COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Romania

DATA PROTECTION & CYBER SECURITY LAW

Contributor

Bondoc si Asociatii SCA

Lucian Bondoc

Managing Partner | lbondoc@bondoc-asociatii.ro

Monica Iancu

Partner | miancu@bondoc-asociatii.ro

Diana Savu

Senior Associate | dsavu@bondoc-asociatii.ro

Andra Gheorghe

Senior Associate | agheorghe@bondoc-asociatii.ro

Alexandru Daniliuc

Associate | adaniliuc@bondoc-asociatii.ro

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

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

ROMANIA
DATA PROTECTION & CYBER SECURITY LAW

1. Please provide an overview of the legal and regulatory framework governing data protection and privacy 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). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

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:

- 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;
- 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;
- 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 Directive 2016/680[2] in the Romanian legislation;

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.*

While Romanian stakeholders are still getting acquainted to the compliance requirements imposed under the GDPR, certain changes in the data protection and privacy law landscape are still expected in the following years. The main piece of legislation that will bring significant amendments to the current legislative framework is the e-Privacy Regulation[3], currently going through the ordinary legislative procedure before the Council of the European Union, which 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 will also have consequences in terms of personal data processing and the protection of individuals' privacy, including the transposition into national legislation of the European Communication Code[4] and the adoption of the regulatory acts necessary for the effective implementation of the National Interoperability Framework[5].

As for cybersecurity matters, the main 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[6] 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 essential services operators, various technical norms and regulations *etc.* At European level, the NIS2 Directive[7] is due to replace the current NIS Directive, currently going through the ordinary legislative procedure before the Council of the European Union. Once adopted, the NIS2 Directive will have to be properly transposed into the Romanian legislation.

References

[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] 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)

[4] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code

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

[6] 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

[7] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

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

There are no registration or licensing requirements under 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 essential service operators (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 National Cyber Security Directorate ("**NCSD**") in order to be registered within the Registry of essential services operators.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

In Romania, the definition of „*personal data*" is the one provided under Article 4 para. (1) of the GDPR[1]. Also, the definition of „*special categories of personal data"* is the one provided under Article 9 para (1) of the GDPR[2].

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.*

References

[1] 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.

[2] 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

4. What are the principles related to, the general processing of personal data or PII – for example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction or must personal data or PII 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.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

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.

6. 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.

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

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)[1] and Article 9 para. (2) letter g)[2] 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.

References

[1] 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

[2] 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

8. How do the laws in your jurisdiction address children's personal data or PII?

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.

9. Does the law include any derogations, exclusions or limitations other than those already described? 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.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

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*, the NSAPDP drew attention to the importance of such a principle being addressed under the internal procedures of a data controller.

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

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.

12. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

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[1].

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, the employees' salary statements must be kept for 50 years, 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.

Reference

[1] 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).

13. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

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

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in 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. 174/2008**"), 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.

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[1] adopted by Article 29 Working Party.

Reference

[1] 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

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) 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 7 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 7 point (iii) above*). The DPO's legal responsibilities are laid down in Article 39 of the GDPR.

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

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.

Article 4 of the Romanian Data Privacy Law is the only one that 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 7 point (ii) above*.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (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.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

The general regime of data controllers and data processors set out under the GDPR applies entirely, including, but not limited to, the mandatory contractual clauses set forth in Article 28 of the GDPR.

19. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

The Romanian legislation does not require a minimum contract term, nor any 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.

20. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions 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 7 point (i) above*; (ii) monitoring systems at the workplace – *please see Question 9 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.

21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

There is no definition established in the relevant Romanian legislation for the specific concept of '*cross-contextual behavioral advertising'*. Definitions of related concepts, together with more detailed views on behavioral advertising are provided in Opinion 2/2010 on online behavioral advertising[1].

Although not expressly defined under GDPR or other applicable laws, there are certain restrictions imposed on such advertising practices, considering their particularities (*i.e.*, the fact that these are, almost invariably, carried out via automated processing of personal data or profiling). Article 22 para. (2) of the GDPR establishes an express general prohibition on decision-making based *solely* on automated processing, including profiling, which produces legal effects or similarly significantly affects data subjects. There are certain exceptions to this rule (including the explicit consent of the data subject), conditioned by appropriate measures that must be implemented to safeguard the data subjects' rights, freedoms and legitimate interests.

In addition, the Romanian e-Privacy Law sets forth that if cookies are used to implement behavioral or contextual advertising, such data processing is only permitted if the data subject gave his or her prior consent, after having been provided with clear and comprehensive information (as detailed under *Question 20 above).*

Reference

[1] 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.

22. Please describe any laws in your jurisdiction addressing the sale of personal information. How is "sale" or 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[1].

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). At the same time the buyer, 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.

Reference

[1] 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/

23. Please describe any 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.

24. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these 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 7 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 14 points b) and e) above.*

25. Is the transfer of personal data or PII outside the 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? Does a cross-border transfer of personal data or PII require 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.

In addition, in Romania, transfers of data in the law enforcement sector are subject to the provisions of Law no. 363/2018, which transposes Directive 2016/680. 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.

26. What security obligations are imposed on personal data or PII owners/controllers and on 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 the operators of essential services (as defined therein) 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.

27. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "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.

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

The Romanian Data Privacy Law provides some special security requirements with respect to certain processing operations, as follows:

i. In relation to the processing of a national identification number, the controller must apply adequate technical and organizational measures to observe, in particular, the principle of data minimization, as well as to ensure the security and confidentiality of personal data processing, alongside other safeguards – *please see Question 7 point (ii) above*;
ii. In the context or carrying out a task in the public interest, such processing is allowed provided that the controller or the third party has instituted adequate technical and organizational measures to observe the principles listed under Art. 5 of the GDPR, especially in terms of data minimization and the principle of integrity and confidentiality, alongside other safeguards – *please see Question 7 point (iii) above*.

Also, with respect to entities that are deemed as operators of essential services 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 shall apply.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice 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[1] 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 ANSPDCP are the guidelines issued by the European Data Protection Board ("**EDPB**") on this matter, namely the *Guidelines on personal data breach notification under Regulation 2016/679*[2] and the *Guidelines 01/2021 on examples regarding personal data breach notification*[3].

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

i. the operators of essential services 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 providers of digital services must notify NCSD about each incident that has a significant impact on the provision of the relevant digital services.

References

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

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

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

30. Does your jurisdiction have any specific legal requirement or guidance regarding

dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

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.

31. 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.

32. Do the 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 the rights, how they are exercised, what exceptions exist 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.

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

Generally, the data subject should exercise his/her individual data privacy rights (as listed above 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.

34. Does the law in your jurisdiction provide for a private right of action and, if so, in 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. 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.

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

Yes, individuals are entitled to monetary damages or compensation if they are affected by breaches of data privacy laws.

As a matter of law, under the general procedure rules, an individual may claim compensation based on breaches of data privacy laws even when lacking a material damage, a moral damage / injury of feelings sufficing. Nevertheless, this is a matter that may be differently interpreted in practice by courts of law on a case by case basis.

36. How are the laws governing privacy and data protection enforced?

The laws governing privacy and data protection are enforced through by NSAPDP and the courts of law.

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

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 fulfill 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), while the smallest fine totaled EUR 500. Numerous warnings have also been issued. As per a press release issued by the NSAPDP in January 2022[1], between May 25, 2018 and the end of December 2021, the fines imposed by the ANSPDCP amounted to a total of EUR 721,000.

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.

Reference

[1] https://www.dataprotection.ro/index.jsp?page=Comunicat_Presa_10_01_2022&lang=ro

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

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 application and setting of administrative fines*[1] may be taken into consideration.

Reference

[1] https://ec.europa.eu/newsroom/article29/items/611237/en

39. Can personal data or PII owners/controllers 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.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

We have not identified any relevant proposals expressly reforming the data protection or cybersecurity legislation in Romania.

Contributors

Lucian Bondoc
Managing Partner
lbondoc@bondoc-asociatii.ro

Monica Iancu
Partner
miancu@bondoc-asociatii.ro

Diana Savu
Senior Associate
dsavu@bondoc-asociatii.ro

Andra Gheorghe
Senior Associate
agheorghe@bondoc-asociatii.ro

Alexandru Daniliuc
Associate
adaniliuc@bondoc-asociatii.ro