industry. Scientists from all nationalities, and in any research area, may apply to FCT for funding' (https://www.fct.pt/apoios/index.phtml.en).

The FCT is obviously bounded to respect the applicable laws on data protection and even has a Data Protection Officer (https://www.fct.pt/dpo/index.phtml.en). I tried to contact the FCT and the Data Protection Officer about their duties on this regard but I did not receive any answer.

In any case, I suppose that FCT does not have autonomous functions regarding data protection. In their website they disclose the mechanism implemented by the FCT to comply with the GDPR and with the national applicable regulations:

i) Identification of a Data Protection Officer for the government area, under the responsibility of the General Secretariat for Education and Science;

ii) Creation of a communication channel, through the email address: protecao.dados@sc-geral.mec. pt.;

iii) Identification of Data Protection Officers in the governing bodies, including the FCT, the Directorate-General for Higher Education and the Directorate-General for Education and Science Statistics:

iv) Creation of a Personal Data Protection Unit within the General Secretariat of Education and Science, integrating the services, agencies, structures and entities of the governing area of Science, Technology and Higher Education.

v) Creation of a network of Data Protection Officers in the field of science, technology and higher education, including institutions of higher education, to share best practices, questions and doubts and to disseminate information:

vi) Conducting training and clarification sessions on the implementation of the RGPD coordinated from the General Secretariat of Education and Science:

vii) Creating support guides and best practices.

None of these measures involve the implementation of autonomous data protection procedures.

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

To our knowledge, there are no such regulations in Portuguese law.

23 Romania

Daniel-Mihail Șandru (Legal Research Institute "Acad. Andrei Rădulescu", Romanian Academy), Valentina Pavel (ApTI, Association for Technology and Internet)

23.1 Informed consent

23.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Law no. 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/servlet/ViewDocument?id=858	hard law	The establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing
Law no. 190/2018 on measures implementing the 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)	https://www.dataprotection.ro/servlet/ViewDocument?id=1520	hard law	Law implementing the General Data Protection Regulation
Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector		hard law	The processing of personal data and the protection of privacy in the electronic communications sector
Law no 284/2018 on the use of data from the register with passenger names in air transport for preventing, identifying, investigating and criminal prosecution of serious and terrorist offences, as well as for prevention and removal of threats to national security	http://legislatie.just.ro/Public/DetaliiDocumentAfis/208096 http://www.cdep.ro/pls/legis/legis_pck.htp_act?ida=154599	hard law	Transposition of the Directive 2016/681.

Law no 363/2018 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, detection, investigation, prosecution and fight against criminal offences or the execution of criminal penalties, education and security measures as well as on the free movement of such data	https://www.dataprotection.ro/servlet/ViewDocument?id=1620	hard law	Transposition of the Directive 2016
Law no. 362/2018 on ensuring a high level of security of network and information systems	http://legislatie.just.ro/Public/DetaliiDocument/209670	hard law	NIS Directive
Decision no. 128/2018 on the approval of the standard form for the personal data breach notification in accordance with 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)	https://www.dataprotection.ro/servlet/ViewDocument?id=1516	The Decision of the Authority for Personal Data Processing President	Notification of security breaches
Decision no. 133/2018 on the approval of the procedure for receiving and solving the complaints	https://www.dataprotection.ro/servlet/ViewDocument?id=1517	The Decision of the Authority for Personal Data Processing President	The procedure for receiving and solving the complaints
Decision no 161/2018 on the approval of the Procedure for conducting of investigations	https://www.dataprotection.ro/servlet/ViewDocument?id=1542	The Decision of the Authority for Personal Data Processing President	The procedure for conducting of investigations

Decision no 174/2018 on the list of the kind of processing operations which are subject to the requirement for a data protection impact assessment	https://www.dataprotection.ro/servlet/ViewDocument?id=1556	The Decision of the Authority for Personal Data Processing President	The list of operations for which it is compulsory to carry out the impact assessment on personal data protection

Main regulatory tools addressing data protection issues and informed consent in Romania

(i) The GDRP does not apply to purely personal or household activity. Is there any provision under national law for the protection of these data categories?

There are no specific provisions in the Romanian legislation regarding data protection for family or domestic purposes. Generally, the Civil Code provides the civil-law protection of dignity and privacy (Articles 70-77), emphasizing that "any processing of personal data, by automatic or non-automatic means, can be done only in the cases and conditions provided by the special law." Moreover, Article 75 of the Civil Code lists the facts that could constitute violations of privacy:

a) Unlawfully entering or staying in the house or taking any objects without the consent of the person who occupies it legally;

b) The unlawful interception of a private call, made by any technical means, or the informed use of such interception;

c) Capturing or using image or voice of a person being in a private space, without his/her consent;

d) Dissemination of images presenting interiors of a private space, without the consent of the person who occupies it legally;

e) Monitoring the private life, by any means, except for the cases expressly provided for by law;

f) Dissemination of news, debates, investigations or written or audio-visual reports on intimate, personal or family life, without the consent of the person concerned;

g) Dissemination of materials containing images regarding a person undergoing treatment in the healthcare units, as well as personal data on health status, diagnosis issues, prognosis, treatment, circumstances related to the disease and other various facts, including the result of the autopsy, without the consent of the person concerned, and if he/she is deceased, without the consent of the family or the persons entitled;

h) The use, in bad faith, of the name, image, voice or resemblance with another person;

i) Dissemination or use of correspondence, manuscripts or other personal documents, including address, residence and telephone numbers of a person or his/her family members, without the consent of the person these belong to or, as the case may be, has the right to dispose of them.

Some situations could amount to data protection violations. In the future, the case-law could contain a clear distinction between the breach of privacy (regulated by the Civil Code) and the violation of the protection of personal data regime (regulated mainly by

Regulation 2016/679), in view of the Court of Justice of the European Union case-law on Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

Specifically, the Civil Code protects the right to one's own image, according to which " In the exercise of the right to his/her own image, the natural person may prohibit or prevent reproduction, in any manner, of the physical appearance or his/her voice or, as the case may be, the use of such reproduction." (Article 73(2)). We have not identified relevant case-law to date.

There are some specific provisions aimed at establishing rules for the use of video cameras for guarding objectives and the use of surveillance cameras. On a sectoral basis, such regulations can contribute to increase the level of privacy protection because they are aimed at establishing standards. They also imply the necessity of obtaining administrative authorizations from those who want to set up and use video surveillance cameras. In this regard, see Law no. 333/2003 regarding the protection of objectives, goods, values and the safety of persons. In the same context, a soft law measure is the adoption of guidelines for homeowners associations using video surveillance (prior to the GDPR, instructions were issued by the National Supervisory Authority for Personal Data Processing the for homeowners associations).

(ii) The GDPR does not apply to national security. Is there any national regulation covering this topic (in terms of data protection issues)?

In the field of national security, the relevant legislation is Law no. 51/1991 regarding the national security of Romania[185], which sets out, at Article 13, regarding the personal data that the bodies with attributions in the field of national security: "capture certain operative moments by photographing, filming or by other technical means, or can make personal findings regarding public activities carried out in public places, if this activity is carried out occasionally; can request the data generated or processed by public electronic communications networks providers or electronic communications services providers intended for the public, other than their content, and retained by them according to the law; can carry out specific activities for the collection of information involving the restriction of the fundamental human rights or freedoms exercise, carried out in compliance with the legal provisions."

According to Article 14 of Law no 51/1991, the specific activities for the collection of information that imply the restriction of the fundamental human rights or freedoms exercise are performed only in certain situations and under the control of the judge. Some of these activities are directly related to personal data, such as:

- The interception and recording of electronic communications, carried out in any form;

- Searching for information or documents for which access to a place, to an object or opening an object are necessary;

- The installation of objects, their maintenance and removal from where they placed, supervision through photographing, filming or by other technical means or personal findings, systematically performed in public places or carried out in any manner in private places;

- Locating, tracking and obtaining information by GPS or other technical means of surveillance.

[185] Official Journal no. 190/2014.

There are no provisions specific to the data protection, and only general references to the limitation of the rights and freedoms of persons, judicial control in such cases and the potential information of the person subject to the limitation.

One of the personal data safeguards, namely the information security level, is ensured in the national security system activity by Law no. 182/2002 on the protection of classified information. This law allows a certain degree of lack of transparency regarding the data processing, because information contained in the classified documents is difficult to obtain by the data subject, insofar as the court does not declassify it.

On the other hand, Law no. 363/2018 implements EU Directive EU 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data.

Authority Name	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
National Supervisory Authority for Personal Data Processing **[Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal]** **https://www.dataprotection.ro/index.jsp?page=home&lang=en**	Yes, according to Article 1 from Law no. 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing[186]	No accurate information on the exact number of employees. In June 2018, there were under 50 employees, however, the total number of posts after implementing the GDPR was raised to 85.	Moderate. It does not issue opinions or guidelines There is a lack of transparency in applying sanctions as the decision is not fully published but the sanctioning activity and the presence in the court is quite high	In 2008 there were 4822 complaints and 200 referrals

Information regarding Data Protection Authority

[186] In theory, yes. In practice, the President is politically appointed. As the Association for Technology and Internet, a Romanian digital rights NGO, has reported in a recent complaint, there are strong concerns regarding the independence of the DPA. More information here: https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf

(iii) Does your national legislation introduce a specific definition of "data processing for research purposes"? Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

Article 8(1) of Law no. 190/2018 provides that "[t]he provisions of Articles 15, 16, 18 and 21 of the General Data Protection Regulation do not apply if personal data are processed for scientific or historical research purposes, to the extent that the rights mentioned in these Articles are likely to make it impossible or to seriously affect the achievement of the specific purposes, and the respective derogations are necessary for the fulfilment of these goals." Also, Law no. 363/2018 provides an exception from changing the data processing basis, in accordance with Article 5(1)(b) of GDPR. Relevant case-law on the application of the two above mentioned provisions was not identified.

A general definition for "research in public interest" does not exist, but there are regulations regarding the free access to information, and data protection is one of the limitations of this right of access (Law no. 544/2001).

(iv) Does your national legislation implement Article 89 of the GDPR, introducing in particular some specific safeguards to adopt in case of data processing for research purposes?

(v) Article 8 of Law no. 190/2018 refers to the safeguards in Article 89 of the GDPR, without introducing specific and more detailed provisions.

Article 9 (2) of Law no. 190/2018 allows the processing of all personal data, including special categories of data, without explicit consent, by political parties, organizations of citizens belonging to national minorities and non-governmental organizations.

The law does not specify which legal basis applies for such processing and it mentions the following as "safeguards":

1) that data subjects are informed that personal data processing is taking place, and

2) data subjects are shown the mechanisms through which they can exercise their rights to rectification and deletion (which would be mandatory anyway according to Articles 13 or 14 of the GDPR).

Additionally, the national implementation introduces specific cases for processing special categories of data described in the question below (see "Are there any special requirements regarding data processing at the national level?").

(vi) Does your national legislation provide specific cases and safeguards for processing sensitive data beyond article 9 of the GDPR? Which cases? Which safeguards?

Law no. 206/2004 on good conduct in scientific research, technological development and innovations, mentions in Article 12 that the ethical evaluation of research-development and innovation projects is performed by the evaluation committees and it is mandatory that the evaluation include checking the project against general ethical regalement on personal data protection.
Data confidentiality is a general rule for all employers who conclude employment contracts with natural persons (according to Article 16[1] of the Labour Code[2]). Separately from the conclusion of employment contract between the parties (employee and employer), a confidentiality contract may be concluded "regarding the information provided to the employee, prior to the conclusion of the individual employment contract" (Article 17(7) of the Labour Code). The confidentiality clause allows the parties to agree

that, throughout the duration of the individual employment contract and after its termination, they will not transmit data or information that they became aware of during the contract execution, under the conditions established in the internal regulations, in the collective labour contracts or in the individual employment contracts "(Article 26 of the Labour Code).

In the field of healthcare, we can mention Law no. 46/2003 on patient rights, as amended by Law no. 347/2018 (Official Journal no. 3/January 3rd, 2019): "The patient has the right to designate, by an agreement recorded in the annex to the general clinical observation sheet, a person who has full access, both during the patient's life and after the patient's death, to the confidential information in the observation sheet."

The patient's electronic health file is regulated by Law no. 95/2006 on healthcare reform. "The electronic health file contains clinical, biological, diagnostic and therapeutic data and information, personalized, accumulated throughout the patients' lives" (Article 346^{1}). Appropriate technical and organizational measures must be adopted to ensure an adequate level of data security and confidentiality, in accordance with the provisions of Article 32 of the General Regulation on data protection." (Art. 346^{5}) The principle of the free movement of data under GDPR conditions is also included.

We must also mention the confidentiality obligation stipulated in the law, as well as in certain documents. For example, there are several codes of medical ethics (for psychologists, pharmacists, general practitioners, dentists, etc.). The obligation of confidentiality is also covered by the Criminal Code, which incriminates in Article 227 the professional secrecy disclosure that harm the privacy of the individual.

In the field of education, the ministry in the field, through Law 1/2011, Article 94, letter w) "coordinates the collection and ensures the analysis and interpretation of statistical data for the national system of education indicators."

(vii) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

The National Authority for Personal Data Processing did not issue a Code of Ethics within the meaning of GDPR. However, some codes have been adopted at the level of the research and university institutions based on the Law of National Education no. 1/2011, Law no. 206/2004 on good conduct in scientific research, technological development and innovation, including its subsequent amendments and additions, and on the Law no. 319/2003 on the Statute of the research and development personnel. These laws do not contain express provisions on data protection, but there is a general principle, namely that of quality, based on international standards and good practices.

Also, there are Codes of Conduct adopted for notarial and law practice fields, by their corresponding supervisory unions.

(viii) Does your national legislation give specific definitions of data processing for "statistical purposes"? Are there specific rules that apply to such data processing?

The Romanian legislation does not provide definitions, but the Law no. 190/2018 regulates in Article 8 (above-mentioned) certain rules regarding the statistics field.

There are no specific regulations except Article 8 of Law no. 190/2018.

(ix) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

The Romanian legislation does not provide definitions, but the Law no. 190/2018 regulates in Article 8 (above-mentioned) certain rules regarding the statistics field.

There are no specific regulations except Article 8 of Law no. 190/2018.

23.1.2 Rights of data subjects and data processing

(i) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

There is no specific legislation

(ii) Are there any special requirements regarding informed consent at the national level?

There is no specific legislation

(iii) Are there any special requirements regarding data processing at the national level?

First, Article 3 of Law no. 190/2018 specifies that the processing of genetic data, of biometric data or of health data for the purpose of automated decision-making or profiling is permitted with the explicit consent of the data subject or if the processing is carried out under explicit legal provisions, with appropriate measures protecting the rights, freedoms and legitimate interests of the data subject. The law does not mention what are "appropriate measures".

Second, if national ID numbers are processed (national identification number, passport, driver's license, national health and social security number) the data controller is obliged to introduce the following safeguards specified in Article 4 (2):

a) implement appropriate technical and organizational measures for data minimization, and ensuring the security and confidentiality of personal data processing, in accordance with the provisions of Article 32 of the General Data Protection Regulation;

b) have a data protection officer, in accordance with the provisions of Article 10 of this law;

c) set retention periods according to the nature of the data and the purpose of the processing, as well as specific deadlines in which personal data must be erased or revised for deletion;

d) have regular training concerning the obligations of persons who, under the direct authority of the controller or processor, process personal data.

Third, in the case of electronic monitoring and/or video surveillance systems installed by employers, Article 5 of Law no. 190/2018 introduces specific criteria for meeting the legitimate interest requirement:

a) the legitimate interests pursued by the employer are duly justified and prevail over the interests or rights and freedoms of the data subjects;

b) the employer has carried out the mandatory, complete and explicit information of the employees;

c) the employer consulted the trade union or, as the case may be, the representatives of the employees before the implementation of the monitoring systems;

d) other less intrusive forms and ways to achieve the goal pursued by the employer have not proven their effectiveness before; and

e) the retention period of personal data is proportionate to the purpose of the processing, but not more than 30 days, except in cases expressly provided for by law or in cases duly justified.

Fourth, if the processing of personal data and of special categories of data is necessary for the performance of a task carried out in the public interest, the controller or third party need to implement the following safeguards:

a) implement adequate technical and organisational measures for data minimisation, and respect the integrity and confidentiality;

b) have a data protection officer, if this is necessary in accordance with Article 10 of Law no. 190/2018;

c) set retention periods according to the nature of the data and the purpose of the processing, as well as specific deadlines in which personal data must be erased or revised for deletion.

Fifth, Article 7 of Law no. 190/2018 introduces derogations for the processing of personal data for journalistic purposes. The provisions mention only three alternative scenarios under which personal data can be processed for journalistic purposes:

1) if it concerns personal data which was clearly made public by the data subject;

2) if the personal data is tightly connected to the data subject's quality as a public person; or

3) if the personal data is tightly connected to the public character of the acts in which the data subject is involved.

If either of these three situations applies, the GDPR (except for the Sanctions chapter) is entirely excluded from application.

(iv) Are there any special requirements to exercise data subject's rights (right of access, correction, deletion of personal data)?

There is no specific legislation.

23.1.3 Minors, sensitive data and other additional categories of data

(i) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

(ii) Are there any special rules when processing personal data of children? At what age can a minor provide consent according to your regulation?

There are no specific rules. The age is 16.

Article 41 of the Civil Code regulated the *limited exercise capacity.*

(1) The minor who has reached the age of 14 years has a limited exercised capacity.

(2) The legal acts of the minor with limited exercise capacity are concluded by him/her with the parent's, or, as applicable, legal guardian's consent, and in the cases provided by the law, with the trusteeship court's approval. The consent or approval may be provided when the document is concluded, at the latest.

(3) However, the minor with limited exercise capacity may conclude on his/her own preservation acts, management acts that do not affect him/her, as well as disposition acts with small value, current character, executed at the date of their conclusion.

(iii) Are there other vulnerable individuals identified in your national legislation?

No, they aren't.

23.1.4 Deceased individuals and personal data

(i) As recital 27 clarifies, the GDPR does not apply to deceased individuals. However, some countries provide people with the right to have all their personal data deleted once they pass away. Some others empower their close relatives to do the same. In some others, these data cannot be used at all without an explicit judicial mandate. What is the situation in your country?

The law implementing the GDPR does not include provisions around deceased individuals or close relatives of the deceased. However, the Civil Code introduces in Article 74 g) a provision mentioning that distributing materials with images of a deceased person without the permission of the family or of the rightful persons, is a violation of the right to private life. At the same time, Article 79 of the Civil Code specifies that the memory of the deceased person is protected in the same way as the image and reputation of a living person.

Finally, according to Article 21 of Law no. 46/2003 on the rights of the patients "all the information on the patient's condition, the results of the investigations, the diagnosis, the prognosis, the treatment, the personal data are confidential even after his/her death."

23.1.5 Accountability and Data Protection Impact Assessment

(i) Does your national regulation introduce further provisions related to general accountability? Any particular requirements? Any specific procedures?

There is no national specificity regarding DPIA, except the list of operations for which it is compulsory to carry out the impact assessment on the protection of personal data.

Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

Decision no. 174/2018 on the list of operations for which it is compulsory to carry out the impact assessment on the protection of personal data, Official Journal no. 919/October 31st, 2018 https://www.dataprotection.ro/servlet/ViewDocument?id=1556

Law no. 190/2019 introduces a discriminatory application regime in favour of public authorities. Under article 13, the Data Protection Authority must issue tailor-made "remedy plans" for public authorities engaged in data protection violations. Only if the public authorities do not comply with the DPA's remedy plan, then the DPA can issue fines of between 10 000 and 200 000 RON (approximately between 2 104 EUR and 42 091 EUR). This is a significantly low upper fine limit in comparison to the GDPR. Therefore, this creates a lack of practical application of the GDPR in the public sector.

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research

There are no specific procedures for data protection impact assessments and no reference to research.

23.2 Commercialization of data

23.2.1 General Regulatory Framework

There is not a specifics law regarding data commercialisation, it is governed by the general regime.

Regulation	Link	Type of regulation	Brief description and scope
Civil Code	http://legislatie.just.ro/Public/DetaliiDocument/109884 (Romanian)	Hard law	Provisions on sale contracts (art. 1650)

23.2.2 Practice

(i) In practice, does your country allow contracts based on exchange of personal data for services (for instance, to gain access to an app)?

There is no provision under national legislation that prohibits contracts based on exchange of personal data for services. However, the validity of such contracts would nevertheless depend on the compliance with the requirements of contract law. It is debatable whether such a provision would be qualified as a immorality clause or error.

(ii) Do you know if these practices are routinely performed?

No.

(iii) Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data?

No.

(iv) Do you have any particular national regulation on the secondary use of data?

Law no. 109/2007 (updated in 2015) on the re-use of public sector information is meant to encourage the development of new information products and services which can be used for commercial and non-commercial purposes.

(v) Do you have any specific protection for metadata or non-personal data in your country?

Romania implemented Directive 2007/2/EC establishing an infrastructure for spatial information in the European Community (Inspire) under national Law no. 190/2010 (which approves Government Ordinance no. 4/2010).

Article 12 (2) d) of Government Ordinance no. 4/2010 specifies that public authorities can limit public access to special data sets and complementing services or to electronic commerce services if the public access negatively affects the confidentiality of personal

data and/or files about a person, if the person did not consent to public sharing of information (where such confidentiality is covered by a national or European Union legislation).

At the same time, Article 12 (6) of Government Ordinance no. 4/2010 mentions that all public authorities forming the Council for National Infrastructure on Special Information (INIS Council) must respect national data protection regulation (the law has not been updated and it still mentions the previous law on personal data protection, Law no. 677/2001).

23.2.3 Nature of Data

(i) How does your country classify data? Is it a product/commodity/good or service? Do you have an additional construct for data?

There is no regulation classifying the data.

(ii) Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

The national copyright legislation does not protect data itself. There is no mechanism to determine the value of data.

23.3 Security and cybersecurity

23.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Criminal Code	http://legislatie.just.ro/Public/DetaliiDocumentAfis/210277 (Romanian)	Hard law	Contains provisions on the violation of private life
Law 161/2003 regarding certain measures for ensuring transparency of public dignitaries, public positions and within the business environment, corruption prevention and its sanction (updated)	http://legislatie.just.ro/Public/DetaliiDocument/43323 (Romanian)	Hard law	Title III of Law 161/2003 contains provisions on preventing and countering cybercrime
Law no. 64/2004 ratifying the	http://legislatie.just.ro/Public/DetaliiDo	Hard law	National law ratifying the Cybercrime Convention

Cybercrime Convention	cument/51288 (Romanian)		
Law no. 362/2018 concerning measures for a high common level of security of network and information systems	http://legislatie.just.ro/Public/DetaliiDocument/209670 (Romanian)	Hard law	National law implementing the NIS Directive 2016/1148
Law no. 535/2004 on preventing and countering terrorism	http://legislatie.just.ro/Public/DetaliiDocumentAfis/197775 (Romanian) The law was updated in 2019: http://legislatie.just.ro/Public/DetaliiDocument/212619 (Romanian)	Hard law	Includes provisions for setting up a Terrorism and Organised Crime Division.
Law no. 51/1991 on national security	http://legislatie.just.ro/Public/DetaliiDocument/1517 (Romanian) https://www.sri.ro/fisiere/legislation/Law_national-security.pdf (English)	Hard law	Contains provisions regarding interception
Government Decision no. 271/2013 for approving the Romania's Cyber Security Strategy and the National Action Plan on the implementation of the national cyber security system	https://cert.ro/vezi/document/strategia-de-securitate-cibernetica Romanian	Hard law	Romania's Cyber Security Strategy and the National Action Plan on the implementation of the national cyber security system
Government Decision no. 494/2011 on the establishment of the National Cyber Security Incident	https://cert.ro/vezi/document/hg-494-2011-infiintare-cert	Hard law	National Cyber Security Incident Response Center - CERT-RO CERT-RO is a public institution with legal personality, under the

Response Center - CERT-RO			coordination of the Ministry of Communications and the Information Society. It aims at preventing, analysing, identifying and responding to incidents within cyber infrastructures that provide functionalities of public utility or provide information society services.

Main regulatory tools addressing security and cybersecurity in Romania

23.3.2 Implementation of EU Law

(i) Are any particular procedures described in your national regulation?

No.

(ii) What is the status of the implementation of the NIS directive in your country towards data protection/security of data?

The NIS Directive was implemented in January 2019 by Law no. 362/2018[187].

Law no. 362/2018 implementing the NIS Directive mentions that in 6 months from entering into force of the law, the Romanian National Computer Security Incident Response Team (CERT RO) proposes to the Ministry of Communications the minimum technical measures for assuring the security of the network and information systems. Article 25 (3) of the law lists certain criteria for establishing the technical norms that essential service operators and digital service providers are obliged to comply with.

(iii) The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. Is this prevention reflected in your national regulation?

Law no. 362/2018 regulates the minimum-security requirements, and according to Article 25(1): "In order to ensure a common level of security of information networks and systems, the operators of essential services and digital service providers have the obligation to comply with the technical norms elaborated by CERT-RO, pursuant to provisions of Article 20, let. b.

(2) "CERT-RO elaborates, in consultation with the authorities that regulate the sectors and subsectors provided in the annex, guides to support the implementation of the minimum-security measures for operators and suppliers" mentioned in this law.

(3) The technical norms applicable to the essential services operators are established on the basis of at least the following categories of activities to ensure the security of the networks and information systems:

a) Management of access rights;

b) User awareness and training;

[187] For legislative history of the transposing law see http://www.cdep.ro/pls/proiecte/upl_pck.proiect?idp=17075

c) Logging and ensuring the traceability of activities within the networks and information systems;

d) Testing and assessing the security of computer networks and systems;

e) Management of computer networks and system configurations;

f) Ensuring the availability of the essential service and the operation of computer networks and systems;

g) Management of the continuity of the essential service operation;

h) Management of user identification and authentication;

i) Incident response;

j) Maintenance of computer networks and systems;

k) Management of external memory medium;

l) Ensuring the physical protection of computer networks and systems;

m) Carrying out security plans;

n) Ensuring the security of the personnel;

o) Risk analysis and assessment;

p) Ensuring the protection of products and services related to computer networks and systems;

q) Management of vulnerabilities and security alerts.

(4) The technical norms applicable to digital service providers are established on the basis of the following categories of activities to ensure the security of networks and information systems:

a) Security of systems and facilities;

b) Incident management;

c) Managing of the activity continuity;

d) Monitoring, auditing and testing;

e) Compliance with European and international standards.

(5) When implementing the measures in par. (1), the essential services providers:

a) Identify the computer networks and systems supporting the provision of essential services;

b) Elaborate and implement own security plans for computer networks and systems;

c) Ensure that incident management does not affect the security of computer networks and systems;

d) Prevent unauthorised access to computer networks and systems;

e) Prevent dissemination of data held in computer networks and systems by other persons than those authorised to know their content;

f) Implement a risk management system;

g) Implement action plans according to the security alert levels of computer networks and systems.

h) Ensure continuity of services.

(6) The technical norms provided in par. (1) are issued in compliance with the European and international standards and requirements, without imposing or discriminating for the use of a certain type of technology.

23.3.3 Personal Data Breach Notification

(i) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

Decision no. 128/2018 on the approval of the standard form for the personal data breach notification in accordance with 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)

Law no. 362/2018 regulates the notification of security incidents in Article 26.

Article 26

(1) The notifications made by the essential services operators, pursuant to Article 10, par. (1), let. c) must fulfil the conditions and contain the information provided in the technical norms set out in Article 20, let. c).

(2) The notifications made by the digital services providers, pursuant to the provisions of Article 12, par. (1), let. c), must fulfil the conditions and contain the information provided in the technical norms set out in Article 20, let. c).

(3) The incident notification contains, the following mandatory information:

a) The identification elements of the infrastructure and the operator or provider concerned;

b) Incident description;

c) The period of the incident;

d) The estimated impact of the incident;

e) Preliminary measures taken;

f) The list of state authorities affected by the incident;

g) The potential geographical extent of the incident;

h) Data on potential cross-border effects of the incident.

(4) The notification provided in para. (1) and (2) will not contain:

a) Classified information;

b) Data that may affect the rights and freedoms of citizens or the legitimate interests of third parties involved in the incident, according to the law.

23.3.4 Supervision of cybersecurity

(i) Does a supervisory body in a narrow sense with enforcement powers exist in your country?

There is no body with cybersecurity enforcement powers, as legislative proposals for adopting cybersecurity regulation have been either declared unconstitutional or stopped[188].

In 2013, Romania adopted the Cybersecurity Strategy which creates the National Cybersecurity System (SNSC). SNSC is the general cooperation framework among public institutions and authorities competent on security issues. The Operational Council for Cyber Security (COSC) is the body that ensures the unitary coordination of the SNSC[189]. The technical coordinator of COSC is the National Cyberint Center (CNC), inside the Romanian Intelligence Agency (SRI). CNC informs on an operational level on cybersecurity incidents which can affect the national security.

(ii) Is in your country an institution like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or something similar established? If yes, what are the competences and responsibilities?

There is no institution like the German BSI.

A similar organisation to a limited degree would be the Romanian National Computer Security Incident Response Team (CERT-RO). CERT-RO is an independent structure for research, development and expertise in the field of cybersecurity. It is a specialised organisation responsible for the prevention, analysis, identification and response to cybersecurity incidents. CERT-RO is responsible for elaborating and disseminating public policy on preventing and counteracting incidents in cyber infrastructures[190].

As a national CSIRT, CERT-RO has the following responsibilities:

a) Monitors the security incidents of the networks and information systems at national level;

b) Issues early warnings, alerts and announcements and disseminates information on risks and incidents to the managing authorities of the classified information, as well as any public or private law entity with potentially affected computer networks and systems security;

c) Receives notifications regarding incidents affecting the networks and systems of the essential service operators or digital service providers;

d) Provides to the essential services operator that made the notification, as far as possible, relevant information regarding the actions subsequent to the notification;

e) Establishes, based on the notifications received, the national and cross-border impact of the incidents and informs the relevant authorities at national level, as well as the similar authorities in other potentially affected states;

188 Romanian cybersecurity law reloaded, article available at https://edri.org/romanian-cybersecurity-law-reloaded/

189 National Cybersecurity Strategy 2013, available in Romanian at https://cert.ro/vezi/document/strategia-de-securitate-cibernetica

190 Decision 494/2011 on establishing the National Security Incident Response Centre, available in Romanian at https://cert.ro/vezi/document/hg-494-2011-infiintare-cert

f) Regularly provides to the public and whenever is necessary, warnings, alerts and information concerning risks and threats, possible measures to prevent and counteract them, in order to make the public aware and enabling them to take appropriate measures, and publishes statistics regarding incidents identified at national level, in compliance with the requirements of this law;

g) Ensures the response to incidents within the limits of this law;

h) Elaborates dynamic risk and incident analyses;

i) Cooperates, at national level, with CSIRT teams on an incident management platform for information exchange;

j) Participates in joint actions within the CSIRT network at European level, as well as, as needed, in the actions requested within the international cooperation networks;

k) May request the assistance of ENISA for carrying out its tasks;

l) Establishes, maintains and operates the alert and cooperation service with the essential service operators and service providers.

(3) In order to adequately manage major incidents at national level or to manage incidents that require high specialisation and specialised technical training, CERT-RO can develop partnerships and build joint teams composed of its own specialists and specialists from other institutions or entities from the private environment., in compliance with the law and ensuring the conditions regarding confidentiality and access to information within the law and with the consent of the parties involved in the incident.

(iii) How can damages caused by lack of cybersecurity be claimed (and compensated)? Are such issues sufficiently regulated in your country?

Damages can be claimed in court under the common procedure.

23.4 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment?

Law no. 362/2018 specifies that the actions constitute administrative offences or, taking into account their gravity criminal offences.

Criminal offences against personal freedom such as harassment (done by shrivelling a person's house or workplace, or by repeated phone calls or electronic communications) is punished by a few months imprisonment or by a fine.

Fraud related offences committed through computer systems or electronic payment means, as well as fraudulent financial operations are punished with imprisonment.

Violence of correspondence is punished either with imprisonment or a fine.

Computer data forgery is punished with imprisonment.

Access without a right to a computer system is punishable with imprisonment from 3 months to 3 years or a fine. More severe forms of illegal access to a computer system are punished only with imprisonment.

Illegal interception of computer data transmission is punished with imprisonment.

Offences such as altering computer data integrity, disruption of the functioning of computer systems, unauthorized computer data transfers are punished with imprisonment.

Illegal operations with devices or software are punished with imprisonment or a fine.

Accessing child pornography through computer systems or other means of electronic communication are punished with imprisonment from 3 months to 3 years or a fine. Producing, possessing for display or distribution, purchasing, storing, displaying, promoting, distributing and providing child pornography materials through electronic means is punished with 2-7 years of imprisonment.

Electronic vote fraud and forgery of documents and voting related records is punished by imprisonment.

(ii) Are there administrative fines related to data protection issues?

Law no. 190/2018 implementing the GDPR lists the administrative fines which are applied for lack of compliance (see Chapter VI on Corrective measures and sanctions, available in English).

Article 12: General provisions regarding corrective measures and sanctions

(1) Violation of the provisions listed in Article 83, para. (4) - (6) of the General Data Protection Regulation is a contravention.

(2) The main contravention sanctions are the warning and the contravention fine.

(3) Violation of the provisions of Articles 3-9 of this law constitutes a contravention and is sanctioned under the conditions provided in Article 83, par. (5) of the General Regulation on data protection.

(4) Finding the contraventions provided by the this law and applying the contravention sanctions, as well as the other corrective measures provided by Article 58 of the General Data Protection Regulation is made by the National Supervisory Authority, in accordance with the provisions of the General Data Protection Regulation, of Law no. 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for the Processing of Personal Data, including its subsequent amendments and additions, and of the this law.

Article 13 Application of corrective measures to public authorities and bodies

(1) If the violation of the provisions of the General Data Protection Regulation and this law is found in the case of public authorities/bodies, the National Supervisory Authority concludes a finding and sanctioning minute for the contravention, applying the sanction of warning and attaching a remediation plan.

(2) The term of remediation is established according to the risks associated with the processing, as well as the measures necessary to be fulfilled to ensure the conformity of the processing.

(3) Within 10 days from the expiration of the term of remediation, the National Supervisory Authority may resume control.

(4) The responsibility for carrying out the remedial measures lies with the public authority/body which, according to the law, bears the contraventional responsibility for the established facts.

(5) The model of the remediation plan that is annexed to the minutes of finding and sanctioning the contravention is provided in the Remedy Plan annex, which is an integral part of the present law.

Article 14: Finding contraventions and applying sanctions to public authorities and bodies

(1) If, following the control provided in Article 13, par. (3), the fact that the public authorities/bodies did not completely fulfil the measures provided in the remedy plan is found, the National Supervisory Authority, depending on the circumstances of each case, may apply the contravention sanction of fine, considering the criteria provided in Article 83, par. (2) of the General Data Protection Regulation.

(2) The violation made by the public authorities/bodies of the following provisions of the General Data Protection Regulation constitute a contravention:

a) The controller's or processor's obligations pursuant to the provisions of Article 8, Article 11, Articles 23-39, Articles 42 and 43;

b) The certification body's obligations pursuant to the provisions of Articles 42 and 43;

c) The monitoring body's obligations, Articles 41, par. (4);

(3) The violation made by the public authorities/bodies of the provisions of Articles 3-9 of this law is a contravention.

(4) The contraventions provided in para. (2) and (3) are sanctioned with a fine from LEI 10,000.00 up to LEI 100,000.00.

(5) The violation made by the public authorities/bodies of the following provisions of the General Data Protection Regulation constitute a contravention, concerning:

a) The fundamental principles for processing, including the conditions regarding consent, according to Article 5-7 and Article 9;

b) The rights of the data subjects according to Articles 12-22;

c) Transfers of personal data to a recipient from a third party country or international organisation, in accordance with Article 44-49;

d) Any obligations under the national legislation adopted under Chapter IX;

e) Failure to observe a decision or a temporary or definitive limitation on the processing or suspension of data flows, issued by the National Supervisory Authority pursuant to Article 58 par. (2), or failure to grant access, in violation of the provisions of Article 58 par. (1).

(6) By derogation from the provisions of Article 8, par. (2) let. a) of the Government Ordinance no. 2/2001 regarding the legal regime of contraventions, approved with modifications and completions by Law no. 180/2002, including its subsequent amendments and additions, the contraventions provided in par. (5) shall be sanctioned with a fine from LEI 10,000.00 lei up to LEI 200,000.00.

(7) The violation by the public authorities/bodies of a decision issued by the National Supervisory Authority pursuant to Article 58 par. (2) in conjunction with Article 83 par. (2) of the General Regulation on data protection.

(8) By derogation from the provisions of Article 8 par. (2) let. a) of the Government Ordinance no. 2/2001, including its subsequent amendments and additions, the contraventions provided in par. (7) shall be sanctioned with a fine from LEI 10,000.00 up to LEI 200,000.00.

In Law no. 362/2018, transposing the NIS Directive, 49 situations are regulated. The sanctions are provided in Article 39:

(1) The contraventions provided in Article 38 are sanctioned as follows:

a) With a fine from LEI 3,000.00 to LEI 50,000.00, and in case of repeated violations, the maximum limit of the fine is LEI 100,00.00;

b) By derogation from the provisions of Article 8 par. (2) let. a) of the Government Ordinance no. 2/2001 regarding the legal regime of contraventions, approved with modifications and completions by Law no. 180/2002, including its subsequent amendments and additions, for persons with a turnover of more than LEI 2,000,000.00, with a fine in the amount of 0.5% to 2% of the turnover, and, in the case of repeated violations, the maximum limit of the fine is 5% of the turnover.

(2) In order to individualize the sanction, CERT-RO will take into account the degree of concrete social danger of the act.

(iii) Do data protection offences constitute an official offence or are only prosecuted by the injured party's request?

The Criminal Code contains computer related offences which can be prosecuted with or without receiving a formal complaint.

23.5 Governance

(i) At least in the biomedical sciences research involving human participants usually is subject to ethical review by research ethics committees or similar bodies. Data protection, however, not only affects the biomedical sciences, but potentially all fields of research. Are you aware of any committees (e.g. research ethics committees, ethical review boards) or agencies (e.g. national research funding agencies, national security agencies) in your country that review data protection issues in research projects? If yes, are reviews mandatory and governed by specific guidelines or regulations? Do you know which aspects of data protection review bodies focus on? Are reviews only conducted before the actual research starts or is the research process monitored as well?

There are no specific bodies that review data protection issues in research projects, however, as mentioned above Law no. 206/2004 on good conduct in scientific research, technological development and innovations mentions that the evaluation of research projects must include checking the project against general ethical standards on personal data protection.

Universities are required to establish councils for ethics. For example, Babeș Bolyai University developed guides for ethical research which includes ethical issues around data protection[191].

[191] Babeș Boylai University, Ethical Research Guide, available in Romanian at https://cercetare.ubbcluj.ro/wp-content/uploads/2018/02/Ghid-AEC.pdf and University of Bucharest,

(ii) What instruments (e.g. ethics self-assessments at the proposal stage), if any, do research funding agencies and other research supporting bodies in your country use to promote data protection in ICT R&I? Do they facilitate the use of these instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

In the example of Babeș Bolyai University mentioned above, the guidelines warn against excessive data collection and advise to collect only what's strictly necessary. The guide also speaks about sensitive data, tracking and international transfer of data to third countries. An ethics approval needs to be obtained before the research starts. The guide mentions that data protection covers the processing operations all throughout the research, however it does not mention any monitoring during the research process[192].

As another example, University of Bucharest Code of Ethics includes a section on confidentiality and personal data protection. It specifies that the information needs to be stored securely and that if the study is made public it should contain only anonymised data[193].

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

Romania closely implemented Council Regulation no. 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology, modified by Council Regulation no. 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

Emergency Ordinance no. 129/2006 on export controls regime of dual-use goods and technology (approved by Law no. 136/2007) implements the Council Regulation no. 1334/2000[194].

Emergency Ordinance no. 158/1999 on the control regime of exports, imports and other operations with military goods[195] transposes Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfer of goods related to defence within the community. The body issuing export control certificates is the National Export Control Agency (ANCEX), functioning under the Ministry of Foreign Affairs.

Research Ethics Code, available in Romanian at https://cometc.unibuc.ro/wp-content/uploads/2018/10/Codul-de-etic%C4%83-a-cercet%C4%83rii-03.2017.pdf

192 Idem, Ethical Research Guide, p. 6-8

193 University of Bucharest, Research Ethics Code, available in Romanian at https://cometc.unibuc.ro/wp-content/uploads/2018/10/Codul-de-etic%C4%83-a-cercet%C4%83rii-03.2017.pdf

194 Emergency Ordinance no. 129/2006 on export controls regime of dual-use goods and technology, unofficial English translation available at http://www.ancex.ro/old_ancex/site_rom/legislatie/ORD%20129%20engl.pdf

195 Emergency Ordinance no. 158/1999 on the control regime of exports, imports and other operations with military goods, English translation available at http://www.ancex.ro/upload/OUG_158_republicata_2013_engleza_Cor.pdf