

Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Data Protection & Privacy

Portugal

Helena Tapp Barroso and Tiago Félix da Costa

Morais Leitão, Galvão Teles, Soares da Silva & Associados

practiceguides.chambers.com

2021

PORTUGAL

Law and Practice

Contributed by:

Helena Tapp Barroso and Tiago Félix da Costa

Morais Leitão, Galvão Teles, Soares da Silva & Associados see p.16



Contents

1. Basic National Regime	p.2	4. International Considerations	p.12
1.1 Laws	p.2	4.1 Restrictions on International Data Issues	p.12
1.2 Regulators	p.2	4.2 Mechanisms That Apply to International Data Transfers	p.12
1.3 Administration and Enforcement Process	p.2	4.3 Government Notifications and Approvals	p.13
1.4 Multilateral and Subnational Issues	p.2	4.4 Data Localisation Requirements	p.13
1.5 Major NGOs and Self-Regulatory Organisations	p.3	4.5 Sharing Technical Details	p.13
1.6 System Characteristics	p.3	4.6 Limitations and Considerations	p.13
1.7 Key Developments	p.3	4.7 “Blocking” Statutes	p.13
1.8 Significant Pending Changes, Hot Topics and Issues	p.3		
2. Fundamental Laws	p.4	5. Emerging Digital and Technology Issues	p.13
2.1 Omnibus Laws and General Requirements	p.4	5.1 Addressing Current Issues in Law	p.13
2.2 Sectoral and Special Issues	p.7	5.2 “Digital Governance” or Fair Data Practice Review Boards	p.14
2.3 Online Marketing	p.10	5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation	p.14
2.4 Workplace Privacy	p.10	5.4 Due Diligence	p.14
2.5 Enforcement and Litigation	p.11	5.5 Public Disclosure	p.14
		5.6 Other Significant Issues	p.14
3. Law Enforcement and National Security Access and Surveillance	p.11		
3.1 Laws and Standards for Access to Data for Serious Crimes	p.11		
3.2 Laws and Standards for Access to Data for National Security Purposes	p.12		
3.3 Invoking Foreign Government Obligations	p.12		
3.4 Key Privacy Issues, Conflicts and Public Debates	p.12		

1. Basic National Regime

1.1 Laws

Portugal has had national constitutional privacy provisions for almost five decades and Article 35 of the Portuguese Constitution sets forth structuring principles and guarantees on personal data protection.

It guarantees all citizens rights to access, correct and update, any computerised data relating to them; as well as full information rights on the purposes and intended uses of such data. The Constitution also contains reinforced provisions regarding sensitive data and establishes a general restriction towards third-party access to personal data.

Although Article 35 is focused on the use of information technology regarding data processing, the provision extends the protection and guarantees to personal data kept in manual files.

The legal framework for personal data protection in Portugal derives from direct application of Regulation (EU) 2016/679 (General Data Protection Regulation or GDPR), and from the Portuguese Law No 58/2019 of 8 August, which ensures the implementation of the GDPR in Portugal.

Law No 41/2004 of 18 August (as subsequently amended) transposed into national law Directive 2002/58/EC (Directive on privacy and electronic communications).

1.2 Regulators

The supervisory authority responsible for monitoring compliance with data protection rules and principles in Portugal is the *Comissão Nacional de Protecção de Dados* (CNPd). The CNPD holds broad powers of investigation, specifically, the powers to request information, to perform data protection audits and to obtain access to the data controller's or data processor's facilities, including equipment and data processing means.

The CNPD's main duties and responsibilities are:

- to supervise and monitor compliance with personal data protection laws and regulations;
- to issue prior opinion on legal provisions and projects, in EU or international institutions, relating to the processing of personal data;
- to exercise investigative powers on personal data processing activities;
- to exercise powers of authority, including blocking, erasure or destruction of data, or imposing temporary or permanent bans on the processing of personal data;
- to warn or publicly censure controllers for failure to comply with legal provisions on data protection;

- to be engaged in legal proceedings, in cases of breach of personal data protection legislation; and
- to report to the Public Prosecution Office any data protection criminal offences and to take necessary urgent measures to produce evidence.

The CNPD's decisions are binding and may be appealed from before the administrative courts.

1.3 Administration and Enforcement Process

Portugal's regulatory offence procedure is split into two phases:

- an administrative phase, where the supervisory authority investigates the relevant facts and decides on imposing penalties; and
- a judicial phase, where the respondent may challenge the supervisory authority's decision in court.

Under the Portuguese Regulatory Offence Act, no penalty may be imposed without the defendant having been heard on the facts under investigation.

Defendants in a regulatory offence procedure enjoy most due process rights granted in criminal defence; namely, the presumption of innocence, the right to produce and present evidence, and the right to appeal unfavourable decisions. However, in these procedures, the privilege against self-incrimination may be mitigated, since controllers and processors are obliged to co-operate with the CNPD; namely, by supplying the authority with the documents and information requested at the investigation stage.

1.4 Multilateral and Subnational Issues

Being an EU member state, all privacy regulation is either European legislation or local legislation based on European instruments. More than a year after the application start date of the GDPR, a national data protection act was issued – Law No 58/2019, of 8 August – repealing the 1998 Data Protection Act that had transposed Directive 95/46/EC (which had been repealed by the GDPR). One point of interest of Law No 58/2019 is that the Portuguese supervisory authority (CNPd) issued a decision, on 3 September 2019, indicating a number of provisions in the law which it considered to have exceeded the terms for admitted national level regulation. In this decision (No 2019/494), the CNPD listed the provisions of Law No 58/2019 it considered as being incompatible with EU law (specifically the GDPR) and, which, for that reason and based on the principle of the primacy of EU law, the supervisory authority has stated it will not be following in future cases.

The first specific data protection act in Portugal was issued in 1991, and its provisions were essentially based on the principles

and provisions contained in the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), adopted by the Council of Europe.

Among the relevant international instruments adopted in Portugal, Convention 108, the European Convention on Human Rights (Article 8); and the Charter of Fundamental Rights of the European Union (Articles 7 and 8) should be mentioned.

Specific laws or specific legal provisions regarding personal data protection should also be considered, including Law No 41/2004, which plays an important role, not only for electronic communications providers but also for all data controllers in respect of cookies, geolocation data and direct marketing. Please see **2.2 Sectoral and Special Issues** (Communications Data) and (Internet, Streaming and Video Issues) and **2.3 Online Marketing** for further detail.

1.5 Major NGOs and Self-Regulatory Organisations

There are no relevant, active privacy and data protection NGOs in Portugal, although there are a few associations associated with the roles of data protection officers and privacy professionals.

1.6 System Characteristics

Being an EU member state the Portuguese legal system follows the European model. EU Regulations – such as the GDPR – are directly applicable in Portugal.

The legal regime for the protection of personal data in force in Portugal is highly developed and the CNPD is a very demanding authority.

1.7 Key Developments

The most important development in data protection in the last 12 months have largely focused on:

- cross-border data transfers and the need to adjust to the impact of both the Schrems II decision and the impact of Brexit; and
- privacy issues connected to COVID-19.

Track and Tracing Apps

As in many other jurisdictions worldwide, Portugal experienced COVID-19 tracing and tracking app development and implementation, featuring a voluntary contact tracing and warning app, known as STAYAWAY COVID. Following a publicly available data protection impact assessment (DPIA) on which the CNPD was called upon to issue an opinion, specific legislation was issued: Decree Law No 52/2020 of August 11. This law:

- appointed the Portuguese health authority (DGS) as the data controller for processing under the STAYAWAY COVID system;
- strictly limited the processing purposes under the app; and
- ruled on the exceptional and transitional nature of such processing, limited to the duration of the “epidemiological situation... [and] the need to keep processing”.

The app adopts a decentralised approach and resorts to user proximity sensors – using Bluetooth Low Energy technology – and no geolocation data (proximity data being, additionally, pseudonymised). At a certain point, legislative measures were planned for use of the app to become mandatory in schools, higher education and the workplace, but this was strongly opposed, including by the CNPD, and the government withdrew the proposal before it reached parliamentary discussion or voting.

COVID-19 Data Protection Guidelines

The CNPD issued several guidelines on the collection and processing of personal data in the context of the COVID-19 pandemic, and on data protection and privacy guarantees in that context, including on:

- publicly available information on COVID-19 infections (and measures to prevent information from allowing infected person being identified or becoming identifiable);
- remote work employee monitoring (focused on the mandatory remote work provisions in the context of the COVID-19 pandemic);
- employee health data processing by employers for the prevention of the spread of COVID-19 in the workplace;
- processing of student and teacher data in the context of remote education measures;
- processing of student health data for the prevention of the spread of COVID-19 in schools and higher education institutions;
- processing of health data for temperature monitoring and testing requirements to access premises; and
- questionnaires for contact tracing and infection chain detection.

1.8 Significant Pending Changes, Hot Topics and Issues

COVID-19

Privacy issues related to COVID-19 were, and still are, at the centre of discussions around data protection and privacy in Portugal.

Issues such as the data processing involved in temperature taking or testing as a pre-requirement to allow access to premises (particularly, employee access to the workplace but also in

schools) were under active discussion and the object of specific transitory regulation, particularly in the emergency state or equivalent regulations. Vaccination requirements, immunity passports and immunity (or vaccination) data digitisation are also hot topics and issues to be looked into. This is particularly the case in the workplace, upon returning once lockdown provisions are mitigated.

E-Privacy Regulation

Other significant changes on the horizon include the progress and, eventually, approval of the E-Privacy Regulation which will repeal Directive 2002/58/EC, after the Council of the EU, under Portuguese presidency, released a new draft version for discussion.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Data Protection Officers

Before the GDPR there were no specific local law requirements for the appointment of privacy or data protection officers (DPO). Portuguese Law No 58/2019 of 8 August contains specific rules for the designation of DPOs, for both the public and private sectors. As far as the public sector is concerned, the provisions define the entities that qualify as public authorities or bodies for the purposes of the requirement of DPOs and provide rules on the appointment requirements and role.

Private entities are required to appoint a DPO in accordance with the criteria contained in the GDPR (ie, in the case of controllers or processors whose core activities consist of processing operations which – by virtue of their nature, their scope and/or their purposes – require regular and systematic monitoring of data subjects on a large scale; or consist of processing, on a large scale, of special categories of data and/or data relating to criminal convictions and offences). Portuguese Law No 58/2019 of 8 August does not provide for other cases where the appointment of DPO would be required.

Even when not strictly legally required to do so, other private sector controllers or processors may choose to appoint a DPO as encouraged by EU regulators.

Under Law No 58/2019, the following roles and responsibilities of the DPO, additional to those indicated in Articles 37 and 38 of the GDPR, are listed:

- guaranteeing the performance of periodic and ad hoc audits;
- raising awareness so as to ensure the prompt detection and reporting of security incidents to the security officer; and

- ensuring the relationship with data subjects on matters covered by the GDPR and national laws on data protection.

Authorised Data Collection

Under the GDPR principles, data controllers must process personal data lawfully, fairly and in a transparent manner in relation to the data subject; and personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Lawful bases for processing personal data include:

- the data subject's specific, free (and, therefore, withdrawable at any time), unambiguous and informed consent (explicit consent for one or more specified purposes is additionally required for the processing of sensitive data, when such processing is based on data subject consent);
- processing being required 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;
- the legitimate interest of the data controller or a third party – typically, in the case of data processing performed by a private sector controller – except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data;
- processing required by public interest or, in the case of public authorities or bodies in the performance of their tasks, in the exercise of official authority vested in the controller;
- processing needed to comply with legal obligations imposed on the controller; and
- processing necessary to protect the vital interests of the data subject or another natural person.

When it comes to the processing of special categories of data (sensitive data) – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, 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 – processing is only admitted under the processing exceptions of Article 9 (2) of the GDPR.

Privacy by Design or by Default

When developing and designing products and services that involve the processing of personal data – and when selecting and using solutions to support, develop and offer such products or services – controllers must take into account the right to data protection of potential clients, customers, employees and other affected data subjects in accordance with a principle of data protection by design.

Similarly, the concept and principle of data protection by default, as established in Article 25 of the GDPR, is also fully applicable in Portugal requiring that controllers implement appropriate technical and organisational measures to ensure that, by default, only the personal data that is necessary for each specific purpose of the data-processing is processed. This applies to, among other things, (i) the amount of personal data collected, (ii) the extent of its processing, and (iii) the period of its storage accessibility.

Privacy Impact Analyses

Processing operations that are likely to result in a high risk to the rights and freedoms of data subjects must be subject to prior assessment by the controller. The assessment should evaluate the origin, nature, particularity and severity of the risk to those rights and freedoms that the intended processing activity will represent and allow the controller to determine which measures should be adopted to ensure the processing conforms with all applicable legal principles – such as those of lawfulness, fairness, transparency, purpose limitation and minimisation – and also to guarantee data accuracy, integrity and confidentiality.

With reference to Article 35 (4) and (6) of the GDPR, the CNPD established a list of processing operations subject to prior data protection impact assessment (DPIA).

The list was published in CNPD's Regulation No 1/2018 of 16 October and aims at identifying processing operations likely to result in a high risk and which therefore require a DPIA.

In the case of Portugal, the operations that require a prior DPIA are:

- processing of information arising from the use of electronic devices which transmit, through communication networks, personal data relating to health;
- processing of special categories of personal data or personal data relating to criminal convictions and offences or data of a highly personal nature, where such data is not collected directly from the data subject and it is not possible or feasible to ensure compliance with the GDPR's information duties;
- processing of personal data which involves or consists of large-scale profiling;
- processing of personal data to trace the location or conduct of the respective data subjects (eg, workers, customers) that has the effect of evaluating or classifying them, except where the processing is indispensable for the provision of services specifically required by the data subjects;
- processing of special categories of personal data, personal data relating to criminal convictions and offences, or data of a highly personal nature, for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes, except for the processing of personal data regulated by law that provides adequate guarantees of the rights of the data subjects;

- processing of biometric data for the unambiguous identification of data subjects when they are vulnerable persons, except for processing regulated by law;
- processing of genetic data of vulnerable persons, except for processing regulated by law;
- processing of special categories of personal data or personal data relating to criminal convictions and offences or data of a highly personal nature with the use of new technologies or new use of existing technologies.

Privacy Policies

Although there is no strict provision determining that the controller must adopt internal or external privacy policies, these are, based on best practices, relevant measures for establishing compliance with the GDPR, where policies should meet the principles of data protection by design and data protection by default.

Data Subject Access Rights

Law No 58/2019 of 8 August does not provide for any specific formalities for data subjects to exercise their right of access to data.

The right of access comprises the data subjects' entitlement to:

- obtain confirmation from the data controller as to whether or not personal data concerning the data subjects are being processed; and
- that being the case, an entitlement to have access to the personal data, to all the information provided for in Article 15(1) (a) through (h) and (2) of the GDPR, and to obtain a copy of the personal data undergoing processing.

Data subjects are also entitled to require the correction or updating of inaccurate or outdated data from the controller.

Data subjects are entitled to object at any time to the processing of information relating to them:

- on justified grounds; or
- in any case, and free of charge, if information is meant for the purposes of direct marketing or any form of market research.

Additionally, data subjects are entitled to the right not to be subject to a decision that produces legal effects concerning them or significantly affecting them, and which is based solely on automated processing of information intended to evaluate certain personal aspects of the data subjects.

Data subjects are also granted erasure rights and the right to restriction of processing, particularly when the data held by the controller does not comply with the provisions and principles set out for processing under the GDPR.

All other substantive rights granted to individuals by the GDPR fully apply, including the right to data portability within the limits foreseen in Article 20 of the GDPR.

Naturally, none of the above rights are unrestricted. They should be exercised under the conditions foreseen in Articles 15–22 of the GDPR.

Anonymisation, De-identification and Pseudonymisation

Anonymisation

Personal data is effectively anonymised if the person to whom the data relates is not or no longer identifiable. Effective anonymisation requires taking into account possible new technologies which may enable re-identification of data once considered anonymous. Anonymisation should be irreversible in the sense that one cannot identify an individual by coupling the anonymised data with any additional information.

Personal data which has been anonymised is no longer considered to be personal under the GDPR, and therefore out of scope for data protection legislation application.

De-identification

De-identification is the process used to prevent personal identifiers from being connected with information.

If the person to whom the data relates is no longer identifiable, the data will no longer be considered to be personal data as defined in the GDPR.

If it is possible to identify the person to whom the data relates, the data is personal data under the GDPR, and therefore the requirements under the data protection legislation will apply to the processing of such data.

Pseudonymisation

According to the GDPR, “pseudonymisation” means “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person”.

If the identifying elements of personal data are removed, but are kept separately and could be re-united with the remaining elements of the data, it is possible to identify the data subjects

so this will remain as personal data. The requirements under the applicable data protection legislation shall, therefore, be observed for pseudonymised data.

Data and Technology

Profiling

Pursuant to the GDPR, controllers can carry out profiling and automated decision-making as long as they can meet all the principles and have a lawful basis for the processing involved. Additional safeguards and restrictions apply in the case of solely automated decision-making which has a legal effect or similarly significantly affects the data subject.

With respect to “profiling”, which does not have any legal effects or does not similarly significantly affect the data subject, the GDPR provides that a data subject shall have the right to object, on grounds relating to their particular situation, at any time, to profiling which is necessary:

- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- for purposes of the legitimate interests pursued by the controller or by a third party.

In such a situation, the controller shall no longer process the personal data unless it demonstrates compelling and legitimate grounds for the processing (which override the interests, rights and freedoms of the data subject) or for the establishment, exercise or defence of legal claims.

Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of data concerning them such purpose, which includes profiling to the extent that it is related to such direct marketing.

Automated decision-making

The GDPR excludes decision making resulting in legal or other significant consequences for the data subject, based solely on automated processing, including profiling.

Exceptions to the above, under the GDPR are decisions:

- (i) necessary for the performance of, or entering into, a contract with the individual;
- (ii) based on the data subject's explicit consent; or
- (iii) authorised by EU or member state law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

For cases under points (i) and (ii), the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. These measures should include, at least, the right to obtain human intervention on the part of the controller, the right of the data subject to express their point of view and the right to contest the decision.

Online monitoring or tracking

GDPR principles must be respected when personal data is processed in the context of online monitoring or tracking. Particularly relevant are the rules on the principle of purpose limitation, the legal basis for the processing and retention periods. According to the GDPR, personal data can only be kept while necessary for the purposes for which they were collected and the controller shall establish retention periods in line with this rule.

Moreover, Article 5 (1) of Portuguese Law No 41/2004 of 18 August requires the collection of informed consent before information in the user's (or subscriber's) terminal device is stored or accessed, which includes the use of cookies. Consent to technical storage or access to such information is not required if it is (i) used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) strictly necessary for the provider to provide an information society service explicitly requested by the subscriber or user.

Under the CNPD's Regulation No 1/2018, the processing of personal data to trace the location or conduct of the respective data subjects (eg, workers or customers) resulting in their evaluation or classification, except where the processing is indispensable for the provision of the services specifically required by the data subjects, is likely to result in a high risk and requires a DPIA.

Big data analysis, AI and algorithms

Personal data processing in this context must comply with GDPR rules and principles, including those on purpose limitation, the legal basis for the processing and retention periods.

Personal data which has been anonymised is no longer considered to be personal data under the GDPR.

The Concept of "Injury" or "Harm"

Damages suffered by data subjects, as a result of an act or omission purportedly of the controller, in breach of the GDPR provisions or other legal provisions for the protection of personal data, will trigger an entitlement to compensation for damage claimable through the courts. Compensation for serious injury to feelings may be also claimed.

However, punitive damages – ie, the possibility for a court, in a civil liability action, to order the payment of compensation in an amount of money exceeding the amount of the damages

suffered as a result of the unlawful conduct – have a very limited scope of application in Portugal.

The right to claim monetary damages and compensation is exercisable through the judicial system and not directly enforced by the supervisory authority.

2.2 Sectoral and Special Issues

Sensitive Data

In Portugal, the special categories of data (sensitive data) are those set forth in Article 9 (1) of the GDPR (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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).

The GDPR states the general rule that the processing of such special categories of data is prohibited with the exception, only, of the processing of such data on the grounds laid out in, or as required in the cases foreseen by, Article 9 (2) of the GDPR.

Exceptions include, among other things:

- explicit consent given by the data subject to the processing of that personal data for one or more specified purposes, except where the law provides that the processing prohibition may not be lifted by the data subject;
- processing necessary for compliance with obligations or to exercise rights under employment and social security and social protection laws, as set out in the law or a collective agreement pursuant to the law providing for appropriate safeguards for the rights and freedoms of data subjects;
- protection of the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent;
- processing required for the establishment, exercise or defence of a legal claim or whenever courts are acting in their judicial capacity;
- processing necessary for reasons of substantial public interest on the basis of legal provisions which are proportionate, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the rights and interests of the data subjects;
- processing required for preventative or occupational medicine, medical diagnosis, provision of health or social care or treatment or management of health or social care systems and services on the basis of the law or pursuant to a contract with a health professional; and
- requirements resulting from archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of legal provisions.

Portuguese Law No 58/2019 of 8 August did not include further conditions with regard to the processing of genetic data, biometric data or data concerning health under the provision contained in Article 9 (4), with the exception of employee biometric data whose processing is admitted for access control and working hours control.

Financial Data

Directive 2014/65/EU on markets in financial instruments (MiFID II Directive) has been implemented in Portugal and this has involved an increase in record keeping regarding financial transactions, including requirements on financial intermediaries to keep a record of market orders and information exchanged with investors that involves relevant personal financial data processing, and maintaining high levels of security regarding the electronic processing of data as well as reinforced requirements regarding the integrity and confidentiality of the data recorded.

Health Data

Under the GDPR the processing of data concerning health (as is the case with other special categories of data) is only admitted under the specific exception grounds foreseen in Article 9 (2).

In addition, the Portuguese Law No 58/2019 of 8 August contains specific provisions for processing health and genetic data, which include that:

- the access to health and genetic data being governed by the need-to-know principle;
- in the cases provided for in Article 9, paragraph 2, (h) and (i), of the GDPR, the processing of health and genetic data shall be carried out by a professional bound to secrecy or by another person bound by a duty of confidentiality, and appropriate information security measures shall be guaranteed;
- access to health and genetic data shall be made exclusively through electronic means, unless it is technically impossible or the data subject expressly indicates otherwise;
- the disclosure or subsequent transmission of health and genetic data is prohibited;
- the data subject shall be notified of any access to their health or genetic data, and the controller shall ensure the availability of this traceability and notification mechanism; and
- the members of corporate bodies, workers and service providers of the controller, the DPO, students and researchers in the area of health and genetics, and all health professionals who have access to health and genetic data are obliged to a duty of confidentiality.

Communications Data

The processing of data in the context of electronic communication service providers and services (telecoms sector) is subject

to specific legislation. Currently the regulation is contained in Portuguese Law No 41/2004 of 18 August.

Additionally, Portuguese Law No 32/2008 of 17 July implemented Directive 2006/24/EC (Data Retention Directive).

Content of Electronic Communications

Under the Portuguese Criminal Procedure Code, the interception and recording of telephone, electronic or other kinds of conversations and communications can only be performed by the competent authorities, with a reasoned order from a judge and at the request of the Public Prosecutor, regarding crimes expressly foreseen for this purpose and if there is reason to believe that these measures are indispensable for the discovery of the truth or that the evidence would otherwise be impossible or very difficult to obtain.

Children's Data

Children receive some specific protection as far as the processing of their personal data is concerned. Notably, specific requirements apply to language used to provide any information on data processing addressed to a child; such information is required to be written in language that is sufficiently clear and plain to be easily understood by a child.

Under the Portuguese Law No 58/2019 of 8 August, when consent is the basis for child data processing in relation to the offer of information society services directly to a child, the consent of the holder of parental responsibility is not required where the child is at least 13 years old.

In 2016, the CNPD issued guidelines on the availability of students' (and other data subjects') personal data on school internet pages and, in 2018, additional guidelines were issued on the same subject matter regarding university and equivalent institutions.

Employment Data

Portuguese Law No 7/2009 of 12 February (Portuguese Labour Code) establishes, in Articles 16–22, norms on data processing in the workplace, namely, norms pertaining to the processing of an employee's biometric data, the demand for medical exams as a condition for employment and the use of remote surveillance methods.

Additionally, Article 28 of the Portuguese Data Protection Law regulates the processing of personal data in the employment context.

Internet, Streaming and Video Issues

Article 5 (1) of the Portuguese Law No 41/2004 of 18 August requires the collection of informed consent before informa-

tion in the user's (or subscriber's) terminal device is stored or accessed, which include the use of cookies. However, Article 5 (2) of the Portuguese Law No 41/2004 of 18 August stipulates that consent to technical storage or access to such information is not required if it is (i) used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) strictly necessary for the provider to provide an information society service explicitly requested by the subscriber or user.

Data Subject Rights

According to the GDPR, data subjects have the following rights:

- right of access;
- right to rectification;
- right to erasure;
- right to restriction of processing;
- right to data portability;
- right to object;
- right not to be subject to a decision based solely on automated processing;
- right to withdraw consent; and
- right to lodge a complaint with the supervisory authority.

Special attention should be given to the right of data subjects to be informed. According to this right the controller shall provide the data subjects with a set of information on the processing of their personal data, which includes, but is not limited to:

- the purposes of the processing for which the personal data is intended;
- the legal basis for the processing;
- the recipients or categories of recipients of the personal data; and
- the period for which the personal data will be stored.

Right to be Forgotten

According to the GDPR, the data subject has the right to obtain from the controller the erasure of personal data concerning them, without undue delay and the controller has the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and there is no other legal ground for the processing;
- the data subject objects to the processing of personal data concerning them and there are no overriding legitimate grounds for the processing, or the data subject objects to

the processing of their personal data for direct marketing purposes;

- the personal data has been unlawfully processed;
- the personal data must be erased for compliance with a legal obligation in EU or member state law to which the controller is subject; or
- the personal data has been collected in relation to the offer of social services.

The right of erasure does not apply where the processing of personal data is necessary for the following purposes:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by EU or member state law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right of erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

Data Access and Portability

According to the GDPR, the data subject has the right to receive personal data concerning them, which they have provided to the controller, in a structured, commonly used and machine-readable format.

The data subject also has the right to transmit the personal data concerning them to another controller without hindrance from the controller to which the personal data had originally been provided, where:

- the processing is based on consent or on a contract to which the data subject is party; and
- the processing is carried out by automated means.

In this case, the data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.

Portuguese Law No 58/2019 of 8 August contains a provision on portability that underlines that the data subject's right to data portability only includes data that has been provided by the data subject to the controller, a wording that may be interpreted in accordance with the understanding contained in Article 29 Working Party Guidelines on Portability to include data indi-

rectly “provided” by the data subject through use of a service or device.

Portuguese Law No 58/2019 of 8 August also states that, whenever possible, portability should be operated in an open format. In the case of the public service bodies, it provides that whenever data interoperability is not technically possible the data should be provided to the data subject in an open digital format in accordance with the National Regulation on Digital Interoperability (approved and published by the Government in January 2018).

Right of Rectification

Data subjects have the right to obtain from the controller, without undue delay, the rectification of their personal data. Taking into account the purposes of the processing, data subjects have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

2.3 Online Marketing

Portuguese Law No 41/2004 of 18 August contains specific provisions on unsolicited communications for marketing purposes.

Unsolicited electronic commercial communication aimed at data subjects (natural persons) is limited to cases where prior consent has been provided, except where the controller has obtained the electronic contact of its customers, in the context of the sale of products or services, in which case that controller may address the data subject with direct marketing on products or services marketed by the controller and similar to those previously provided. This possibility is, however, subject to the controller having provided the data subject with the prior possibility of opting out from unsolicited communications, in an easy and free of charge manner, and of providing an easy opt-out on the occasion of each marketing message that is sent.

Under the guarantees granted by the GDPR (particularly Article 21 (2) and (3)), where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to such processing, including to object to profiling – allowing targeted advertising – to the extent that it is related to such direct marketing and where the data subject objects to processing for direct marketing purposes, the controller may no longer process their data for direct marketing purposes.

Once the current proposal for an E-Privacy Regulation is finally approved, enters into force and replaces the existing E-Privacy Directive, Portugal, as an EU member state, will be subject to its direct application.

2.4 Workplace Privacy

Employee Monitoring

The Portuguese Labour Code contains, in Articles 16–22, provisions on employee privacy, including provisions on monitoring and surveillance.

As a rule, the use of surveillance equipment by the employer to control employee performance is excluded. Closed-circuit TV in office premises is lawful only where it aims to protect the safety of persons and goods or when the nature of the activity so requires.

Employees are granted privacy and confidentiality guarantees regarding personal correspondence and messages even when using work email addresses.

Employers are limited in their ability to request information on a candidate's or employee's private life, except for information that is strictly necessary or relevant to assess their aptitude/abilities for the job. In such cases, the specific reasons for requiring the information must be provided in writing by the employer. The same rules apply to information on health or pregnancy and in this case the information must be provided to a doctor who will merely inform the employer on the person's aptitude for the job.

In addition, Article 28 of Portuguese Law No 58/2019 of 8 August regulates to the processing of personal data in the employment context, foreseeing that:

- an employer could process the personal data of its employees for the purposes and within the limits defined in the Portuguese Labour Code and the respective complementary legislation or other employment legislation;
- recorded images and other personal data gathered through the use of video systems or other technological means of remote surveillance, in accordance with Article 20 of the Portuguese Labour Code, can only be used in the context of criminal proceedings – however, these images and personal data can also be used for the purpose of establishing disciplinary responsibility, provided this is limited to criminal proceedings; and
- an employer shall only process its employees' biometric data for the purposes of attendance control and access control to the employer premises.

Employers may rule the terms for use of means of communication provided through company IT, but employees are entitled to keep their private use confidential, including the content of personal emails and internet access. Admissible use of the means of communication provided through company IT should

form part of an internal regulation (policy). The CNPD issued guidelines in 2013 for such purposes.

Before implementing any monitoring system, the employer must inform its employees about the conditions under which the IT and communication equipment made available at the workplace may be used for private purposes and on the monitoring schemes and personal data processing resulting from that monitoring. Generic monitoring methodologies must be adopted avoiding the individual consultation of personal data.

The document includes quite detailed and specific guidelines for phone use and for the use of email and internet access.

However, it should be noted that these guidelines were issued before the GDPR entered into force and Portuguese case law is not unanimous on the rules applicable in this context.

Works Councils and Whistle-Blowing

Consultation with employee work councils is required for certain types of data-processing, particularly for the processing of employee biometric data and the use of closed-circuit TV in office premises.

The CNPD also published a resolution (in 2009) setting forth the conditions according to which whistle-blowing programmes are admissible. Under this resolution the CNPD's understanding is that the purpose of whistle-blowing (and the purpose of the data-processing resulting from whistle-blowing hotlines) must be limited to the internal control of reports of misconduct intended to prevent or repress internal irregularities in the fields of accounting, internal accounting controls, auditing matters, the fight against corruption, and banking and financial crimes.

In general, Portuguese labour law does not establish an obligation to inform work councils about the implementation of this kind of scheme in the company. However, if the company intends to provide binding rules to all employees, the whistle-blower scheme will typically be laid-out in an internal company regulation and this type of instrument is subject to prior consultation with the employee representative structures (works council or union representatives).

2.5 Enforcement and Litigation

Any offence, be it regulatory or criminal, must be defined by law; and its elements, including culpability, must be proven beyond a reasonable doubt in order for any penalty to be applied.

Regulatory offences are investigated by the CNPD, which also has the power to convict, although the CNPD's convictions may be subjected to judicial review.

Criminal offences are investigated by the Public Prosecutor's Office but only a court may convict a defendant.

Under the GDPR, enforcement penalties for data privacy or data protection violations may reach EUR20 million or up to 4% of a company's total worldwide annual turnover in the preceding financial year, whichever is higher.

Criminal offences related to data protection are currently punished with fines or prison terms that range from six months to four years.

On 11 October 2018, the CNPD imposed a EUR400,000 penalty on a public hospital in the greater Lisbon area, for irregularities in the access to patients' medical records. This case is notable for having the first penalty imposed under the new GDPR framework, for having a public entity as a defendant and for dealing with a special category of personal data, specifically medical records.

Legal standards for private litigation regarding alleged data privacy and data protection violations, for now, are the same as any other civil case regarding personal rights.

Portuguese Law No 58/2019 of 8 August contains rules shifting the burden of proof from the plaintiff to the data controller and data processor.

Portuguese Civil Procedure Law allows for class action lawsuits for the protection of consumer interests, which may include consumers' right to privacy and personal data protection.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Law enforcement access to data for serious crimes is covered by the Criminal Procedure Code and the Portuguese Cybercrime Law. Public prosecutors may unilaterally authorise the search and seizure of stored computer data, except for data covered by professional privilege, in which case access to those systems must be ordered by an investigating judge.

Portuguese Law No 32/2008 of 17 July establishes the legal framework for the collection of metadata by law enforcement. The collection of metadata must be authorised by an investigating judge and must be indispensable for the investigation of crimes at hand.

3.2 Laws and Standards for Access to Data for National Security Purposes

Portuguese Organic Law No 4/2017 of 25 August establishes the legal framework for the collection of metadata by intelligence services.

The collection of metadata must be authorised by a special section of the Supreme Court and must be proportionate to the ends for which that data is collected.

However, it should be noted that the Portuguese Constitutional Court has declared the unconstitutionality of:

- the rule set out in Article 3 of the Portuguese Organic Law No 4/2017 of 25 August, in so far as it allows information officers of the Security Intelligence Service (SIS) and the Strategic Intelligence and Defence Service (SIED) access to source data and equipment location data, when they are not supported by a concrete communication, for the purpose of producing information necessary to safeguard national defence and internal security; and
- the rule set out in Article 4 of the Portuguese Organic Law No 4/2017 of 25 August.

3.3 Invoking Foreign Government Obligations

Access to data by foreign governments must be done through the Judicial Police and comply with the principles of international co-operation established in the Cybercrime Law, without prejudice to any applicable international conventions.

Portugal does not participate in a Cloud Act agreement with the USA.

3.4 Key Privacy Issues, Conflicts and Public Debates

Cases such as “Football Leaks” and “Luanda Leaks” have generated considerable public controversy about the legality of evidence obtained in violation of the privacy of individuals.

4. International Considerations

4.1 Restrictions on International Data Issues

According to the GDPR, the transfer of personal data to another European Union member state and to European Economic Area (EEA) member countries is not restricted. However, transfer outside these territories is restricted and shall take place only in the following cases.

- If the European Commission has decided that the country in question ensures an adequate level of protection for personal data.

- If the controller or processor has provided appropriate safeguards (eg, standard contractual binding clauses), and on the condition that enforceable data subjects rights and effective legal remedies for data subjects are available.
- In the absence of an adequacy decision from the European Commission and of appropriate safeguards, and on an exceptional basis, if:
 - (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
 - (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request and the transfer of personal data is occasional;
 - (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
 - (d) the transfer is necessary for important reasons of public interest;
 - (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
 - (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
 - (g) the transfer is made from a register which according to EU or member state law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or member state law for consultation are fulfilled in the particular case.

4.2 Mechanisms That Apply to International Data Transfers

International data transfers may be made under contracts that follow the standard form model clauses approved by the European Commission, although currently approved standard clauses are yet to be adopted and updated to the GDPR.

Prior to the GDPR, the CNPD was amongst the supervisory authorities that rejected “binding corporate rules” as a mechanism for data transfers but this is now allowed under Article 47 of the GDPR.

Transfer to the USA was possible under the EU–US Privacy Shield framework but, in the wake of the CJEU decision in

Schrems II (see 1.7 Key Developments), this is no longer the case and transfers must be based on standard form model clauses and binding corporate rules.

4.3 Government Notifications and Approvals

There are no prior government notifications or approvals required to transfer data internationally in Portugal.

4.4 Data Localisation Requirements

Portuguese law does not provide for any requirement for data to be maintained in-country.

4.5 Sharing Technical Details

Article 27 (1) (o) of the Portuguese Law No 5/2004, of 10 February (Electronic Communications Law) requires electronic communications services providers to install, and make available to the authorities, communications interception systems, as well as decryption methods whenever encryption services are offered.

4.6 Limitations and Considerations

Article 48 of the GDPR establishes that judicial and administrative decisions, which require the transfer or disclosure of personal data, may only be recognised or enforced if they are based on an international agreement, without prejudice to other grounds for transfer found in Chapter V of the GDPR.

4.7 “Blocking” Statutes

The issue does not arise in the Portuguese jurisdiction.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

Automated Decision-Making

The provisions of Article 22 of the GDPR on automated individual decision-making (including profiling) fully apply in Portugal.

Therefore, the right not to be subject to decision based solely on automated processing, which produces legal effects concerning the data subject or similarly significantly affects the latter is granted to all data subjects and such automated decision-making processing is restricted to cases where the decision:

- is necessary for entering into, or for performing a contract between the data subject and the controller;
- is authorised by law applicable to the controller and which lays down suitable measures to safeguard the data subject; or
- is based on the data subject's explicit consent.

Profiling

The data subject has the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them based on legitimate interest or on a public interest task, including profiling. When the subject objects to such processing, the controller must not continue with such processing unless it is able to demonstrate compelling legitimate grounds for the processing – which override the interests, rights and freedoms of the data subject – or for the establishment, exercise or defence of legal claims.

Biometric Data

The use of employee biometric data for access control and control over employee working time was also addressed by the CNPD in specific guidelines issued in 2004 although some of these have to be read in the light of the new legal framework and interpreted accordingly, particularly because a number of principles that, under the prior system, would have been considered by the CNPD to require prior notification of the authority for the processing of biometric data for controlling access and monitoring hours worked, no longer apply.

Portuguese Law No 58/2019 of 8 August contains a provision stating that the processing of employee biometric data is (only) admissible for the specific purposes of access control and monitoring hours worked.

Geolocation

Geolocation is another area in which the CNPD issued guidelines (in 2014) focused on the processing of employee personal data resulting from the use of geolocation devices. The CNPD's understanding – which has found some support in court decisions – is that the use of GPS devices and the tracking they allow is equivalent to a distance surveillance system and their use – and the processing of data that results from their use – should be limited to purposes of safety protection or when the nature of the activity so requires.

The first relevant line drawn by the authority in the guidelines issued is that the employer shall not process data collected by geolocation (typically GPS) systems that reveal employee movements outside their working time. Within the limits of employee working time, the CNPD considers that the processing of such data to pursue purposes of efficiency, service quality, optimisation of company resources or protection of property is legitimate. Geolocation data shall not be used to control employee performance. The CNPD's understanding is restrictive on the possibility of the employer using geolocation devices – and processing information thus collected – on smartphones and laptops attributed to the employees as opposed to the use of the same devices in company vehicles. In the latter case, legitimate use and purposes are specifically indicated in the guidelines,

regarding fleet management in the case of activities involving services rendered to clients outside company premises, for the protection of property against theft and activities involving transportation of dangerous substances or high value goods. Clear and transparent information must be provided by the employer to the data subject employees on the use of geolocation devices included in vehicles or equipment used by the employee when performing their roles.

Drones

The Portuguese Civil Aviation Authority (ANAC) issued Regulation No 1093/2016, in December 2016, implementing specific provisions and rules on the use of drones in the Portuguese airspace.

Drone flights require prior authorisation by the ANAC except in cases where:

- the flight occurs in daylight;
- within a maximum altitude of 120 meters above the ground; and
- visual contact with the drone is kept at all times.

Night flights or flights over groups of more than 12 people require specific prior authorisation.

There are a number of relevant restrictions applicable to drone flights in the areas surrounding airports or other aircraft, and fines (of up to EUR250,000) may apply in the case of a breach of regulatory provisions.

This authorisation does not apply or refer to any data processing that occurs in connection with the use of drones (namely to the collection of photos or filming) and such processing is within the scope of data processing activities subject to the GDPR provisions.

5.2 “Digital Governance” or Fair Data Practice Review Boards

The issue does not arise in the Portuguese jurisdiction.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

See 2.5 Enforcement and Litigation.

5.4 Due Diligence

The issue does not arise in the Portuguese jurisdiction.

5.5 Public Disclosure

The issue does not arise in the Portuguese jurisdiction.

5.6 Other Significant Issues

Cybersecurity regulation in Portugal may be found in a number of different legal acts, particularly:

- Law No 46/2018 of 13 August, which transposed into national law the Directive (EU) 2016/1148 (Networks and Information Systems Directive); and
- Regulation (EU) 2019/881 (Cybersecurity Act).

The Portuguese regulator for the electronic communication industry (ANACOM) also issued Regulation 303/2019, published on April 1st, on the security and integrity of electronic communications networks and services.

A Cybercrime Law (Law No 109/2009, of 15 September) defines cybercrime offences and contains provisions on the surveillance of communications and electronic format evidence collection and seizure.

The *Centro Nacional de Cibersegurança* (CNCS) is the supervisory authority in Portugal with the role of monitoring compliance with the Portuguese law on cybersecurity rules and principles. Its legally defined mission is to “contribute to the free, reliable and secure use of cyberspace in Portugal, through the continuous improvement of national cybersecurity and international co-operation, in co-ordination with all competent authorities, and the implementation of measures and instruments required for the anticipation, detection, reaction and recovery of situations that, in the imminence of occurrence of incidents or cyber-attacks, may compromise the operation of critical infrastructures and national interests” (Article 2(2) of Decree Law No 3/2012, subsequently amended).

Morais Leitão, Galvão Teles, Soares da Silva & Associados (Morais Leitão) is a leading full-service law firm in Portugal with decades of experience, which is widely recognised for its work in several branches and sectors of the law at both national and international level. The firm's reputation amongst both peers and clients stems from the excellence of the legal services provided. Morais Leitão's work is characterised by its unique technical expertise, combined with a distinctive approach and

cutting-edge solutions that often challenge some of the more conventional practices. With a team comprising over 250 lawyers at its client's disposal, Morais Leitão is headquartered in Lisbon and has additional offices in Porto and Funchal. Due to its network of associations and alliances with local firms, and the creation of the Morais Leitão Legal Circle in 2010, the firm can also offer support through offices in Angola (ALC Advogados) and Mozambique (HRA Advogados).

Authors



Helena Tapp Barroso is a partner and a member of both the employment and pensions team and the data protection team. She also co-heads the insurance and reinsurance team. She joined the firm in 2006 and became a non-equity partner in 2010. Helena has wide experience in the

areas of labour and employment (including dispute regulation and litigation activity), and she has acted extensively on data protection and privacy issues. She provides legal assistance in drawing up personal data privacy and protection policies, and assessment and auditing programmes (including sector-specific issues for business areas such as insurance and insurance distribution, media, technology, banking and finance, retail and health), particularly in the GDPR context.



Tiago Félix da Costa is a partner, co-ordinator of the criminal and compliance team and head of the data protection team. He joined the firm in 2007 and became a partner in 2015. Recently, Tiago has acted increasingly in the personal data protection sector,

providing legal assistance on criminal and misdemeanour processes in this area and assisting several companies on the creation of policies and programmes for compliance in the personal data protection sector. Tiago is a member of the Portuguese Bar Association, regularly teaches postgraduates in different law faculties and has contributed to several publications relating to data protection law.

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Rua Castilho, 165
1070-050 Lisboa

Tel: +351 21 381 74 00
Fax: +351 21 381 74 99
Email: mlgtslisboa@mlgts.pt
Web: www.mlgts.pt

M
L **MORAIS LEITÃO**
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS