification[33]") in public places.

Footnote(s):

[31] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[32] Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 2.0, adopted by EDPB on 26 April 2023.

[33] According to AI Act, "*remote biometric identification system*" means an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database. Furthermore, "real-time remote biometric identification system" means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay and comprises not only instant identification, but also limited short delays in order to avoid circumvention.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

There are no specific laws in Romania addressing artificial intelligence or machine learning. Nevertheless, at European level, the AI Act was adopted on 13 March 2024 by the European Parliament. The AI Act shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union and be fully applicable in all Member States 24 months after its entry into force, with some exceptions.

32. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

General transfers of personal data outside the European Economic Area are permitted only under the conditions set forth in Chapter V (*Transfers of personal data to third countries or international organizations*) of the GDPR and do not require notification to, or authorization from, a regulator. Further details as provided by the EDPB in its guidance[34].

In addition, in Romania, transfers of data in the law enforcement sector are subject to the provisions of Law no. 363/2018. Specifically, according to article 43 of Law

no. 363/2018, as a rule, the Romanian competent authorities shall authorize the transfer of personal data to a third country or to an international organization, at the request of a competent authority of a Member State, only if the conditions laid down in the law are fulfilled. The authorization shall be promptly transmitted, but not later than 30 calendar days from the receipt of the request. The EDPB issued guidance for Member States in relation with the requirements for appropriate safeguards ensuring an essentially equivalent level of data protection within the framework of Article 37 ("*Transfers subject to appropriate safeguards*") of the Law Enforcement Directive.

Additionally, on 10 July 2023, the European Commission adopted its adequacy decision on the EU-US Data Privacy Framework[35], based on which personal data can flow freely from the EU to companies in the United States whose level of personal data protection is comparable to the EU.

Footnote(s):

[34] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, version 2.0, adopted on 14 February 2023 by EDPB.

[35] Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

By virtue of the direct effect of the GDPR, all the security obligations (*e.g.* under Article 25, 32 of the GDPR) are also applicable in Romania to data controllers and data processors. Also, the general obligations deriving from the Romanian e-Privacy Law are applicable.

In addition, the Romanian Cybersecurity Law stipulates that OES have, among others, the following obligations, which indirectly also apply to the protection of personal data:

i. to implement appropriate and proportionate technical and organizational measures for meeting the minimum-security requirements;
ii. to immediately notify the NCSD of incidents that have a significant impact on the continuity of essential services;
iii. to immediately ensure a response to the incidents that occur, to restore in the shortest time the operation of the service to the parameters they had before the incident and to perform the security audit, according to the Romanian Cybersecurity Law.

The Cyber-defence Law, beside the training obligations (mentioned at Question 21), provides that the relevant subjects (including certain private entities that provide public services or services of public interests and that own, organize, manage, or use informational networks or systems) must implement proactive and reactive measures, as follows:

a. establishment and operation of operational security centres;
b. establishing a reserve of cyber security resources and capabilities that can be used in case of necessity;
c. development of proactive capabilities, which allow anticipatory knowledge of threats from the cyberspace;
d. financing for the development of cyber security and defence capabilities, including from the perspective of research, development, innovation and digitization in the field and the assimilation of emerging technologies;
e. cooperation and exchange of information between the competent authorities and the private sector to identify cyber threats;
f. implementation of cyber security solutions, which increase the detection capacity and the prevention capabilities for cyber-attacks;
g. development of strategies, norms, policies, procedures, risk analyses, plans and technical control measures regarding cyber defence and security;
h. demonstration of the level of maturity reached by cyber security capabilities within the exercises organized at national or international level;
i. implementation of incident response and contingency plans in the field of cyber security;
j. use of the reserve of cyber security resources and capabilities;
k. restoring the functionality of networks and IT systems within the affected institutions;
l. disseminating information about cyber events through alerts in the inter-institutional environment for risk assessment and reducing the possibilities of exploiting vulnerabilities;
m. deterrence by publicly attributing the authors of cyber-attacks, according to legal

attributions;
n. implement cyber-security risk management procedures for the supply chain, which must cover specific topics;
o. designate a person responsible for cyber-security that must have specific attributions;
p. establish action plans for each type of cyber-security alerts.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

The Romanian Data Privacy Law does not provide a specific definition, therefore the provisions of GDPR in what regards "*personal data breach*" apply. According to the GDPR, a personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A similar definition is also provided under the Romanian e-Privacy Law.

On the other hand, the Romanian Cybersecurity Law provides a broad definition for a "*security breach*", meaning any event that has a real negative impact on the security of networks and information systems.

The Cyber-defence Law also provides several relevant definitions that can be correlated with a security breach:

i. cyber threat – any circumstance, event or potential action that could cause damage or disruption at the level of informational networks and systems, as well as at the level of users of such systems and other people or that may have another kind of negative impact on them.
ii. cyber security risk – the probability that a threat will materialize, exploiting a specific vulnerability of informational networks and systems.
iii. cyber crisis – a state of fact that represents a real threat or damage to a cyber infrastructure, likely to cause damage to informational networks and systems that provide essential, digital services or of national interest.
iv. cyber-attack – hostile action carried out in cyber space likely to affect cyber security.
v. cyber security incident – an event occurring in cyberspace that disrupts the operation of one or more informational networks and systems and whose consequences are likely to affect cyber security.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

The providers of public electronic communications networks or electronic communications services intended for the public have the following obligations, in accordance with the Romanian e-Privacy Law:

i. traffic data relating to subscribers and users processed and stored by the provider must be erased or made anonymous when they are no longer needed for the transmission of a communication, but not later than 3 years from the date of communication;
ii. the processing of location data is permitted only if the data in question is rendered anonymous or if the user has given his/her prior consent or if the service is for the unidirectional and undifferentiated transmission of information to users.

In addition, the said providers have the obligation not to change the identity of the caller, as well as not to hide and not to present to the called user the identity of the caller, without the latter's consent[36].

Also, with respect to entities that are deemed as OES or providers of digital services under the Romanian Cybersecurity Law, the *Technical norms on the minimum requirements for ensuring the security of computer networks and systems applicable to the operators of essential services*[37] shall apply. Also, for all the OES and DSP is applicable the list of European and international standards and specifications – LSSEINIS, which includes 80 procedures and policies issued by various entities, including the International Organization for Standardization, the European Telecommunications Standards Institute, the International Society for Automatization.

Footnote(s):

[36] According to Decision no. 70/2023 regarding the general authorization regime for the provision of electronic communications networks and services.

[37] Approved by Order no. 1323/2020

36. Under what circumstances must a

business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

The general provisions under Article 33 – 34 of the GDPR apply with regards to personal data breaches. The NSAPDP has a dedicated page[38] on its website in order to facilitate the online notification of a security breach. Also relevant for Romanian data controllers when assessing whether to notify the NSAPDP are the guidelines issued by the EDPB on this matter, namely the *Guidelines on personal data breach notification under Regulation 2016/679*[39] and the *Guidelines 01/2021 on examples regarding personal data breach notification*[40].

In addition, in relation to security breaches, based on the provisions of the Romanian Cybersecurity Law:

i. the OES must notify NCSD about each incident that has a significant impact on the continuity of the relevant essential services. Such notification must also be made where the incident adversely affects a provider of digital services upon which the provision of essential services depends.
ii. the DSP must notify NCSD about each incident that has a significant impact on the provision of the relevant digital services.

On the other hand, according to the Cyber-defence Law, a cybersecurity incident must be notified immediately, but no longer than 48 hours since becoming aware of the incident via the National Cyber Security Incident Reporting Platform.

We have not identified specific provision that require notifying the law enforcement authorities or criminal bodies about security breaches. However, the general provisions that regulate the obligations to inform the criminal bodies are applicable and they may cover, in certain cases, also actions or omissions that involve security breaches when such breaches amount to criminal offences. For instance,

i. According to Article 291 of the Romanian Criminal Procedure Code, any individual holding an executive position within a public administration authority or other public authorities, public institutions or public law legal entities, as well as any person vested with control prerogatives who, in the exercise of their prerogatives, became aware of the commission of a criminal offence in respect of which a criminal action is initiated *ex officio*, have the obligation to immediately notify the criminal investigation bodies and to take steps in order to make sure that the criminal offence traces, *corpus delicti* and any kind of evidence do not disappear.
ii. Article 12 of the *Government Emergency Ordinance no. 78/2016 for establishing and functioning of the Directorate for the Investigation of Organized Crime and Terrorism* provides that persons vested with managing or control prerogatives must inform about any data and information that reveal that a criminal offence has been committed. Further, the same persons have the obligation to protect and conserve the criminal offence traces, corpus delicti and any kind of evidence.

Footnote(s):

38 https://www.dataprotection.ro/formulare/formularBresaGdpr.do?action=view_action&newFormular=true

39 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_en

40 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

Law no. 161/2003 on certain measures to ensure transparency in the exercise of public dignity, public office and in the business environment, the prevention and sanctioning of corruption, as well as the Romanian Criminal Code regulate the prevention and fight against cybercrime through specific measures to prevent, detect and sanction crimes committed through computer systems, ensuring respect for human rights and protection of personal data.

However, there are no specific provisions on the

payment of ransoms and the general rules referred to above shall apply. Nevertheless, we mention that NCSD has repeatedly mentioned in its materials published on its website on the topic of ransomware, both general[41] and particular[42] (e.g., addressing specific ransomware attacks) that it "strongly recommends that no one pay ransom to the attackers".

Some of the materials[43] issued by NCSD point out several actions to be considered/ taken in order to prevent or manage a cyber-attack, such as:

i. limiting the use of Remote Desktop Protocol service on network stations and servers and taking additional measures to secure this type of service;
ii. using complex passwords and changing them periodically, enabling two-step authentication;
iii. making backups of critical data and storing it either offline or on a different segment of the network;
iv. isolating and retaining encrypted data in the event that an online decryption application could occurs;
v. scanning with a security solution installed on the device, or one available for free online, for suspicious links or attachments in the mailbox;
vi. reporting suspicious emails to the IT department for isolation and investigation;
vii. periodically checking the rules of the email account, which can be set for automatic forwarding all messages, which could lead to a data leak if there is a virus;
viii. using the lowest level of privileges required to perform actions/ operation, both for applications and users;
ix. emergency updating operating systems, antivirus software, web browsers, email customers and Office programs;
x. installing an application control solution that provides whitelist of applications and/or directories;
xi. regularly training the staff.

Footnote(s):

41
https://dnsc.ro/vezi/document/evaluare-asupra-evolutiilor-fenomenului-ransomware;
https://dnsc.ro/vezi/document/sfaturi-protectie-ransomware–mobil;

42
https://dnsc.ro/vezi/document/alerta-backmydata-ransomware-indicatori-de-compromitere-iocs;
https://dnsc.ro/vezi/document/alerta-backmydata-ransomware-pdf;

43
https://dnsc.ro/vezi/document/alert-backmydata-ransomware-eng-pdf;
https://dnsc.ro/vezi/document/evaluare-asupra-evolutiilor-fenomenului-ransomware;
https://dnsc.ro/vezi/document/ghid-protectie-ransomware

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

Yes, such regulator is NCSD, established as an independent structure for research, development, and expertise in the field of cyber-security and a specialized organization responsible for preventing, analysing, identifying, and reacting to cyber incidents. NCSD is responsible for developing and distributing public policies for the prevention of and counteracting to incidents that occur within the national cyber infrastructures and has the legal power to issue fines and to enforce certain provision under the Romanian Cybersecurity Law.

In addition, following the entry into force of Cyber-defence Law, the National Cyber Security System ("**NCSS**") was established as a general cooperation framework bringing together public authorities and institutions with responsibilities in the field of cyber security.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, any exceptions and any other relevant details.

The data subjects' rights provided under Chapter III (*Rights of the data subject*) of the GDPR apply, namely:

a. right on information regarding the processing of their personal data;
b. right of access;
c. right to rectification;
d. right to erasure;
e. right to restriction of processing;
f. right to data portability;
g. right to object;
h. right to not be subject to a decision based solely on automated processing, including

profiling, which produces legal effects concerning him or her or similarly significantly affects him or her;

i. right to withdraw consent at any time.

However, the Romanian Data Privacy Law provides certain exceptions from the applicability of such rights for specific processing operations or purposes, as follows:

i. *Derogation from all rights* – where data is processed for journalistic purposes or for academic, artistic, or literary expression, provided that it refers to personal data that was expressly made public by the data subject or which is strictly related to the data subject as a public person or the public character of facts that the person was involved in.
ii. *Derogation from the right of access, right to rectification, right to restriction of processing and right to object* – where personal data is processed for scientific or historical research purposes, insofar as such rights, by their nature, render impossible or seriously impair the achievement of the specific purposes and those derogations are required for the fulfilment of these purposes.
iii. *Derogation from the right of access, right to rectification, right to restriction of processing, right to data portability and right to object* – if personal data is processed for archiving purposes in the public interest, insofar as such rights, by their nature, render impossible or seriously impair the achievement of the specific purposes and those derogations are required for the fulfilment of these purposes.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

Both. Generally, the data subject should exercise his/her individual data privacy rights (as listed above at *Question 39* under letters a) through i)) by addressing a request in this regard to the data controller. If the data subject is dissatisfied with how the request was solved or did not receive a response from the controller within the legal term, he/she may submit a complaint to the NSAPDP or to the court, at their own choosing.

With respect to Romanian Cybersecurity Law, it provides for a notification of the NCSD where a person believes that an OES or DSP did not observe such law.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

The data subject has a private right of action, which includes two prerogatives, without any of them being conditioned by the other. On the one hand, the data subject has the right to lodge a complaint with NSAPDP, if the data subject considers that the processing of his/her personal data infringes the applicable legislation on data privacy (as per Article 77 of the GDPR). On the other hand, without prejudice to any available non-judicial or administrative remedy, including the right to lodge a complaint with NSAPDP, each data subject shall have the right to an effective judicial remedy before the courts of competent jurisdiction (as per Article 79 and 82 of the GDPR).

Romanian Cybersecurity Law provides only for the right to notify the NCSD, which, in turn, may commence an investigation against a certain OEP or DSP.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

Yes, individuals are entitled to monetary damages or compensation if they are affected by data privacy breaches, in accordance with Article 82 of the GDPR. The cybersecurity framework does not explicitly state a similar right of compensation in case of cybersecurity breaches.

However, under the general procedure rules regarding tort liability, any unlawful act that causes damage and is committed with fault (therefore, also a breach, as long as these conditions are met) can lead to the reparation of the damage (material and/or moral) by payment of compensation. Nevertheless, granting moral damage even when lacking a material damage may be differently interpreted in practice by courts of law on a case-by-case basis. In any case of damage (material or moral), the consequences of the breach must exist and be proven. In this context, we recall the decision of the European Court of Justice, granted in Case C-300/21[44], where the court settled that Article 82 of the GDPR:

i. must be interpreted as meaning that the mere infringement of the provisions of GDPR is not

sufficient to confer a right to compensation;
ii. must be interpreted as precluding a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached a certain degree of seriousness.
iii. must be interpreted as meaning that for the purposes of determining the amount of damages payable under the right to compensation enshrined in that article, national courts must apply the domestic rules of each Member State relating to the extent of financial compensation, provided that the principles of equivalence and effectiveness of EU law are complied with.

Footnote(s):

[44] Available at: https://curia.europa.eu/juris/document/.

43. How are data protection laws in your jurisdiction enforced?

The laws governing privacy and data protection are enforced through by NSAPDP and the courts of law. On another hand, the laws governing cybersecurity are enforced against private entities through by NCSD and the courts of law.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

The general sanctioning regime for breaches of the data privacy laws is the one provided by the GDPR, where the fines for failure to comply with its provisions may reach (a) up to 4% of the global annual turnover or (b) up to EUR 20,000,000, whichever is higher. However, the Romanian Data Privacy Law provides for a specific sanctioning regime applicable to public authorities and bodies, which have a different regime. Instead of the GDPR sanctioning regime, in case of violations, the Romanian public authorities and bodies firstly receive a warning and a remediation plan and only afterwards, if they do not fulfil the remediation plan, can they be subject to a fine of up to approx. EUR 40,000. So far, in Romania, the maximum penalty for breaches of the data privacy legislation has amounted to EUR 150,000 (issued against a banking institution).

On the other hand, if a violation specifically falls under the provisions of the Romanian e-Privacy Law, the sanctions amount from EUR 1,000 to 2% of the annual turnover of the company in breach, whereas if they fall under the provisions of the Romanian Cybersecurity Law, the sanctions may reach up to 2% of the annual turnover and even 5% of the total turnover, in case of repeated breaches.

As regards Romanian Cybersecurity Law, non-compliance is sanctioned by fines between approximately EUR 600 and EUR 10,000, and in case of repeated breaches, the maximum amount is up to EUR 20,000. For economic operators with an annual turnover higher than approx. EUR 400,000, the fines are increased, ranging between 0,5% and 2% of the annual turnover, and in the case of a repeated violation, the maximum fine shall be up to 5% of annual turnover.

In principle, the Cyber-defence Law provides for sanctions for non-compliance with the cyber incidents reporting obligation consisting of fines ranging between EUR 1,000 and 10,000 for certain misdemeanours regulated by the law, and in the case of a repeated violation within a six-month period, the maximum penalty shall be of up to EUR 40,000.For economic operators with an annual turnover higher than approx. EUR 200,000, the fine shall be up to 1% of the net turnover, and in the case of a repeated violation within a six-month period, the maximum fine shall be up to 3% of annual turnover. The consequences of a breach in terms of liability may, of course, be much broader in practice.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Regarding data privacy, the Romanian legislation does not provide such guidelines or rules; hence, the general provisions under Article 83 para. (1) – (3) of the GDPR are applicable. Moreover, the EDPB's *Guidelines on the calculation of administrative fines under the GDPR* [45] may be taken into consideration.

Regarding cybersecurity (both for the Romanian Cybersecurity Law and the Cyber-defence Law), in order to individualize the sanction, the NCSD will take into account the degree of the actual social danger, the period of time during which the legal obligation was violated, as well as, if applicable, the consequences of the violation.

Footnote(s):

[45] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-

administrative_en

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

Yes, based on the general legal provisions regulating the acts of public authorities, as well as based on NSAPDP's Decision no. 161/2018 on the approval of the procedure for conducting investigations. Therefore, one may file an appeal against the NSAPDP's record of findings / sanctioning and/or decision to apply corrective measures, as the case may be. The appeal shall be lodged with the administrative disputes section of the competent court, within 15 days from receiving it.

As regards the Romanian Cybersecurity Law and the Cyber-defence Law, these pieces of legislation provide a term of 30-days for challenging the decision issued by the NCSD.

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

By reference to the latest report published by the NSAPDP, namely the one for 2023[46], out of 548 investigations (derived from 4772 complaints and notifications), a total of 73 fines were applied, with a total amount of RON 2,348,265 (approximately EUR 470,000):

i. 67 fines were imposed based on the GDPR, amounting approx. EUR 449,000;
ii. 4 fines were imposed based on the Romanian e-Privacy Law, amounting approx. EUR 20,000;
iii. 2 fines were imposed based on the Romanian Data Privacy Law, amounting approx. EUR 4,000.

The main reasons for sanctioning were referring, in particular, to the following: (i) processing of personal data by infringing the provisions of Art. 5 (Principles relating to processing of personal data) and Art. 6 (Lawfulness of processing) of the GDPR; (ii) infringement of the data subjects' rights, in particular of the right of access and the right to erasure; (iii) failure to take corrective actions and provide the information requested by the NSAPDP.

In relation with security breaches, the main reasons for sanctioning concerned: (i) the infringement of security and confidentiality measures for the processing of personal data, given that the controllers did not adopt the appropriate technical and organizational measures regarding the security of the processing, including in the online environment following the poor configuration of the websites/computer applications used by the controllers; (ii) confidentiality/ availability/ integrity of the personal data affected especially following the unauthorized disclosure or following a ransomware informatic attack incident; (iii) the processing of images through the video surveillance systems, inclusively though mobile video surveillance means (body-cams); (iv) the publication/ disclosure of personal data in the online environment, especially on social platforms.

Footnote(s):

46 https://www.dataprotection.ro/?page=Materiale_informative&lang=ro

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

Currently, we have not identified any relevant proposals expressly reforming the data protection or cybersecurity legislation in Romania, other than the ones resulting from Question 2 above. However, due to the entry into force of the NIS 2 Directive on January 16th, 2023, future steps should be taken to transpose it into the national legislation.

Contributors

Lucian Bondoc
Managing Partner
lbondoc@bondoc-asociatii.ro

Monica Iancu
Partner
miancu@bondoc-asociatii.ro

Diana Savu
Managing Associate
dsavu@bondoc-asociatii.ro

Andra Gheorghe
Managing Associate
agheorghe@bondoc-asociatii.ro

Alexandru Daniliuc
Senior Associate
adaniliuc@bondoc-asociatii.ro