- the clinical trial number in the European clinical trials database (EudraCT);
- The names and addresses of the trial sites where the clinical trial is being performed;
- identification of the phase of the clinical trial;
- name of the investigational medicinal product;
- name of the active substance;
- number of clinical trial participants;
- characteristics of the groups of clinical trial participants;
- name, surname and place of residence or registered office of the sponsor;
- name, surname and title and degree of the investigator;
- name, surname and title and degree of the clinical trial coordinator, if involved;
- the date of notification of the clinical trial;
- date of the end of the clinical trial;
- clinical trial decision information;
- clinical trial number in the Central Register of Clinical Trials.

I am not aware of 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. However, as states above, according to the provisions of the Pharmaceutical Law Act, the President of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products exercises control over the conduct of clinical trials..

22 Portugal

Vera Lúcia Raposo (Macau University, University of Coimbra) Carla Barbosa (University of Coimbra)

Brief report on the implementation of the GDPR in Portugal

More than one year after the entry into force of the General Data Protection Regulation ("GDPR"), Law n. 58/2019 (hereafter, Law on Data Protection) was published on August 8, 2019, to ensure the implementation of the RGPD in the Portuguese legal order.

The delay in the transposition of the Regulation was due to delays in its drafting. Moreover, disagreements between the Government, the National Data Protection Commission (CNPD) and the members of the national Parliament created additional difficulties to the legislative process.

Law n. 58/2019 repealed the former law on personal data protection, Law n. 67/98 of 26 October, and amended the law on the organization and functioning of the National Data Protection Commission ("CNPD"), Law No. 43/2004 of 18 August.

Law n. 58/2019 contains some minor specifications of the GDPR. Among the various specificities of the Portuguese law, the most relevant relates with fines. According with the GDPR, in the most severe cases of non-compliance fines can reach up to 20 000 000 euros or 4% of the company's annual gross revenue in global terms from the preceding year,

whatever is higher (Article 83/5 of the GDPR). However, Law 58/2019 settled minimum limits for the fines (Articles 37 and 38 of Law 58/2019). For instance, for the most severe administrative offenses, the amounts start in the 5000 euros for the big companies, in the 2000 euros for small and medium-sized enterprises, and in 1000 euros for natural persons. In sum, fines are graded at three levels depending on whether it is a large company, an SME (small or medium company) or a natural person, though maintaining the maximum limits provided for in the GDPR.

The CNPD was from the very beginning very critical of this law. In line with its position, on September 3, 2019, the CNPD approved Deliberation 2019/494, which states the position of the CNPD regarding Law n. 58/2019.

The main content of this Deliberation can be summarised as such:

1. The CNPD believes that certain provisions of this law are manifestly incompatible with the law of the European Union. Therefore, it prepared this Deliberation to focus the provisions which, due to their relevance and frequency of application, give rise to an urgent common position about them and their significance.

2. Based on the principle of primacy of European Union law and in the remaining arguments set out in the Deliberation (exposed below), the CNPD announces that in the future it will disregard the referred provisions in cases referring data processing.

3. The provisions of Law n. 58/2019 in questions are:

(a) Article 2/1 and 2/2, where the scope of the Law is established. According to the CNPD, this rule jeopardizes the application of procedural rules and the distribution of powers among national supervisory authorities in what concerns cross-border treatments.

(b) Article 20/1, which restricts the rights of information and access in the event of a duty of secrecy against the data holder. The CNPD believes that its content goes beyond the limits that may be placed on the rights of information and access of the data holders, as provided for in the GDPR, and that legal limitations to the exercise of rights, in particular the exercise of a fundamental right such as the right of access, can never result from the content of a generic rule as Article 20/1.

(c) Article 23, which refers to the processing of personal data by public entities and the possibility of transferring data within public entities for different purposes than those that justified the collection of data. The CNPD considers that such a broad definition of public interest cannot supersede the data holders' rights and cannot be extended in such a way that it loses its inherent characterization. In addition, the CNPD considers that the article in question contravenes the purpose principle, as stated in Article 5 of the RGPD.

(d) Article 28/3/a, which stipulates that, unless otherwise provided by law, the worker's consent does not make the processing of his/her data lawful whenever the processing results in a legal or economic advantage for the worker. The CNPD considers that this is an excessively restrictive limitation of the workers' consent, which does not guarantee their dignity nor their fundamental rights.

(e) Article 37/1/a, which stipulates that the processing of data with intentional (dolus) non-compliance with the principles set out in Article 5 of the RGPD constitutes a very serious breach. The CNPD considers that the RGPD does not distinguish between intentional and negligent non-compliance with these principles, and thus all breaches, whether intentional or negligent, should be punishable.

(f) Articles 37/1/h and 38/1/b, where it is stated that the failure to provide information considered relevant under Articles 13 and 14 of the GDPR constitutes a serious breach, and that the failure to provide the remaining information referred in those norms constitutes a breach. The CNPD clarifies that the GDPR does not distinguishes between information considered relevant and non-relevant, and therefore all situations of failure to comply with the information duties provided for in Articles 13 and 14 of the GDPR should be punishable as very serious breaches;

(g) Article 37/1/k, which stipulates that the refusal to cooperate with the CNPD is a very serious offense, which is in contradiction with the GDPR, that states that this behaviour is a less serious administrative offense.

(h) Articles 37/2 and 38/2, which set different administrative offenses according to the size and legal nature of the agent. The CNPD considers that the GDPR makes no differentiation in this regard, so the Portuguese lawmaker cannot surpass the maximum ceiling for administrative offenses established by the GDPR.

(i) Article 39/1, which establishes criteria for setting the concrete amount of fines. The CNPD understands that these criteria go beyond the provisions of the GDPR.

(j) Article 39/3, which stipulates that, except in case of intent (dolus), the initiation of a proceeding for an administrative offense requires a prior warning to the agent. The CNPD believes that the provision of a special regime for negligent conducts is not compatible with the GDPR.

(k) Article 61/2 stipulates that when a contract is terminated because the data holder's consent has expired, the processing of data is lawful until such the termination takes place. The CNPD considers this rule incongruent because it confuses two types of legal basis, consent and contract enforcement. In fact, the contract to which the data subject is a party is sufficient to justify the processing of the data necessary for its performance.

(l) Article 62/2, which provides for the retroactive (from 25 May 2016) non-application of norms imposing authorizations of data processing by the CNPD or notifications of data processing to this same entity. The CNPD clarifies that the GDPR only became applicable on 25 May 2018.

This Deliberation demonstrates that Law n. 58/2019 was not well received by the CNPD and very likely its execution and compliance will face several challenges.

22.1 Informed consent

22.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Law 58/2019, from 8 August	https://dre.pt/web/guest/pesquisa/-/search/123815982/details/maximized (all in Portuguese)	Law (hard law)	It ensures the implementation, in the national legal order, of Council Regulation (EU) 2016/679

			Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of this data.
Law 59/2019, from 11 August	https://dre.pt/web/guest/pesquisa/-/search/123815983/details/maximized	Law (hard law)	Adopts the rules on the processing of personal data for the purpose of preventing, detecting, investigating or prosecuting criminal offenses, or for the execution of criminal sanctions, transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016
Law 12/2005, from 26 January	http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1660&tabela=leis		Personal genetic information and health information
Law 41/2004, from 18 August	http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=707&tabela=leis&so_miolo=		Personal data protection and privacy in telecommunications
Law 32/2008, from 17 July	https://www.ulisboa.pt/sites/ulisboa.pt/files/documents/files/lei672007_2v.pdf		Conservation of data generated or processed by electronic communication services
Law 5/2004, from 10 February	http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1439A0048&nid=1439&tabela=leis&pagina=1&ficha=1&nversao=		Law of electronic communications
Law 34/2013, from 16 May	https://dre.pt/pesquisa/-/search/261089/details/maximized		Establishes the regime for the exercise of private security activities and makes the first amendment to Law 49/2008 of 27 August (Criminal Investigation Organization Law)
Lei 1/2005, from 10th January	http://www.pgdlisboa.pt/leis/lei_mostra_articula		Regulates the use of camcorders by security

	do.php?nid=319&tabela=leis&so_miolo=		forces and security services in public places
Law-Decree 207/2005, from 19 November	http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=620&tabela=leis&ficha=1&pagina=1		Regulates road surveillance systems and treatment of information
Law 33/2007, from 13 August	https://dre.pt/pesquisa/-/search/636950/details/maximized?print_preview=print-preview		Regulates the installation and use of cab video surveillance systems
Law 109/2009, from 15 September	http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis		Cybercrime law
Law 2/94, from 19th February	https://dre.pt/pesquisa/-/search/516036/details/maximized	Law (hard law)	Establishes the control and surveillance mechanisms of the Schengen Information System

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

(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?

The fundamental right to privacy enshrined in article 26.º of the Constitution of the Portuguese Republic does not contain an exception for personal or household activities. It is however limited to personal data with a legitimate interest worthy of protection. Also Article 35 of the CRP establishing a right to informational self-determination.

From another point of view, we can also refer to the personality rights provided for in our Civil Code.

Even though the GDPR excludes purely personal and domestic activities, such activities are still submitted to the regulation of the Criminal Code, in particular Chapter VI (Articles 190 to 198), entitled "Crimes against the protection of private life". This chapter includes, among other provisions, the following norms, which are relevant for data privacy:

Article 192 (Intrusion in private life)

1 - Who, without consent and with the intention of intruding into the private life of others, namely the intimacy of family life or sexual life:

(a) Intercepts, photographs, films, uses, transmits or disseminates conversation, telephone communication, e-mail messages or detailed invoicing;

b) Captures, photographs, films, records or disseminates images of people or intimate objects or spaces;

(c) Observes or listens in secret people in a private place; or

(d) Discloses facts relating to the private life or serious illness of another person;

is punished with a prison term up to one year or a fine up to 240 days.

2- The fact provided for in subheading d) of the preceding paragraph is not punishable when practiced as an appropriate medium to achieve a legitimate and relevant public interest.

Article 193 (Invasion through computer)

1 - Anyone who creates, maintains or uses an automated file of individually identifiable data relating to political, religious or philosophical beliefs, to party or trade union membership, to private life or ethnic origin, shall be punished with imprisonment up to 2 years or with a fine up to 240 days.

2 - The attempt is punishable.

Note: The decision of Évora Court of Appeal of 05/11/2013 considered that this norm was revoked by the Law on the Private Data, now replaced by Law n. 58/2019.

Article 194 – Intrusion in correspondence or telecommunications

1 - Who, without consent, opens an package, letter or any other writing that is closed and is not addressed to him/her, or becomes aware, by technical processes, of its contents, or in any way prevents it from being received by the addressee, is punished with imprisonment up to 1 year or a fine up to 240 days.

2. The same penalty applies to anyone who, without consent, intrudes on or becomes aware of telecommunication content.

3 - Anyone who, without consent, discloses the contents of letters, orders, closed writings, or telecommunications referred to in the preceding paragraphs, shall be punished with imprisonment of up to 1 year or a fine of up to 240 days.

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

Indeed, the GDPR does not apply to national security matters, and based on this exclusion Law n. 58/2019 (Law on data protection) also does not apply. Moreover, Law n. 59/2009 (Law on data protection in criminal investigation) expressly excludes, in its Article 2/3, national security issues from its scope.

The Portuguese Criminal Code contains a crime intended to protect national security: Article 316 (violation of State secrets)

1 - Who, endangering the fundamental interests of the Portuguese State, transmits, makes accessible to unauthorized person, or makes public, in whole or in part, and regardless of the form of access, information, fact or document, plan or object classified as a secret which, in the name of those interests, must remain secret, is punished with a prison sentence of 2 to 8 years.

2 - Whoever destroys, subtracts or falsifies information, fact or document, plan or object as referred to in the previous number, endangering the interests therein indicated, is punished with imprisonment from 2 to 8 years.

3 - If the perpetrator commits a fact described in the preceding paragraphs in violation of a duty specifically imposed by the statute of his/her function or service, or the mission conferred upon him/her by a competent authority, the perpetrator is punished with imprisonment of 3 to 10 years.

4 - If the perpetrator commits the act described in paragraph 1 through means or in circumstances that facilitate its dissemination through the use of social media, digital platforms or platform of any other kind, he/she shall be punished with imprisonment of 3 to 10 years.

5 - If the perpetrator commits negligently the facts referred to in paragraphs 1 and 2, having access to the objects or secrets of the State by reason of his/her function or service, or the mission conferred upon him/her by a competent authority, he/she shall be punished with imprisonment up to 3.

6 - The fundamental interests of the State are those related to national independence, the unity and integrity of the State or its internal or external security, the preservation of constitutional institutions, as well as resources devoted to defence and diplomacy, the safeguard of population in national territory, the preservation and security of strategic economic and energetic resources and the preservation of the national scientific potential.

Name of Authority	Independent body?	Number employees[178]	Level of activity	Response to requirements, questions, etc. made by the public
Comissão Nacional de Proteção de Dados - National Data Protection Commission **https://www.cnpd.pt/english**	Yes[179]	The CNPD is composed by seven members: (a)The President and two members elected by the Parliament; (b) A judicial	Very active [180]	The CNPD answers frequently to queries and provides clarifications, an activity that was especially intensive in the months following the publication of the GDPR. Still according with its Report of Activities for 2017-2018, in the GDPR first month the CNPD received 1500 requests of clarification regarding its content. In addition to the attributions and powers that article 57 of the GDPR assigns to supervisory authorities, Article 6 of Law n. 58/2019 assigns to

[178] Numbers provided by the Report of Activities of the CNPD for 2017-2018, that can be found at https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201718.pdf.

[179] According to its website, "The CNPD is an independent body, with powers of authority throughout national territory. It is endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law".

[180] The CNPD is very active. One of the main reasons for being so productive is that in Portugal every single activity performed that in some way operates with private data required a previous authorization by the CNPD. According with the Report of Activities of the CNPD for 2017-2018, its activities can be classified in 5 main domains:

i) Decision-making activities;
ii) Advisory and advisory activities;
iii) Supervisory and sanctioning activities;
iv) Public awareness activities;
v) International activities;
vi) Internal management activities.

/index_en.htm		magistrate, with a career of more than 10 years, appointed by the Judiciary Superior Council; (c) A public prosecutor with more than 10 years of career, appointed by the Superior Council of the Public Prosecutor; (d) Two Government-appointed members; Besides the members of the CNPD, there are also 20 workers assisting their work		the CNPD the following additional tasks: i) To advise (it is a non-binding advise) on legislative and regulatory measures concerning the protection of personal data and about legal instruments in preparation at the European level or by international institutions on the same subject; ii) To supervise compliance with the provisions of the GDPR and other legal and regulatory provisions relating to the protection of personal data and the rights, freedoms and guarantees of the data subjects, and also about ways to rectify and sanction the non-compliance; iii) To provide a list of data protection impact assessment treatments in accordance with Article 35/4 of the GDPR and also to define criteria for the concept of "high risk" used in Article 35/1 of the GDPR; iv) To develop and submit to the European Data Protection Board a draft of the criteria to be used in the accreditation of certification bodies and bodies aimed to monitor codes of conduct; v) To cooperate with the Portuguese Institute of Accreditation, I.P. (IPAC, I.P.) regarding the accreditation of certification bodies in matters of data protection, as well as the definition of additional accreditation requirements in this area.

Information regarding Portugal Data Protection Authority

(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 31 of Law 58/2019 (Law on data protection) refers to data processing for archival purposes with public interest, for scientific or historical research purposes or for statistical purposes. However, there is no definition of the expression "data processing for research purposes". Likewise, there is no definition in the law of the concept "research in public interest".

However, for the processing of personal data for archiving purposes of public interest, Decree-Law no. 16/93 of 23 January, as amended, is applicable. Consent to the processing of data for scientific research purposes may cover various research areas or may be given only for certain specific research fields or projects, and in any case the ethical standards recognized by the scientific community must be respected. Without prejudice to the provisions of the National Statistical System Law, personal data processed for statistical purposes should be anonymized or pseudonymised, in order to safeguard the protection of data subjects, in particular as regards the impossibility of re-identification once the statistical operation is completed.

Decree-Law No. 63/2019 of 16 May 2019 estates that "research" is the set of knowledge production and dissemination activities as defined in the Frascati Manual of the Organization for Cooperation and Development. Economic, including research activities derived from scientific curiosity and practice-based, professional-oriented activities by referring data processing to specific legislation on the processing of personal data.

(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?

Article 31 of Law 58/2019 (Law on data protection) is the norm that intends to implement Article 89 of the GDPR.

Article 31/1 imposes anonymisation or pseudonymisation of the data to guarantee the protection of the data subjects, as longs as the aims envisaged with data processing can be achieved that way. This solution is similar to the one of Article 89/1 GDPR.

In the case of data processing for research purposes (but the same is valid for processing for archival purposes with public interest and for statistical purposes), the rights of access, rectification, limitation of treatment and opposition might be exempted insofar the exercise of those rights would render it impossible or seriously impair the achievement of the research aims. The limitation or exclusion of the referred rights shall be operated only in the measure required to achieve the aim purposed (article 31/2). This solution is very similar to the one stated in Article 89/2 of the GDPR.

Article 31/4 clarifies that the consent to the processing of data for scientific research purposes may cover various research areas or may be given only for specific research domains or projects, but, in any case, the ethical standards recognized by the scientific community shall be respected.

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

Law 58/2019 (Law on data protection) does not include specific provisions for sensitive data in general, but merely to genetic and health data: Article 29.

Article 29 starts by stipulating that in the processing of health and genetic data, access to personal data is governed by the principle of the need to know information (Article 29/1).

The norm imposes a special procedure in what regards the situations described in article 9/2/h and 9/2/1 of the GDPR, that is "for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to

contract with a health professional" (h) and "for reasons of public interest in the area of public health" (i). In those cases the processing of data shall be carried out by a professional bound by secrecy or by another person subject to a duty of confidentiality. In addition, appropriate security measures shall be ensured to protect the information (Article 29/2).

It is established that access to this type of data is made solely by electronic means, except in situations of technical impossibility or express indication of the data subject to act differently. It is forbidden its disclosure or further transmission (Article 29/3).

The norms imposes a duty of confidentially on the ones that have access to health and genetic data, such as people working for the data controller (office holders, workers and service providers), the data protection officer, students and researchers in the field of health and genetics, and all health professionals who had access to health data (Article 29/4).

This norms raises two doubts in what regards the ones to which the duty of confidentiality applies:

(a) The text of the norm only refers people working for the data controller, not the data processor. Are the workers of the later entity also bound to this duty?;

(b) The text of the norms only refers health professionals who had access to health data. Does the duty of confidentially include genetic data, not related with health, to which the health professional had access?

These two questions are particularly pertinent since Article 29/5 extends the duty of confidentiality to all office holders and workers who, in the context of monitoring, financing or supervision of the activity of health care, had access to health data. Therefore, it seems the duty is very inclusive, nonetheless, some players are not expressly mentioned in these provisions.

Article 29 declares that the data subject shall be notified of any access to his/her personal data. It's a task for the data controller to ensure that traceability and notification mechanisms are made available (Article 29/6).

The security measures and technical requirements for the processing of health and genetic data shall be approved by regulation issued by the members of the Government responsible for health and justice (Article 29/7).

There is, however, a regulation in Portugal jurisdiction which includes a specific norm about special categories of personal data: Law 59/2019, from 11 August (Law on data protection on criminal investigations). In its Article 6 it regulates the handling of special categories of personal data.

Article 6/1 refers the following categories of sensitive data: data revealing racial or ethnic origin, opinions, religious or philosophical beliefs or trade union affiliation, genetic data, biometric data intended to unambiguously identify a natural person, data about health or sexual orientation. It also states that the handling of these data shall be limited to the strictly necessary and subject to adequate safeguards to protect rights and freedoms of the data subject. Furthermore, the handling of these can only take place if one of the following situations verifies: (a) it is legally authorised; (b) it is aimed to protect the vital interests of the data subject or another natural person; (c) or the data at stake are related to other data manifestly made public by the data subject.

The definition of profiles that can lead to the discrimination of anyone based on the special categories of sensitive personal data referred above is prohibited by Article 6/2.

(vi) 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.)?

Article 15 of Law 58/2019 establishes that the National Commission for Data Protection is responsible for promoting the development of codes of conduct that regulate specific activities, and also that the processing of personal data by the direct and indirect administration of the State is subject to its own codes of conduct.

In Portugal many scientific institutions have their own Code of Conduct for Research, usually including some provisions regarding data collection and data processing. For instance:

- The Code of the University Institute of Lisbon determines that all data collected as part of an investigation shall be stored and maintained in a safe and accessible manner, for a period of at least five years since the end of the study/project or, if the data are reported in scientific publications, from the date of the original publication. During that time research data should be made available to those who intend to replicate the study, subject to possible limitations imposed by specific legislation and the general principles of confidentiality, protection and security of the participants. At the end of the storage period, the eventual disposal or destruction of data must be made in accordance with applicable ethical and legal requirements, with special consideration for the general principles of confidentiality, the protection of the ones and their safety.[181]
- The Code of the Interdisciplinary Centre of Education Studies[182] provides that any data collection requires a previous authorization from the National Commission for Data Protection. If the data are collected in a school, authorization from the General Direction of Education is also required. All information collected from research participants should be treated with confidentiality in such a way that identification is not possible. The information able to identify participants should be converted into anonymous data, fictitious names or anonymous identification codes. In research carried out within schools, hospitals, companies or other organizations, the institution should not be identified unless agreed by all parties. All data collected in the framework of the investigation should be stored in a secure place and made accessible for a minimum of five years counting from the study, or, if the data are reported in scientific publications, from the date of the original publication. Research data shall be made available to anyone who wants to replicate the study or work on the results to develop the existing knowledge. However, this possibility cannot, under any circumstances, call into question the principles of anonymity and data confidentiality, nor the rights of the participants in the study. At the end of the storage period, data must be deleted in accordance with the ethical principles of confidentiality, protection and security of the participants.

[181] Código de Conduta ISCTE-IUL 2016, at https://www.iscte-iul.pt/assets/files/2018/10/11/1539270104878_codigo_conduta_etica_na_investigacao_iscte_iul.pdf

[182] Código de Conduta Ética na Investigação do Centro Interdisciplinar de Estudos Educacionais, 2018, at https://www.eselx.ipl.pt/sites/default/files/media/2018/aprovado_codigo_etica_0.pdf

- The Code of Ethical Conduct of Minho University[183] provides that research shall be done guaranteeing the confidentiality of personal data and in compliance with the applicable legal regulations. In particular, it states that: "Confidentiality of the personal information collected during the research must be ensured. These data should not be retained for a period of time longer than necessary, in agreement with the opinion of the competent ethical body(ies) and or relevant laws and directives, after which time they are to be destroyed. Any information of a personal nature gathered during the course of the research shall be considered confidential and handled in compliance with rules concerning the protection of data and private life. Further safeguards should be taken into account when the research concerns vulnerable groups such as children, pregnant women, the elderly or persons with disabilities or infectious, contagious or oncological diseases. The information provided upon collection of the informed consent must be very clear regarding the confidentiality of the data and anonymity of the participants, but also about possible suffering and stress-related consequences for humans".

It should be noted that all these Codes refer to the previous regime on data privacy. Since Law 58/2019 was very recently enacted there was no time yet to create new Codes of Conduct.

We have no knowledge in any national Code of Conduct for data processing in research.

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

In Portugal there is no definition of data processing for "statistical purposes", nor specific rules in place.

However, Lei n 22/2008, from 13 May, de Law on the National Statistical System Law, provides in its article 2 some related definitions:

(a) 'official statistical activity': the set of methods, techniques and procedures used in the production and dissemination of official statistics;

(b) 'official statistics': statistical information produced usually within the implementation of the statistical program from the National Statistics System and the organizations Portugal is a member of, with due respect for technical standards and in accordance with the principles set out in this Law;

(c) 'individual statistical data': data that allow the direct identification of statistical units or that due to their characteristics (nature, structure, content, importance, number, relation to other data or degree of disaggregation) allow their indirect identification without involving a disproportionate effort and cost;

(d) 'anonymised individual statistical data': data modified in order to reduce the possibility of identifying the statistics units to which they refer without involving disproportionate effort and cost and in accordance with the best methodological practices;

[183] University of Minho Code of Ethical Conduct, July 2012, at https://www.uminho.pt/PT/uminho/Etica/Codigo-de-conduta-etica/Documents/Conduta_UMinho_V01.3.pdf

(e) 'administrative data': data that are collected by industry entities about natural or legal persons, including individual data related with administrative procedures that normally have a primary purpose that it is not statistical;

(f) 'statistical metadata': information describing the characteristics of series and statistical data, as well as the relevant concepts and methodologies involved in its production and use.

(viii) 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.)

Yes. The most relevant regulation in this regard is Law n. 21/2014, from 16 April (Law on Clinical Investigation), last amended in 2018 (therefore, before the Law 58/2019, but after the GRDP).

Article 6/1/c of the Law requires that the participants in clinical studies shall be informed about their privacy rights and about the protection guaranteed to their personal data.

According with Article 19/5, in studies funded directly or indirectly through public funds, the researcher or sponsor must make available to the competent ethical commission, a public version of the databases created in the clinical trial, as long as duly authorized by the CNPD and in compliance with the intellectual property rights of the sponsor and researcher, within three years of the end of the participation of the last participant in the clinical study

A database on clinical trials and clinical studies must be created by INFARMED, the national drug authority (article 38/1). The database might include personal data, that identify or make it possible to identify the data holder, but in that case proper justification regarding the need to include those data must be provided (article 38/2/h). The data included in the database might be made available to other entities that demonstrate to have a relevant interest in accessing those data, but guarantees of confidentiality must be observed at all time (article 38/3).

Article 51 refers specifically to guarantee of confidentiality. It states that the information transmitted under Law n. 21/2014 is confidential, and all who are aware of it are subject to the obligation of confidentiality. The duty of confidentiality does not prevent the disclosure of information necessary to safeguard public health, nor the fulfilment of the obligations of the competent authority regarding reciprocal information and the dissemination of warnings. Number 3 of article 51 clearly states that anyone who, in any capacity, intervenes in clinical studies or who is aware of its performance in any way, shall be bound by the duty of confidentiality regarding any personal data to which they have access, even after the end of their duties.

22.1.2 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.)

No, there are not.

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

No, there are not. The only specificity regards the consent of minors.

There is, however, a particularity regarding consent for the handling of personal data in the context of employment. Article 28/3 of Law n. 58/2019 (Law on data protection) establishes that the consent of the work is not required for data processing in two cases: (a) if the treatment results in a legal or economic advantage for the worker; or (b) if such treatment falls within the scope of Article 6/1/b of the RGPD, that is, if "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".

In its final and transitional provisions (Article 61/1), Law n. 58/2019 expressly states that in what regards data processing based on the consent of the data subject, in progress at the date of the entry into force of this law, it will not be necessary to obtain a new consent, as long as the one provided in the past has complied with the requirements of the GDPR.

Also in labour relations the law states that Unless otherwise provided by law, the consent of the worker shall not constitute a requirement for the legitimacy of the processing of his personal data: (a) if the processing results in a legal or economic advantage for the worker; or (b) if such treatment is covered by Article 6 (1) (b) of the GDPR (Article 28 (3)).

Finally, as regards the processing for archival purposes of public interest, scientific or historical research purposes or statistical purposes, Article 31 (4) provides that consent for the processing of data for scientific research purposes may cover several areas of research or be given only for specific domains or research projects, in any case the ethical standards recognized by the scientific community must be respected. This clearly includes an option for open consent, which facilitates the development of research.

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

National law shall apply to the processing of personal data carried out outside national territory when: (a) it is carried out in the course of the business of an establishment situated in national territory; or b) Affect data subjects that are in the national territory, when the processing activities are subject to the provisions of paragraph 2 of article 3 of the GDPR; or c) Affect data that is entered in consular posts held by Portuguese residents abroad. It does not apply to personal data files constituted and maintained under the responsibility of the Portuguese Republic Information System, which is governed by specific provisions under the law.

The processing of personal data by public authorities for purposes other than those determined by the collection is exceptional in nature and must be duly substantiated with a view to ensuring the pursuit of the public interest which may not otherwise be protected under paragraph (e). Article 6 (1), Article 9 (4) and Article 9 (2) (g) GDPR. The transmission of personal data between public entities for purposes other than those determined by the collection is exceptional in nature, must be duly substantiated in the terms referred to in the previous number and must be the object of a protocol that establishes the responsibilities of each intervening entity, either in the act of transmission, or other treatments to be carried out (Article 23).

The law also provides for legal provisions for the processing of personal data and freedom of expression and information (Article 24) for the processing of personal data and publications in the Official Journal (Article 25) for the processing of personal data. and administrative documents (Article 26), processing of personal data and publication of data in the context of public procurement (Article 27), industrial relations (Article 28) and

processing of health and genetic data (29). and 30) and treatments for public interest archiving, scientific or historical research purposes or statistical purposes (Article 31).

With regard to the processing of personal data for the purpose of preventing, detecting, investigating or prosecuting criminal offenses or the execution of criminal sanctions, transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 Law 59/2019 of 8 August in Chapter III defines the rights of data subjects.

This legislative decree stipulates that personal data collected by the competent authorities for the purposes set out in Article 1 may not be processed for different purposes unless such processing is authorized by law, in which case data processing for such and other purposes shall apply. The provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and of Law No 58/2019 of 8 August. Where the competent authorities carry out tasks for purposes other than those provided for in Article 1, the processing of data for such other purposes, including those of public interest archives, scientific or historical research or statistical purposes, shall apply. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Law 58/2019 of 8 August. If the competent authority transmits data the processing of which is subject to specific conditions, the transmitting authority shall inform the recipient of the personal data of those conditions and of the obligation to comply with them. When transmitting data to Eurojust, Europol and other bodies of judicial and police cooperation in criminal matters established within the framework of the European Union, as well as to the competent authorities of other Member States, no specific conditions other than those laid down for similar data transmissions between national authorities.

Law n. 58/2019 (Law on data protection) does not include a list of rights for the data holders. Therefore, in general the content and requirements of those rights are exactly the same as stated in the GDPR.

However, there are some exceptions:

(a) Regarding the right to data portability (Article 20 of the GDPR), Article 18 of Law n. 58/2019 clarifies that: i) The right to data portability covers only the data provided by their holders (n. 1); Data portability should, whenever possible, take place in open format (n. 2); Within the Public Administration, whenever data interoperability is not technically possible, the data subject has the right to require them to be delivered in an open digital format (n. 3);

(b) The exercise of the rights of information and access to personal data within the scope of the RGPD (Articles 13 to 15 of the GDPR) are limited when the controller or processor is legally bound by a duty of secrecy that is enforceable against the data subject himself. However, the data subject may request the CNPD to issue an opinion on the enforceability of confidentiality (Article 20 of Law 58/2019).

22.1.3 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)?

Law n. 58/2019 contains a norm - Article 29 - about the processing of health and genetic data.

According with Article 29/3, in the cases described in Articles 9/2/h ("processing is necessary for the purposes of preventive or occupational medicine, for the assessment of

the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3") and 9/2/I ("processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy") of the GDPR, access to the data is done solely by electronic means, unless it is technically impossible or expressly stated otherwise by the data subject.

There is also a duty to notify the data subject of any access made to his or her personal data, and the controller shall ensure the provision of such a traceability and notification mechanism (Article 29/6).

Finally, the processing of health and genetic data is subject to minimum safety measures and technical requirements that will be regulated by government ordinance (Article 29/7).

In addition, the Portuguese jurisdiction contains several regulations regarding categories considered by the GDPR as special data (Article 9 GDPR):

(a) Law n. 12/2005, of 26 January, on personal genetic information and health information;

(b) Law n. 5/2012, of 23 January, which regulates the requirements for personal data processing for the creation of nationwide files containing health data using information technology and within the framework of the National Health Service;

(c) Law n. 53/2017, of 14 of July, which creates and regulates the National Cancer Registry;

(d) Law n. 26/2016, of 22 August, which approves the regime for access to administrative and environmental information and for the reuse of documents, transposing Directive 2003/4 / EC of the European Parliament and of the Council of 28 January 2003 and Directive 2003/98/EC of the European Parliament and of the Council of 17 November.

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

According with Article 16/1 of Law 58/2019, from the age of 13 people are entitled to give their free, specific, informed and explicit consent, without the need of any other consent from the parents or other legal representative. This solution is different from the one stated in article 8 of the GRDP, which states the age of 16 years old, but it is still allowed under the final part of Article 8/1 of the GDPR.

In that regards minors with less f 13 years old, consent it to be provided by their legal representatives (Article 16/2).

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

The Portuguese law does not contain special provisions for other potentially vulnerable groups.

22.1.4 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?

In spite of the exclusion of data belonging to deceased individuals from the scope of protection of the GDPR, in Portugal Law n. 58/2019 provides legal protection to some of those data.

According with Article 17/1 of Law n. 58/2019, titled "Protection of personal data of deceased persons", some personal data of deceased persons are protected under the RGPD and the present law. The data under protection are:

(a) Special categories of personal data referred in Article 9/1 of the GDPR (that is, personal data revealing racial or ethnic origins, 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);

(b) Data related to intimacy, privacy, image;

(c) Data relating to communications.

However, if the situation falls under one of the cases described in Article 9/2 of the GDPR this protection does not apply.

Number 2 of article 17 clarifies that in what concerns the protection provided to the supra mentioned data, the rights involving those data, namely the rights of access, rectification and deletion, are exercised by whom the deceased person has designated for this purpose or, in their absence, by the heirs of the deceased. However, as stated in number 3 of Article 17, the data subject may also prevent the exercise the rights referred to in the preceding paragraph after their death, under the applicable legal terms.

Regulation concerning professional secrecy of state officials, doctors or lawyers stay in force.

22.1.5 Accountability and Data Protection Impact Assessment

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

The CNPD disseminates a list of data processing types for which prior impact assessment is not required. This does not prevent controllers from making a prior impact assessment on their own initiative (Article 7 of Law 58/2019).

In the case of the processing of personal data for the purpose of prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal sanctions, the controller shall take into account the nature, scope, context and purposes of the processing of data, as well as the risks to the rights, freedoms and guarantees of persons, shall take appropriate technical and organizational measures to ensure and be able to demonstrate that treatment is carried out in accordance with this law. These adopted measures are regularly evaluated and updated. The controller applies appropriate technical and organizational measures to ensure that only the personal data necessary for each specific processing purpose are processed. The controller assesses the volume of

personal data collected, the extent of processing, the retention period and accessibility and should ensure that by default personal data are not made available to an undetermined number of persons without the consent of the data subject. of the data. These measures are ensured both at the time of design, development and application of the means of treatment and at the time of the treatment itself, in order to allow, inter alia, pseudonymisation and minimization of data (Law 59/2019). Where a certain type of treatment is likely to pose a high risk to the rights, freedoms and guarantees of persons, the person responsible for the treatment must carry out an impact assessment of its component operations before commencing it. Taking into account the rights, freedoms and guarantees of persons, the impact assessment shall include: (a) a general description of the planned processing operations; (b) an assessment of the risks to the rights, freedoms and guarantees of data subjects; c) The measures envisaged to address the risks mentioned in the previous paragraph; d) Guarantees, security measures and mechanisms to ensure the protection of personal data and to demonstrate the compliance of the processing with this law. (Article 29 Law 59/2019). The controller or processor shall consult the supervisory authority before processing personal data to be incorporated into a file to be created where: (a) the impact assessment provided for in the previous article indicates that the processing would result in a high risk, in the absence of appropriate measures to mitigate this risk; or (b) the type of processing involves a high risk to the rights, freedoms and guarantees of data subjects, including the use of new technologies (Article 30 Law 59/2019).

(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?

Article 7 states that in order to comply with Article 35/5 of the GDPR, our national data authority (CNPD) will publish a list of types of data processing for which prior impact assessment is not mandatory (the inclusion on that list does not prevent the controllers from making a prior impact assessment on their own initiative). Article 7 does not refer that the CNPD will also prepare the list for which a prior impact assessment is required. This silence is especially strange since Article 7 also states, in its n. 3, that the lists referred to in paragraphs 4 and 5 of article 35 of the GDPR - that it, the list of types of data processing that do not require prior impact assessment, but also the list of the types of data processing that do require it - shall be published on the CNPD website.

This above-mentioned list was published in *Diário da República*, 2nd Series, through Regulation 1/2018, of November 30, 2018. It is a dynamic list, being updated whenever necessary, remembering that compliance with the obligation to carry out such an assessment does not exempt those responsible from fulfilling the other obligations provided for in the GDPR or in special legislation.

The following are subject to impact assessment:

1 - Processing of information arising from the use of electronic devices that transmit personal health-related data over communication networks; 2 - Interconnection of personal data or processing relating to personal data provided for in Article 9 (1) or GDPR 10 or highly personal data; 3 - Processing of personal data provided for in paragraph 1 of article 9 or article 10 of the GDPR or data of a highly personal nature based on indirect collection thereof, when it is not possible or feasible to ensure the right to information pursuant to Article 14 (5) (b) of the GDPR; 4 - Processing of personal data that implies or consists in the creation of large-scale profiles; 5 - Processing of personal data that allows tracking the location or behavior of their holders (e.g. workers, customers or just

passers-by), which has the effect of their evaluation or classification, except when processing is indispensable for the provision of services. specifically required by them; 6 - Processing of data provided for in Article 9 (1) or 10 of the GDPR or highly personal data for the purposes of public interest archiving, scientific and historical research or statistical purposes, except the treatment provided for and regulated by law providing adequate guarantees of the rights of holders; 7 - Processing of biometric data for the unambiguous identification of their holders when they are vulnerable persons, except for treatments provided for and regulated by law that have been preceded by a data protection impact assessment; 8 - Processing of genetic data of vulnerable persons, with the exception of statutory and statutory treatments that have been preceded by a data protection impact assessment. 9 - Processing of personal data as provided for in Article 9 (1) or 10 of the GDPR or highly personal data (11) using new technologies or re-using existing technologies.

22.2 Commercialization of data

22.2.1 General Regulatory Framework

There are no specific regulations on data commercialization. Article 22 of Law n. 58/2019 (Law on data protection) refers, *en passant*, the transference of data for non-EU countries, but only to state that these transactions are to be done in accordance with Article 49/4 of the GDPR.

Nonetheless, Decree-Law No. 446/85, of 25 October (with 5 amendments - the most recent DL No. 323/2001, of 17/12) General Contractual Clause[184], establishes the legal regime of the general contractual clauses which also contains regulations when Stipulations in the Terms of Service are inadmissible

22.2.2 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)?

No regulations specific for the contractual exchange of personal data as a payment for services exist. Based on national regulation, the arguments for illegality are sparse. The only reason coming to mind would be because of "unclear or incomprehensible" language in a contract between a consumer and a company (general contractual clauses). This would depend on the contract wording and cannot be determined without a concrete case.

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

Yes. Contracts as such are very common, especially in the field of telecommunications and insurance policies.

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

No general regulation for all kinds of data exist. Special regulations exist for artistic works data protected by copyright, for details see the answer to the next question.

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

[184] https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=837&tabela=leis

It is not directly about data but about samples but which eventually have associated data in the case of health, Law 12/2005 of 12 January (Personal Genetic Information and Health Information Act) in Article 19 no. 6 determines that In the case of retrospective use of samples or in special situations where the consent of the persons concerned cannot be obtained due to the amount of data or subjects, their age or other comparable reason, the material and data may be processed, but only for the purpose of scientific research or for obtaining epidemiological or statistical data.

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

It was published on 25 August 2017, the Organic Law No. 4/2017 that regulates the access by the Security Intelligence Service (SIS) and the Strategic Defence Information Service (SIED) to data of telecommunications and internet and will take effect on August 30, 2017.

Accordingly, these Information Services are now allowed access to identification, location and traffic data relating to users of electronic communications services for national defence, internal security and prevention of sabotage, espionage, terrorism, proliferation of weapons of mass destruction and highly organized crime.

However, access by the Information Services to such data is not unrestricted and subject to certain conditions, including prior and subsequent judicial review.

Inspection of the so-called Metadata Law by the Constitutional Court was requested, which in September 2019 declared the same as unconstitutional preventing the indiscriminate access of secret to communications records. The ruling states that the governing bodies have "the burden of rigorously and precisely setting out the criteria that may justify, under Article 3 of Organic Law No. 4/2017, access by public entities to base and location of citizens 'equipment'.

22.2.3 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?

In Portugal, there are only two categories of legal entities: things (*res*, which are the objects of legal relations) and persons (the subject of legal relations). According with article 202/1 of the Civil Code, every object of legal relations is considered a thing. Since personal data can be object of legal relations, they are considered things.

Data by itself is not classified in any legal category. Depending on the connection to a natural or legal person, it may fall under different legal regimes. For example, data constituting creative works by authors is protected by copyright and data pertaining to business secrets of companies are protected under the act against unfair competition. There is no overarching concept of what legal status data shall have by its own right.

(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?

According with Article 4/1 of Law Decree 122/2000, of 4 July, which transposes Directive 96/9/EC of the European Parliament and of the Council of 11 March on the legal protection of databases, databases can be considered a form of literary work when they constitute an intellectual creation. Therefore, databases are protected under de regime of author's rights.

In Portugal, the Code of Author's Rights protects intellectual property and copyrights. This protection covers, among other pieces of intellectual creation, also literary works (article 1/1 of the Code of Author's Rights).

22.3 Security and cybersecurity

22.3.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Law 46/2018, from 13 August	https://dre.pt/web/guest/home/-/dre/116029384/details/maximized?print_preview=print-preview	Hard law	Establishes the legal framework for cybersecurity, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, on measures to ensure a high common level of security for networks and information across the EU.
Law 109/2009, from 15 September	http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis	Hard law	Approves the Cybercrime Law, transposing the Council Framework Decision 2005/222 / JHA of 24 February on attacks against information systems, and adapts national law to the Cybercrime Convention of the Council of Europe
Resolution of the Council of Ministers no. 92/2019, from 23 May 2019	https://www.cncs.gov.pt/content/files/ensc_2019-2023_2.pdf	Soft law	Approved the national security strategy for cyberspace 2019-2023
Law 59/2019 of 8 August	https://dre.pt/web/guest/pesquisa/-/search/123815983/details/maximized	Hard Law	Rules on the processing of personal data for the purpose of preventing, detecting, investigating or prosecuting criminal offenses or the execution of criminal sanctions, transposing Parliament Directive (EU) 2016/680 European Parliament and of the Council of 27 April 2016

Main regulatory tools addressing security and cybersecurity in Portugal

22.3.2 Implementation of EU Law

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

No, there are not. Portugal follows the general EU procedures.

In the particular case of the GDPR, it is in force in Portugal (as in the remaining European Economic Area) since 25 May 2018. Law n. 58/2019 (Law on data protection) is merely an implementing law, by which the national legislator implemented and developed the content of the GDPR, and introduced some additional regulations regarding the rules resulting from the RGPD.

(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 by Law 46/2018, of 13 August, that establishes the legal framework for cybersecurity, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of network and information security across the Union (hereafter, Law on Cybersecurity).

(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 n. 58/2019 (Law on data protection) refer twice the need to implement technical and organizational measures in its Article 21:

(a) When it is not possible to determine in advance the time when it is no longer necessary the retention of data, data can be retained longer (this happens mostly in cases of processing for purposes of archiving of public interest, scientific or historical research purposes or statistical purposes), provided that appropriate technical and organizational measures are adopted to guarantee the rights of the data subject, in particular the information that data are still retained (Article 21/2);

(b) Data on contributory statements for retirement purposes may be retained without a time limit to assist the holder in re-establishing contributory careers, provided that appropriate technical and organizational measures are taken to guarantee the data subject's rights (Article 21/6).

However, the Law n. 58/2019 does not specify the technical and organizational measures to be implemented.

22.3.3 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?

Personal data breach notification is regulated in Law 46/2018 (Law o cybersecurity, implementing the NIS Directive). There are several notification procedures depending on the particular subject at stake.

(a) Notification of incident for Public Administration and Critical Infrastructure Operators (Article 15): This legal standard provides that the Public Administration and the operators of critical infrastructures shall notify the National Cybersecurity Centre of incidents with a relevant impact on the security of networks and information systems.

This notification shall include information enabling the National Cybersecurity Centre to determine the transboundary impact of the incident. It is clarified that notification does not entail additional responsibilities for the notifying party. Where the circumstances permit, the National Cybersecurity Centre shall provide the notifier with relevant information concerning the follow-up of his notification, including information that may contribute to the effective handling of the incident. The National Cybersecurity Centre, after consulting the notifier, may disclose specific incidents in the public interest, safeguarding the safety and interests of the operators of critical infrastructures.

(b) Incident notification by operators of essential services (Article 17): The service operator shall notify the National Cybersecurity Centre of incidents with a relevant impact on the continuity of the essential services they provide. The notification must include information enabling the National Cybersecurity Centre to determine the cross-border impact of incidents and it does not entail additional responsibilities for the notifying party. Based on the information provided in the notification, the National Cybersecurity Centre shall inform the single contact points of the other affected Member States when the incident has a major impact on the continuity of essential services in those Member States. The National Cybersecurity Centre shall safeguard the security and interests of the operator of essential services, as well as the confidentiality of the information provided in its notification. Where circumstances permit, the National Cybersecurity Centre shall provide the notifier with relevant information concerning the follow-up of its notification, including information that may contribute to the effective handling of the incident. It may disclose information regarding specific incidents in the public interest.

(c) Notification of incidents by digital service providers (Article 19): Digital service providers shall notify the National Cybersecurity Centre of incidents with a substantial impact on the provision of digital services (unless they are micro and small enterprises, which are excluded from this obligation). The obligation to notify an incident only applies if the digital service provider has access to the information necessary to assess the impact of an incident. The notification shall include the information necessary to allow the National Cybersecurity Centre to determine the importance of transboundary impacts. The notification does not entail additional responsibilities for the notifying party. If the incidents concern two or more Member States, the National Cybersecurity Centre shall inform the single contact points of the other affected Member States, however, still safeguarding the security and interests of the digital service provider.

(d) Voluntary incident notification (Article 20): any entity may voluntarily notify incidents of significant impact on the continuity of the services it provides. In any case, voluntary notification cannot impose to the notifying entity obligations to which it would not have been subject if it had not made such notification.

22.3.4 Supervision of cybersecurity

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

Law 46/2018 (Law on cybersecurity) establishes the National Cybersecurity Center, which is the National Cybersecurity Authority, operating under the National Security Office (Article 7 of Law 46/2018).

It performs different types of tasks: regulation, supervision, inspection and sanctioning, in accordance with the powers guaranteed to it by law. It has the power to issue cybersecurity instructions and to set the national cybersecurity alert level. In particular,

the National Cybersecurity Centre has powers to supervise and enforce the sanctions provided for in the above mentioned law (Article 21).

Nonetheless, National Cybersecurity Center, has no authority issue administrative fines for non-compliance.

(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?

Law 46/2018 (Law on cybersecurity) establishes an entity called High Cyberspace Security Council, which is the specific advisory body on cybersecurity matters (Articles 4 and 5). However, it does not have powers of control. Its functions are:

(a) To ensure political-strategic coordination for cyberspace security;

b) To verify the implementation of the National Cyberspace Security Strategy;

c) To emit opinions on the National Cyberspace Security Strategy prior to its submission for approval;

d) To prepare each year, or whenever necessary, an evaluation report on the implementation of the National Cyberspace Security Strategy;

e) To propose to the Prime Minister, or to the Government member with delegated powers, the approval of programmatic decisions related to the definition and execution of the National Cyberspace Security Strategy;

(f) To issue opinions on cyberspace security matters;

g) To respond to requests from the Prime Minister, or the Government member with delegated powers, within the scope of his powers.

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

The Law 46/2018 (Law on cybersecurity) does not contain any special regulation regarding compensation of damages due to cybersecurity breaches; therefore, the general legal regime for damages (contract liability or tort liability) provided by the Civil Code will be applied.

Express provisions referring compensation for damages are only to be found on the laws about data protection.

Article 33 of Law n. 58/2019 (Law on data protection) refers that anyone who has suffered damages due to unlawful processing of data or any other act that violates provisions of the GDPR or the national law on the protection of personal data, has the right to obtain compensation from the controller or processor. It also clarifies that the controller and the processor shall not be liable if they prove that the fact that caused the damage is not attributable to them.

Article 51 of Law n. 59/2019, which approves the rules on the processing of personal data for the purpose of prevention, detection, investigation or prosecution of criminal or

enforcement offenses sanctions, and that transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (hereafter Law on data protection in criminal investigations) establishes that anyone who suffered patrimonial or non-patrimonial damages caused by a violation of the provisions of the referred law is entitled to receive compensation from the controller or from any other competent authority, in accordance with the legal regime of governmental tort liability (and also from other public entities). However, this liability refers to the violation of any legal disposition of this law, not cybersecurity breaches.

22.4 Enforcement: fines and sanctions

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

National Law (Law 58/2019) created various legal types of crime related to the violation of personal data.

Article 46

Use of data incompatible with the purpose of collection

1 - Anyone who uses personal data in a manner incompatible with the purpose of the collection is punished with imprisonment of up to one year or a fine of up to 120 days.

2 - The penalty is doubled in its limits when dealing with the personal data referred to in articles 9 and 10 of the GDPR.

Article 47

Improper access

1 - Who, without due authorization or justification, access, in any way, personal data is punished with imprisonment up to 1 year or fine up to 120 days.

2 - The penalty is doubled in its limits when dealing with the personal data referred to in articles 9 and 10 of the GDPR.

3 - The penalty is also doubled in its limits when access:

(a) is achieved by violation of technical safety rules or

b) Has provided the agent or third parties with a benefit or asset advantage.

Article 48

Data Deviation

1 - Anyone who copies, subtracts, assigns or transfers, for consideration or free of charge, personal data without legal provision or consent, regardless of the purpose pursued, shall be punished with imprisonment of up to 1 year or a fine of up to 120 days.

2 - The penalty is doubled in its limits when dealing with the personal data referred to in articles 9 and 10 of the GDPR.

3 - The penalty is also doubled in its limits when access:

(a) is achieved by violation of technical safety rules or

b) Has provided the agent or third parties with a benefit or asset advantage.

Article 49

Data addiction or destruction

1 - Who, without proper authorization or justification, deletes, destroys, damages, conceals, deletes or modifies personal data, rendering it unusable or affecting its potential use, is punished with imprisonment up to 2 years or with fine up to 240 days.

2 - The penalty is doubled in its limits if the damage done is particularly serious.

3 - In the situations provided for in the preceding paragraphs, if the agent acts negligently he is punished with imprisonment:

(a) up to 1 year or a fine of up to 120 days in the case provided for in paragraph 1;

b) Up to 2 years or fine up to 240 days, in the case provided for in paragraph 2.

Article 50

Entering False Data

1 - Anyone who enters or facilitates the insertion of false personal data, with the intention of obtaining improper advantage for himself or others, or to cause harm, is punished with imprisonment of up to 2 years or a fine of up to 240 days.

2-the penalty is doubled in its limits if the insertion referred to in the preceding paragraph results in an actual damage.

Article 51

Violation of the duty of secrecy

1 - Who, obliged to professional secrecy under the law, without just cause and without due consent, to disclose or disclose in whole or in part personal data is punished with imprisonment up to 1 year or fine up to 120 days.

2 - The penalty is doubled in its limits if the agent:

a) Is a worker in public functions or equivalent, under the terms of criminal law;

b) Is in charge of data protection;

c) Is determined by the intention to obtain any equity advantage or other illegitimate benefit;

(d) endanger the reputation, honour or privacy of the privacy of others.

3 - Negligence is punishable by imprisonment of up to 6 months or a fine of up to 60 days.

Article 52

Disobedience

1 - Any person who fails to comply with the obligations set forth in the GDPR and this law, after exceeding the deadline set by the CNPD for the respective compliance, is punished with imprisonment up to 1 year or a fine of up to 120 days.

2 - The penalty is doubled in its limits if, after being notified, the agent:

(a) not interrupt, cease or block the unlawful processing of data;

b) Not to erase or destroy the data when legally required, or after the storage period established under the terms of this law; or

c) Refuse, without just cause, the collaboration required under the terms of article 8 of this law.

Mere attempt is punishable (Article 53). Legal persons and similar entities, with the exception of the State, of legal persons exercising their powers of public authority and of organizations governed by public international law, shall be liable for the crimes provided for in this Section, in accordance with Article 11 of the Penal Code.

In a first approach there seems to be an overlap between some of the criminal provisions referred in the referred two laws of 2019 and the ones included in Law n. 109/2009 (the Cybercrime law), and also with article 193 of the Portuguese Criminal Code, that establishes the crime of intrusion in private life by using a computer. In what regards conflicts involving norms from the two 2019 laws it is still very early to reach any conclusion (there is no caselaw in this regard, there are no academic studies). In what concerns article 193 of the Criminal Code, it has been arguing that this crime was replaces by the criminal provisions of the former law on data protection, Law n. 67/98, from 26 October (see the decision of the Évora Court of Appeal, process n. 679/05.7TAEVR.E2, decision from 5 November 2013). Therefore, it can be understood that the same is valid regarding the actual criminal provisions of Law n. 58/2019 (Law on data protection).

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

As referred in the previous answer, the Law 46/2018 (Law on cybersecurity), the Law 58/2019 (Law on data protection) and the Law 59/2019 (Law on data protection in criminal investigations) all foresee administrative fines.

When a certain act is simultaneously a criminal and an administrative offense, the former always prevails.

It should also be noted that the fines foreseen in the GDPR were reduced by the Portuguese lawmaker. According with the GDPR, in the most severe cases of non-compliance fines can reach up to 20 000 000 euros or 4% of the company's annual gross revenue in global terms from the preceding year, whatever is higher (Article 83/5 of the GDPR). However, Law 58/2019 (Law on data protection) settled minimum limits for the fines (Articles 37 and 38 of Law 58/2019). For instance, for the most severe administrative offenses, the amounts start in the 5000 euros for the big companies, in the 2000 euros for small and medium-sized enterprises, and in 1000 euros for natural persons. In sum, fines are graded at three levels depending on whether it is a large company, an SME (small or medium company) or a natural person, though maintaining the maximum limits provided for in the GDPR.

There are also some particularities for the determination of the amount of the fine.

In addition to the criteria set out in the GDPR, the CNPD (the authority in charge of data protection) shall take into account additional criteria to establish the amount of the fine (Article 39/1 of Law 58/2019):

i) Regarding natural persons, the economic situation of the agent;

ii) Regarding legal entities, the turnover and annual balance sheet, the continuing character of the infringement, the size of the entity, the number of workers and the nature of the services provided.

There is a particularity in the case of administrative fines. When the act was committed with negligence (thus, without dolus) the filing of the infringement proceeding depends on a prior warning from an agent of the CNPD (the national authority in charge of data protection), to comply with the omitted obligation or the violated prohibition within a reasonable time (Article 39/3 of Law 58/2019).

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

They constitute an official offence - in the cases of crimes and offenses provided for in Law 58/2019.

But, for example, the article of breach of confidentiality provided for in our Penal Code (article 195 CP) is dependent on the complaint of the person who saw his right injured.

22.5 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?

Decree-Law No. 80/2018 of 15 October establishes the principles and rules applicable to ethics committees that operate in health institutions, higher education institutions and biomedical research centres conducting clinical research. Thus, all higher education institutions should have an ethics committee. However, if there is no indication of which fields should be evaluated by these committees, there are always two that are taken into account: consent of participants and processing of personal data.

Also, the Foundation for Science and Technology, the national research and development support agency, always appreciates these aspects before funding is granted. These aspects are controlled before the research begins and during the investigation through periodic reports.

The entity in charge of reviewing data protection practices in clinical research projects is the Ethical Commission for Clinical Investigation (Comissão de Ética para a Investigação Clinica, CEIC).

(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?

Apart from funding offices pertaining to academic institutions and aimed to fund projects developed by the respective institutions, in Portugal there is only one general funding agency, the Foundation for Science and Technology (Fundação para a Ciência e Tecnologia), which is a governmental entity.

According with its website: 'FCT supports the scientific community in Portugal through a range of funding schemes, tailored for individual scientists, research teams or R&D centres. Through its funding schemes, FCT supports graduate education, research and development, establishment and access to research infrastructures, networking and international collaborations, conferences and meetings, science communication and interactions with

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)