Practical Law™

# Data protection in Portugal: overview

- Resource type: Country Q&A
- Status: Law stated as at 01-Jul-2014
- Jurisdiction: Portugal

A Q&A guide to data protection in Portugal.

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data. This article also details the national regulator; its enforcement powers; and sanctions and remedies.

To compare answers across multiple jurisdictions, visit the Data Protection Country Q&A tool.

This article is part of the multi-jurisdictional guide to data protection. For a full list of contents, please visit www.practicallaw.com/dataprotection-mjg.

*Magda Cocco* and *Isabel Ornelas*, *Vieira de Almeida & Associados – Sociedade de Advogados, RL*

## Contents

Magda Cocco, Partner
Isabel Ornelas, Associate

## Regulation

### Legislation

#### 1. What national laws regulate the collection and use of personal data?

**Specific laws**

Specific laws regulate certain areas, such as the electronic communications sector, including the:

- Law governing the processing of personal data in the context of publicly available electronic communications networks and services (Law 41/2004 of 18 August, which implemented Directive 2002/58/EC on the protection of privacy in the electronic communications sector, as amended by Law no. 46/2012, transposing Directive no. 2009/136/EC of the European Parliament and Council, of 25 November).
- Law 32/2008, of 17 June, which implemented Directive 2006/24/EC of the European Parliament and Council of 15 March 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks.

**Scope of legislation**

#### 2. To whom do the laws apply?

As a general rule, only individuals or entities established in Portugal are subject to the rules and provisions of the Data Protection Law.

#### 3. What data is regulated?

Personal data includes any type of information (including sounds and images) relating to an identified or identifiable natural person (*Data Protection Law*).

Personal data concerning any of the following is considered sensitive data:

- Philosophical or political beliefs.
- Political party or trade union membership.
- Religion.
- Private life.
- Racial or ethnic origin.
- Health or sex life, including genetic data.

## 4. What acts are regulated?

Portuguese law sets out a very broad concept of data processing: any operation or use involving personal data is considered to be data processing. This includes the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction of personal data.

## 5. What is the jurisdictional scope of the rules?

Generally, only individuals or entities established in Portugal are subject to the Data Protection Law.

## 6. What are the main exemptions (if any)?

The Data Protection Law can also apply to data processing by companies or individuals with a head office or residence outside of Portugal in the following situations:

- If the processing is carried out in the context of an activity by an establishment of the controller in Portugal.
- If the controller is not established in Portugal, but is established in a location where Portuguese law applies by virtue of international public law.
- If the controller is not established in the European Union (EU) and for the purposes of processing personal data, makes use of equipment (automated or otherwise) situated in Portugal. This is unless the equipment is only used during transit through EU territory.

### Notification

## 7. Is notification or registration required before processing data?

The Data Protection Law requires notification to the Data Protection Authority (*Comissão Nacional de Protecção de Dados*) (CNPD) (*The regulatory authority*) before carrying out any personal data processing, intended to serve a single purpose or several related purposes.

In some situations, prior authorisation from the CNPD is required, such as when processing:

- Sensitive data.
- Personal data related to the credit and solvency of the data subjects.
- A combination of various personal data.
- A personal data transfer to foreign countries.

CNPD has issued decisions exempting some data processing operations from prior notification, including data processing related to billing, contact with clients, and processing

payments. However, these exemptions only apply if the type of processing relates to the type established as exempted in the applicable decision.

## Main data protection rules and principles

### Main obligations and processing requirements

#### 8. What are the main obligations imposed on data controllers to ensure data is processed properly?

In general terms, data controllers must ensure that personal data is, for the purposes for which it was collected and is processed:

- Processed lawfully and respects the principle of good faith.
- Collected for specified, explicit and legitimate purposes and is processed in a way that is compatible with these purposes.
- Adequate, relevant and not excessive.
- Accurate and where necessary, kept up-to-date. Adequate measures must be taken to ensure that inaccurate or incomplete data is erased or rectified.
- Kept in a form that allows identification of its data subjects for no longer than is necessary.

#### 9. Is the consent of data subjects required before processing personal data?

In order to process personal data, it is necessary to obtain the data subject's prior consent. The form of consent must contain:

- The personal data to be collected.
- The purposes of the collection.
- The data controller's identity.
- Information on the right of access, rectification and elimination, and also the means by which these rights can be exercised.
- Information on the transfer of data and its identification (if applicable).
- The countries where the data may be transferred to.

The Data Protection Law does not contain any specific rule regarding the provision and handling of online consent. However, online consent is given where it is considered an 'explicit consent' and can be related to a specific data subject.

There is also no specific rule concerning information on minors. However, under the general rules set out in the Portuguese Civil Code, children under 18 years of age have limited legal capacity and therefore a case by case evaluation should be carried out to evaluate if consent is

within the scope of their admissible capacity. Otherwise, a child's legal representative must provide the consent.

### 10. If consent is not given, on what other grounds (if any) can processing be justified?

The data subject's prior consent is not needed when the processing is required:

- For the performance of a contract which the data subject is party to, or in order to take steps at the data subject's request before entering into a contract or a declaration of his will to negotiate.
- To comply with a legal obligation that the controller is subject to.
- To protect the data subject's vital interests if he is physically or legally incapable of providing consent.
- To perform a task carried out in the public interest or in the exercise of official authority vested in the controller, or in a third party to which the data is disclosed.
- To pursue the legitimate interests of the controller or of a third party to which the data is disclosed. This is with the exception of interests that are overridden by the data subject's fundamental rights, freedoms and guarantees.

Special rules apply in the context of sensitive data (*See Question 11*).

**Special rules**

### 11. Do special rules apply for certain types of personal data, such as sensitive data?

As a rule, processing sensitive data is prohibited. However, under a legal disposition or by obtaining the CNPD's prior authorisation, processing sensitive data is permitted when either:

- The processing is essential for the exercise of the data controller's legal or statutory duties, based on important public interest grounds.
- The data subject has given his prior explicit consent.

In both of the above situations, the data controller must ensure that special security measures are adopted and guarantee that the processing is not discriminatory.

Processing sensitive data is also allowed when one of the following conditions is met:

- The processing is necessary to protect the rights of the data subject or another person, when the data subject is legally or physically incapable of providing consent.
- The processing is carried out with the data subject's consent, in the course of its legitimate activities with appropriate guarantees, by a foundation, association or any other non-profit body with a political, philosophical, religious or trade union aim. This is provided that the

processing relates solely to the members of the body or to persons who have regular contact with it, and data is not disclosed to a third party without the consent of the data subjects.
- The data being processed has been noticeably made public by the data subject, provided the data subject's consent can reasonably and adequately be assumed through his actions.
- The processing is necessary to establish, exercise or defend legal claims.

The processing of data relating to health and sex life, including genetic data, is permitted when it is required for the purposes of:

- Preventative medicine.
- Medical diagnosis.
- The provision of care or treatment.
- The management of healthcare services.

Where the data is processed by a health professional, subject to national law, the CNPD must be notified and the necessary security measures adopted.

The processing of data relating to illegal activities, offences and criminal convictions can only be carried out with prior authorisation from CNPD. This is only permitted where the processing is necessary to pursue the data controller's legitimate purposes (Data Protection Law).

## Rights of individuals

### 12. What information should be provided to data subjects at the point of collection of the personal data?

Data controllers must provide data subjects with the following information:

- Identification of the data controller and his representative.
- The purposes of the processing.
- Other information including:
  - the recipients or category of recipients;
  - whether the replies are obligatory or voluntary, and the consequences of failure to reply;
  - the existence and terms in which the rights of access and rectification may be exercised by the data subject.

If the data is collected on an open network, the data subject must be informed that their personal data may be circulating throughout the network with no security measures in place. They must be informed that their personal data is at risk of being seen and used by unauthorised third parties.

### 13. What other specific rights are granted to data subjects?

The data subject has rights of access, rectification and objection (*Data Protection Law*).

**Access rights**

The data subject has the right to obtain from the controller, without constraint, within a reasonable term and without excessive delay or expense, the following:

- Confirmation of whether or not his personal data is being processed, and information on the:
  - purposes of the processing;
  - categories of data involved;
  - recipients or categories of recipient to whom the data is disclosed.
- Information, in an intelligible form, concerning the data processed and any available information about its source.
- An explanation of the logic used for any automatic processing of the data.

**Rectification rights**

The data subject has the right to ask the data controller:

- To rectify, remove or block data when the data processing does not comply with the provisions set out in the Data Protection Law (particularly if the data is incomplete or inaccurate).
- For notification of any data that has been rectified, removed or blocked to third parties to which the data may have been disclosed (unless notification proves impossible).

**Objection rights**

The data subject has the right to:

- Object to the processing of his personal data, at any time, if there are compelling legitimate grounds relating to his particular situation. The controller can only continue processing the data if it is needed to pursue the legitimate interests of the controller or a third party, unless otherwise provided by law. The data subject's fundamental rights and freedoms can potentially override this.
- Object to the processing of his personal data which the controller anticipates being processed for the purposes of direct marketing (and to which the data subject had provided prior express consent). The data subject can make this objection without incurring any charges.

## 14. Do data subjects have a right to request the deletion of their data?

Data subjects have a legal right to request the deletion of their data. If such a request is made, the data controller must comply promptly and without unnecessary delay, expense or imposition on the data subject. In the event that deletion is not possible (most typically, when data controllers are bound by law or regulation to retain the personal data for a particular period of time and for specific purposes), the data subject must be duly informed.

The data subject also has the right to be informed of the consequences of deleting the data. For example, if the deletion of data will make it impossible to provide a service to the data subject.

## Security requirements

### 15. What security requirements are imposed in relation to personal data?

The data controller must implement appropriate technical and organisational measures to protect personal data against:

- Accidental or unlawful destruction or loss.
- Accidental change or modification.
- Unauthorised disclosure or access to the data, particularly where the data is transmitted over a network.
- All other unlawful measures of processing.

For the processing of sensitive data, the data controller must adopt appropriate measures to:

- Prevent unauthorised persons from entering the premises used to process the data.
- Prevent the media on which personal data is stored from being read, copied, altered or removed by unauthorised persons.
- Prevent unauthorised input and unauthorised information gathering, alteration or elimination of personal data input.
- Prevent automatic data processing systems being used by unauthorised persons at data transmission premises.
- Guarantee that only authorised persons can access data covered by the authorisation.
- Guarantee inspection of the bodies that receive the personal data transmitted from data transmission premises.
- Guarantee that it is possible to check (within a reasonable period of time) where, when and by whom the data was input.
- Prevent unauthorised reading, copying, alteration or elimination of data when transmitting personal data and transporting data media.

CNPD can waive some of these security measures, provided the data controller guarantees that the data subjects' fundamental rights are complied with.

### 16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

In Portugal this rule currently applies in the electronic communications sector, without prejudice to any rules implemented by the anticipated EU Regulation.

In the electronic communications sector it is necessary to notify the CNPD in the event of a data breach. In addition, if the data breach is likely to negatively affect the data subjects (that is, the users or subscribers), companies must also notify the data subjects. This is so they may take the appropriate measures, if the breach results in identity theft, bodily harm, humiliation or reputational damage.

## Processing by third parties

### 17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

When the data controller employs a processor, the processor must provide sufficient guarantees concerning the technical security and organisational measures regulating the processing. In addition, the processing must be regulated by an agreement or legal act.

This agreement must establish that the processor is acting on behalf of the data controller and following his instruction. The processor must also comply with the security obligations.

## Electronic communications

### 18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The legal terms for the use of cookies and their data privacy implications have been set out in the laws concerning privacy in the electronic communications sector (*see Question 1, Specific laws*).

The current rules determine that the use of cookies requires express and informed consent (opt-in) from data subjects (an opt-out option is not sufficient). Therefore data controllers must obtain consent and provide clear, adequate and complete information regarding the purpose of their use of cookies.

The only exception to this general opt-in rule is when the storage or access is technically and strictly necessary for the legitimate purpose of allowing access to a service that has been specifically and expressly requested by the data subject (that is, the subscriber or user).

### 19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

The basic rule regarding commercial communications is that the data subject's prior express consent must be obtained. Therefore consent must be obtained before the following are used for direct marketing purposes:

- Automatic calling machines.
- Facsimile machines.
- E-mail.
- Short message service or enhanced messaging service.

Entities carrying out unsolicited direct marketing communications must maintain a list of persons:

- Not wanting to receive such communications.
- Who have expressly accepted receiving such communications.

Such entities must also routinely check the public opt-out list that is maintained by the General Consumer Officer (*Direção Geral do Consumidor)* and available through their website *www.consumidor.pt/*.

## International transfer of data

**Transfer of data outside the jurisdiction**

**20. What rules regulate the transfer of data outside your jurisdiction?**

Data transfer to other countries within the EU does not require prior authorisation from the CNPD.

Data transfer to countries outside the EU can only take place in compliance with the Data Protection Law. In addition, the receiving state must also provide an adequate level of protection. This is assessed in light of all the circumstances surrounding the data transfer operations in force in that state and its professional rules and security measures, including the:

- Nature of the data.
- Purpose and duration of the proposed processing operation(s).
- Country of origin and country of final destination.
- Rules of law (both general and sectorial).

If the receiving state does not ensure an adequate level of protection, the CNPD can allow the transfer if the data subject has given clear consent to the proposed transfer, or if 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 in response to the data subject's request.
- Necessary for the performance or conclusion of a contract between the controller and a third party that is concluded, or to be concluded, in the data subject's interests.
- Necessary or legally required on important public interests grounds, or to establish, exercise or defend legal claims.
- Necessary to protect the data subject's vital interests.
- Made from a register which is intended to provide information to the public and is open to consultation, either by the public or by any other person who can demonstrate a legitimate interest, provided the conditions laid down in law for consultation are fulfilled.

In addition, the CNPD can authorise a transfer or a set of transfers of personal data to a receiving state that does not provide an adequate level of protection. This can only be achieved if the controller provides adequate safeguards to protect the privacy and fundamental rights and freedoms of individuals. This can be through appropriate contractual clauses or if a transfer to the US, by adhering to the Safe Harbour Privacy Principles.

**Data transfer agreements**

**21. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?**

The European Commission (Commission) has approved the following (depending, respectively, if the recipient acts as a data processor or a third party):

- Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third parties.
- Decision 2002/16/EC on standard contractual clauses for the transfer of personal data to processors established in foreign countries.
- Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in foreign countries, replacing Decision 2001/497/EC, which is effective as of 15 May 2010.

The transfer of data to the US requires prior approval from the CNPD. The company receiving the data can simplify the process by adhering to the Safe Harbour Privacy Principles issued by the US Department of Commerce. If Safe Harbour certification is not obtained or the EU Standard Contractual Clauses is not put in place, CNPD approval is required. Otherwise, a mere notification will be sufficient for the data transfer.

**22. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?**

The transfer of personal data to an EU member state does not require the data subject's prior consent, although the data subject must be given information on the transfer.

When transferring to a state where an adequate level of protection cannot be guaranteed, the data subject's consent is not required if the parties have entered into an agreement containing the standard contractual clauses approved by the Commission. If such an agreement has not been entered, the data subject's consent is required. Likewise for the USA, if the receiving party is Safe-Harbour certified (in which case, consent is not necessary).

### 23. Does the relevant national regulator need to approve the data transfer agreement?

If the contractual clauses approved by the Commission have been adopted, the CNPD is only required to confirm whether the transfer of personal data is made in accordance with those clauses.

## Enforcement and sanctions

### 24. What are the enforcement powers of the national regulator?

The CNPD is the national authority with the power to supervise and monitor compliance with data protection laws and regulations. In particular, the CNPD has:

- Investigative powers, such as powers:
  - of access to data forming the subject matter of processing operations;
  - to collect all the information necessary for the performance of its supervisory duties.
- Effective powers of intervention, such as:
  - ordering the blocking, deletion or destruction of data;
  - imposing a temporary or definitive ban on processing, even if data is included in open networks in servers located in Portugal.
- Powers of delivering opinions before processing operations are carried out and ensuring the appropriate publication of such opinions.
- Powers to engage in legal proceedings where the Data Protection Law provisions have been violated, or to bring these violations to the attention of the judicial authorities.
- Powers to authorise the data processing notified by data controllers.

### 25. What are the sanctions and remedies for non-compliance with data protection laws?

**Financial penalties**

The CNPD can impose fines if the data controller, inter alia:

- Negligently fails to comply with the obligation of notifying the CNPD about the processing of personal data.
- Provides false information.

- Complies with the obligation to notify without observing the request of information or, having been notified by CNPD, continues to allow access to open data transmission networks to controllers who fail to comply with the provisions of the Data Protection Law.

The CNPD can apply the following fines:

- For a natural person: a minimum of EUR249.40 and a maximum of EUR2, 493.99.
- For a legal person or a body without legal personality: a minimum of EUR1, 496.40 and a maximum of EUR14, 963.94.

The limits above can be doubled to an approximate maximum value of EUR30, 000, if the data processing was subject to the CNPD's authorisation, as is the case with sensitive data (*see Question 11*).

In the electronic communications sector, breaching certain rules is also considered to be an administrative offence, punishable with a fine of up to EUR5 million when committed by a legal person.

**Civil and criminal liability**

The data controller can also incur civil or criminal liability. Any person who intentionally does not comply with obligations relating to data protection is liable for up to one year imprisonment or a fine of up to 120 days per offence, when he:

- Omits to notify or apply for authorisation from the CNPD before carrying out any operation that wholly or partly involves data processing, or a set of these operations intended to serve a single purpose or several related purposes.
- Provides false information in the notification process, or in applications concerning the authorisation to process personal data, or makes alterations to the data that are not allowed.
- Misappropriates or uses personal data in a manner that conflicts with the purpose of the collection, notification or authorisation process.
- Promotes or carries out an illegal combination of activities using personal data.
- Fails to comply with the obligations provided under the Data Protection Law and other data protection legislation within the period determined by the CNPD.
- Continues to allow controllers access to open data transmission networks when:
- the controller has failed to comply with the provisions of the Data Protection Law; and
- the CNPD has notified the person not to permit access to such a controller.

The above limits can be increased to up to double the maximum amount when the processing of personal data is connected to sensitive data or relating to:

- Persons suspected of illegal activities, criminal and administrative offences.
- Credit and the solvency of the data subjects.

In addition, if any person accesses certain personal data when prohibited from doing so without proper authorisation, that person is liable for up to one year's imprisonment or a fine of up to 120 days per offence. The limits of this penalty are also doubled when the access:

- Is achieved by violating technical security rules.
- Allows the agent or third parties to obtain knowledge of the personal data.
- Provides the agent or third parties with a benefit or material advantage.

The CNPD can also apply additional penalties, such as blocking or destroying the data, the temporary or permanent prohibition of personal data processing, or publishing the judgment (*Data Protection Law*).

Generally speaking the usual penalties are those related to entities that negligently fail to comply with the obligation to notify CNPD regarding data processing.

## Regulator details

**Portuguese Data Protection Authority (*Comissão Nacional de Proteção de Dados*)**

**W** www.cnpd.pt

**Main areas of responsibility.** The CNDP is the authority responsible for supervising and enforcing compliance with the data protection provisions in Portugal. It has powers to investigate, intervene, deliver opinions, engage in legal proceedings, and authorise data processing.

## Contributor profiles

**Magda Cocco, Partner**

**Vieira de Almeida & Associados**

**T** +351 21 311 3519/ 3487
**F** +351 21 352 2239
**E** mpc@vda.pt
**W** www.vda.pt

**Professional qualifications.** Law Degree, University of Lisbon

**Areas of practice.** Telecommunications; privacy, data protection & cybersecurity practice; media and IT operations,

**Recent transactions**

- Ongoing assistance to several clients regarding the adaptation to the anticipated new EU Regulation.
- Assistance in the drafting of the full package of the new telecommunications and ICT draft legislation to be implemented in Angola (including data privacy).
- Negotiation of several procurement procedures and definition of public policies regarding privacy, cybersecurity and critical infrastructure.
- Assistance in the set-up, design and implementation of technologically sophisticated projects.
- Several data protection compliance programs.

**Languages.** Portuguese, English, Spanish, French

**Professional associations/memberships.** Member of the Portuguese Bar Association, visiting Professor/ Lecturer of Telecommunications Law and Regulation and Privacy and Data Protection at the Catholic University of Lisbon and at the LLM in Public Law at the Management School of Lisbon; Core Member of the Group of Permanent Security in the Society of Information and the Portuguese Association for the Development of the Society of Information. Member of Portuguese Association for the Development of Communications (*Associação Portuguesa para o Desenvolvimento das Comunicações)* (APDC).

**Publications**

- Aspen Publishers (Global Privacy and Security Law Book)
- PLC Cross-Border Handbooks (Data Protection)
- Iberian Lawyer
- Privacy Law and Business
- IT Law Group (Global Privacy and Security Law Chapters for Portugal)

**Isabel Ornelas, Associate**

Practical Law™

**Vieira de Almeida & Associados**

**T** +351 21 311 3519/ 3487
**F** +351 21 352 2239
**E** igo@vda.pt
**W** www.vda.pt

**Professional qualifications.** Law Degree, University of Lisbon, Faculty of Law

**Areas of practice.** Telecommunications; privacy; data protection & cybersecurity.