Practical Law™
GLOBAL GUIDE 2017
DATA PROTECTION

Data protection in Portugal: overview

Helena Tapp Barroso, João Alfredo Afonso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados – Sociedade de Advogados

global.practicallaw.com/2-575-2225

REGULATION
Legislation

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

General laws

The provisions of Directive 95/46/EC on data protection (Data Protection Directive) were implemented into Portuguese law through Law 67/98 of 26 October 1998 (Data Protection Act). The fundamental principles and guarantees on personal data protection are also set out in the Portuguese Constitution (*Article 35 on the use of computerised data*).

Sectoral laws

Sectorial laws or regulations can also be found in Portugal. These laws include the rules applicable to the electronic communication (telecom) sector as contained in Law 41/2004 of 18 August 2004, which implemented Directive 2002/58/EC on the protection of privacy in the electronic communications sector (E-Privacy Directive) (as amended by Law 46/2012 of 29 August 2012 implementing Directive 2002/22/EC on universal service and users' rights (Universal Service Directive) and Regulation (EU) 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC).

The provisions of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive) (amending the E-Privacy Directive) have also been implemented into Portugal through Law 32/2008 of 17 June 2008 on the retention and transfer of personal data for the purposes of the investigation, detection and prosecution of serious crime by competent authorities.

The processing of personal genetic and health information is also subject to sector-specific legislation under Law 12/2005 of January 26 (as amended) and Decree-law 131/2014 of 29 August.

Scope of legislation

2. To whom do the laws apply?

In Portugal, the Data Protection Act (DPA) applies to both public and private entities.

Video surveillance and other forms of personal data collection, processing and broadcasting consisting of sound or image also fall with the definition of personal data processing and are subject to the DPA's provisions, whenever the controller is established in Portugal or uses a network access provider established in Portuguese territory.

The provisions of the DPA also apply to the processing of personal data regarding public security, national defence and state security, without prejudice, however, to any special rules set out in international law instruments to which Portugal is bound or any specific domestic laws.

3. What data is regulated?

Personal data

The Data Protection Act (DPA) defines personal data as "any information relating to an identified or identifiable natural person, regardless of its support, including sound and image". A natural person is deemed to be identifiable when he/she can be directly or indirectly identified, including by reference to an identification number or to one or more features that are specific to his/her physical, physiological, mental, economic, cultural or social identity.

Sensitive personal data

In the DPA, sensitive data refers to personal data that reveals any of the following information regarding the data subject:

- Philosophical or political beliefs.
- Political party or trade union membership.
- Religious beliefs.
- Private life (privacy).
- Racial or ethnic origin.
- Health or sex life (including genetic personal data).
- Suspicion of illegal activities, criminal or administrative offences and decisions applying criminal penalties, security measures, administrative fines or additional conviction measures.

4. What acts are regulated?

All operations qualifying as personal data processing are covered by the provisions of the Data Protection Act. These include all operations performed upon personal data (whether or not my automatic means). This includes data collection, recording, organisation, storage, data adaptation or alteration, data retrieval, data consultation, use and data disclosure by transmission, dissemination or by any other means of making data available as well as data alignment or combination and data blocking, erasure or destruction.

5. What is the jurisdictional scope of the rules?

The provisions of the Data Protection Act (DPA) cover the processing of personal data carried out by entities located within Portuguese territory or where Portuguese law applies by virtue of international public law.

The provisions of the DPA also apply to the processing of personal data carried out by entities established outside the EU that use a means of automated or non-automated processing that is located within Portuguese territory. The only exclusion being cases where such means or equipment, although located in Portugal, serves only for mere data transit purposes to allow data to pass through the country.

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

The Data Protection Act provides an exemption for personal data processing for cases where the processing was carried out by natural persons in the course of purely personal or domestic activities.

Notification

7. Is notification or registration required before processing data?

Before processing personal data, the controller must notify the national data protection authority, the National Commission for the Protection of Data (*Comissão Nacional de Protecção de Dados*) (CNPD).

For the processing of sensitive personal data or data relating to credit or solvency information on the data subjects, and for data alignment or combination not provided for in a legal instrument, prior authorisation from the CNPD is required. The same applies to the use of personal data for purposes different from those which determined the data collection.

The CNPD has issued limited scope decisions that exempt the controller from prior registration or authorisation to process certain pre-defined categories of data for a few specific purposes. These include (among others):

- The processing of specific categories of employee data for payroll purposes or
- The processing of client data for invoicing purposes.

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?

The main obligation on data controllers to ensure that data is processed properly derives from the following principles, which are explicitly set out in the Data Protection Act:

Personal data must be:

- Processed lawfully and fairly (subject to a bona fide principle rule).
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and non-excessive for the purposes for which they are collected and subsequently processed.
- Accurate and, where necessary, updated. Reasonable steps must be taken to ensure that where personal data is inaccurate or incomplete (having regard to the purposes for which they were collected or further processed) is erased or rectified.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was collected or subsequently processed.

The data controller must also ensure that personal data is processed in a manner that ensures appropriate security of the data, including protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage, by using the appropriate technical or organisational measures.

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

Consent of the data subject is not always required prior to processing. For example, the data subject's prior consent is not required when the processing is required for:

- The performance of a contract or contracts to which the data subject is party or in other to take steps, at the data subject's request, prior to entering into a contract or declaring his/her will to negotiate.
- Compliance with a legal obligation, other than a contractual obligation.
- The protection of vital interests of the data subject him/herself if he/she is physically or legally incapable of providing consent.
- Carrying out public functions.
- Pursuing the legitimate interests of the data controller (such as the employer) (or third parties to whom the data is disclosed), unless overridden by the individual's (such as an employee's) fundamental rights, freedoms or guarantees.

There are no specific rules concerning consent by minors.

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

In the case of non-sensitive data, the following grounds, other than the data subject's consent, allow legitimate processing:

- Performance of a contract or contracts to which the individual is a party.
- Completion of pre-contractual steps, at the request of the individual, prior to entering into a contract or declaring his/her will to negotiate.
- Compliance with legal obligations impending over the data controller.
- Protection of vital interests belonging to the individual in cases where the latter is physically or legally incapable of providing consent.
- Performance of task carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party entity to whom such data is disclosed.
- Need resulting from legitimate interests of the data controller (or third parties to whom the data is disclosed), unless overridden by the data subject's fundamental rights, freedoms or guarantees.

Special rules

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

The processing of sensitive data is restricted. Only under express legal disposition or upon prior authorisation granted by theNational Commission for the Protection of Data (CNPD) can such data be processed. In such cases, one of the following grounds for processing must occur:

- Explicit consent provided by the relevant data subject.
- The need to accomplish a task carried out in the public interest and in the exercise of legal or statutory role vested in the data controller.
- Protection of vital interests belonging to the data subject, in cases where the subject is incapable of providing consent for physical or legal reasons.
- The data has been clearly made public by the data subject in terms that allow consent to be clearly inferred.
- Legal proceeding requirements (court proceedings) for the exercise of legal rights.

In the case of (sensitive) data relating to health or sex life, including genetic data, processing is also allowed when required for preventive medical reasons, for diagnosis or to provide medical care or to manage health care-services. The data controller must maintain adequate systems to guarantee logical separation between data relating to health and sex life, including genetic information, and any other personal data.

When processing sensitive data, the data controller must maintain specifically appropriate measures to:

- Guarantee premise entry control.
- Prevent data from being read, copied, altered, removed, used or transferred by unauthorised persons.
- Prevent any unauthorised data input, change or deletion from occurring.
- Restrict the access of authorised persons to the data within the limits processing authorised by the authority.
- Guarantee the recipient entity verification in case of sensitive data transmission.
- Provide for logs being kept for sensitive data input control.

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 the following information to data subjects upon collecting personal data directly from same subjects or at any time before:

- The identity of the data controller.
- The purposes for processing the data.
- Other relevant information including, at least, the following.
- Data recipients or category of recipients.
- Statutory or voluntary nature of responses for data required from the subject (and consequences of not providing response).
- Information that the data may circulate on the network without security measures and may be at risk of being seen or used by unauthorised third parties, when the data collection is made on an open network.
- Information on the subjects rights of access to and correction of his/her personal data.

If the data is not obtained by the controller directly from the data subject, the required information must be provided by the controller when (or before) the first processing operation takes place.

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

Data subjects have the rights of access, amendment (and updating) and objection to processing.

The right of access entitles the data subject to obtain from the controller, without restrictions, excessive delay or expense, all of the following:

- Confirmation on data being processed (that is, confirmation of the data processing purpose, data categories and information on data recipients or categories of recipients).
- Indication in an intelligible form of the data under processing and data source.
- Explanation of the logic underlying any automated processing of the relevant data.
- Rectification, erasure or blocking of data processed in breach of the provisions of the Data Protection Act.
- Notice to third parties to whom the data has been disclosed of any data rectification, deletion or blocking, except if not possible.

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

Data subjects can request the deletion of their data if the data being processed is incomplete or inaccurate, or where the data is being processed in terms that are not compatible with legitimate grounds and purposes of the data controller.

SECURITY REQUIREMENTS

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

Data controllers must put in place appropriate technical and organisational measures to protect data against:

- Accidental or unlawful destruction.
- Accidental loss or alteration.
- Unauthorised disclosure or access.
- Any other unlawful forms of processing.

The level of security required must be appropriate in view of the risks represented by the relevant processing activity and the nature of the data being processed. The appropriateness of this is measured taking into account the state of the art and the cost required for their implementation.

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

The Data Protection Act does not provide a requirement to notify personal data security breaches to the local data protection authority or to data subjects. However, in the electronic communications sector, there is a requirement for entities to notify specific breaches to the national regulator, the National Commission for the Protection of Data.In addition, in this sector data breaches must be notified to the relevant data subject if the breach is likely to have an adverse effect on him/her. This would be the case if the data security breach would, for example, likely cause identity fraud/theft, physical or reputational damage, or humiliation to the individual.

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 a third party (third-party processor) processes data on behalf of the data controller, it must only act on instructions from the data controller, unless required to act by law. The third-party processor must enter into a contract with the controller subject in written form. The contract (or equivalent) must be a mutually binding instrument that must contain provisions ensuring that the third-party processor is bound to act only on instructions from the data controller. The contract must also contain provisions guaranteeing that relevant security measures are also incumbent on the processor.

When selecting a third-party processor, the controller must ensure that the selected entity provides sufficient guarantees in relation to carrying out the required technical and organisational security measures. Compliance by third-party processors with the relevant measures must be ensured by the data controller.

ELECTRONIC COMMUNICATIONS

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

Under the local provisions implementing the E-Privacy Directive, the use of cookies requires consent from the relevant data subject. The data subject must be provided with clear and comprehensive information both on the use of cookies and on the categories of processed data and processing purposes. The clarity of this information is a precondition to the effective and valid consent.

There is no express provision on whether the data subject's consent may or may not be obtained on the basis of a mere opt-out system. The tendency, however, is moving towards opt-in solutions.

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

For natural persons, the receipt of unsolicited electronic commercial communications must be limited to cases where prior explicit consent is provided by the data subject. However, for legal persons, such communications can be sent without prior consent, but the legal person can express its opposition to receiving such communications, in which case no further unsolicited electronic commercial communications can be sent.

There is an exception to the above rule, since a controller that has obtained the electronic contact of its customers, in the context of the sale of products or services, may use the customer's contact details for commercial communications of the products marketed by the controller or similar ones. The controller must, nevertheless, provide the customers with the opportunity to object to such unsolicited communications, in an easy and free-of-charge manner. This must be done both at the time the contact data is collected and on the occasion of each commercial message that is sent.

A valid option to object to future communications must always be provided in all commercial communication sent and updated lists of subjects that have consented (or not objected) to this use must be kept at all times.

INTERNATIONAL TRANSFER OF DATA

Transfer of data outside the jurisdiction

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

Companies and any other categories of data controllers can transfer data they process within the territory of EU member states and EEA member countries. However, transfers outside the EU/EEA is restricted.

Transfer to a third country (that is, a non-EU or non-EEA country) is only permitted when the destination jurisdiction:

- Is compliant with the Data Protection Act's general processing requirements.
- Ensures an adequate level of protection assessed in the light of all the circumstances that surround the relevant transfer operation. Circumstances such as the nature of data being transferred, the purpose and duration of the intended processing, the country of final destination and the legal system and privacy rules in force therein and the professional rules and security measures complied with in such country will all be relevant for this assessment.

If an adequacy decision has been issued by the European Commission on the place of destination for the third country transfer, which acknowledges that the destination jurisdiction will ensure an adequate level of protection by reason of the ruling domestic law or of international commitments that have been undertaken, then transfer will be allowed. Transfer may also occur under contractual terms if these conform to the model clauses approved by the European Commission (*see Question 22*).

"Binding Corporate Rules" are not accepted by the National Commission for the Protection of Data as a basis for the data export to a third country.

Data transfers to the US can be done under the EU-US Privacy Shield framework following the adoption, on 12 July 2016, of the European Commission decision on the EU-US Privacy Shield.

Transfer may also take place, subject to the authority's prior authorisation, if a derogation case applies. This would be the case where there is either:

- Unambiguous consent of the data subject to the proposed transfer.
- The need for transfer based on one of the following cases:
  - contract (between the data subject and the controller) or implementation of pre-contractual measures requested by the subject;
  - contract between the data subject and a third party, in the interest of the subject;
  - legal proceedings; or
  - protection of the subject's vital interests.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

Under the Data Protection Law, there is no requirement to store any type of personal data in Portugal.

Data transfer agreements

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

The standard form transfer agreements adopted in Portugal are those that constitute the standard model clauses approved by the European Commission.

The National Commission for the Protection of Data has also issued guidelines stating that entities within a single corporate group may enter into a single intragroup agreement involving all entities. This single agreement will allow the export of data provided it is structured in line with the standard form model clauses.

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

Prior notification (registration) is required considering that data transfer qualifies, in itself, as data processing. If the transfer of sensitive data is at stake, mere registration will not be sufficient and prior authorisation will be required.

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

All data processing requires prior notification to, or when the processing (including the transfer) relates to sensitive data, prior authorisationfrom theNational Commission for the Protection of Data) (CNPD). In the case of cross-border transfers to non-EU or non-EEA member states, the data controller owner must provide information to the CNPD that transfer of the data to a third country is envisaged. When filing the notification (or authorisation) request, the controller must indicate to the CNPD the framework that allows such transfer (for example, the standard model clauses approved by the European Commission (*see Question 22*), EU-US Privacy Shield (*see Question 20*), Intragroup Agreement and so on).

There is no specific agreement approval as such.

ENFORCEMENT AND SANCTIONS

25. What are the enforcement powers of the national regulator?

TheNational Commission for the Protection of Data (CNPD) is authorised to request information from data controller on any data processing activities being performed. The CNPD also has the right to access the computer systems that support the data processing operations and all documents relating to the data processing and transmission in the context of the authority's responsibilities.

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

Administrative sanctions

Both administrative sanctions or orders and criminal penalties can arise from data breaches or other violations of the Data Protection Act (DPA).

The DPA sets two different levels of fines (which are subdivided into a further two levels of fines for each group) depending on the seriousness of the misdemeanour offence.

For less serious administrative offence acts or omissions, the applicable fines range from EUR498.79 to EUR4,987.97. However, this limit is doubled in the case of specific offences (that is where data is processed without having obtained the data subject's unambiguous consent, except for cases where other legal grounds allow processing and, therefore, such consent is not required).

For more serious offences, the value of the fines is set to three times the amounts indicated above for less serious offences (*see above*). These include offences such as failing to comply with the obligation to notify the competent data protection authority. These amounts are doubled if the offence involves sensitive data.

Sector-specific legislation in the electronic communication sets much higher administrative fines for data protection law breaches, with fines in this sector fixed up to a maximum of EUR5 million.

Criminal sanctions

The DPA also establishes criminal sanctions. Criminal sanctions will apply in cases where the data controller has:

- Intentionally omitted a notification or authorisation application with the competent authority, where applicable.
- Intentionally provided false information to competent authority.
- Intentionally misappropriated personal data.
- Used undue (and unauthorised) access (by any means) to gain personal data that was prohibited to the offender.
- Unauthorised erased, destroyed, damaged, deleted or changed personal data, making it unusable or affecting its capacity for use.
- Breached the legal duty of confidentiality towards personal data.

Criminal offences are punished by a prison sentence of up to two years or a 240-day fine, both of which can be doubled in aggravating circumstances.

REGULATOR DETAILS

National Commission for the Protection of Data (*Comissão Nacional de Protecção de Dados*) (CNPD)

W *www.cnpd.pt/english/index_en.htm*

Main areas of responsibility. The main areas of responsibility of the CNPD include:

- Supervising and monitoring compliance with the laws and regulations regarding privacy and personal data processing.
- Using investigative powers related to any data processing activity.
- Exercising powers of authority which may include the powers to enforce data blocking, erasure or destruction or to impose temporary or permanent processing bans.
- Issuing public compliance warnings to data controllers.
- Imposing fines.
- Reporting criminal offences (to privacy) for prosecution and pursuing measures to provide evidence of such offences having been purported.

ONLINE RESOURCES

National Commission for the Protection of Data (*Comissão Nacional de Protecção de Dados*) (CNPD)

W *www.cnpd.pt/english/index_en.htm*

Description. Official website of the PNPD. Contains up-to-date information on the legal frame, guidelines and main decisions issued by the CNPD. It also contains a public registration of processing activities filed or processing operations authorised by the CNPD, but information may be incomplete or partially unavailable. This website also provides the online forms for controllers to fill in and submit prior registration or authorisation requests. Translations are available for guidance only and the English-language version is not binding.

Practical Law **Contributor profiles**

Helena Tapp Barroso, Partner

Morais Leitão, Galvão Teles, Soares da Silva & Associados – Sociedade de Advogados
T +351 213 817 455
F +351 213 817 494
E htb@mlgts.pt W www.mlgts.pt

Professional qualifications. Portugal, Law Degree, Law Faculty of the Portuguese Catholic University, 1989; Master's Degree in Commercial Law and Capital Markets (Law Faculty of the Portuguese Catholic University, 1995

Areas of practice. Personal data privacy and protection; labour and social security (labour law, labour litigation, social security and pensions).

Languages. Portuguese, English, French and Spanish

Professional associations/memberships. Portuguese Bar Association, 1991; Portuguese Bar Association (member of the Lisbon District Council from 1999 to 2001); member of the IAPP (International Association of Privacy Professionals)

Publications

- Employment & Industrial Relations Law, Volume 27, No. 1 -, IBA Legal Practice Division, Preventing recruitment discrimination: social media and background checks in Portugal, April 2017 *(www.mlgts.pt/xms/files/Publicacoes/Artigos/2017/IBA_Newsletter_Employment___Industrial_Relations_Law.pdf).*
- Data Protection and Privacy, Portugal, Getting the Deal Through, 2017 *(https://gettingthedealthrough.com/area/52/jurisdiction/20/data-protection-privacy-2017-portugal/)*
- *Lex Mundi Global Data Privacy Guide, Portugal, 2017 (https://interactiveguides.lexmundi.com/lexmundi/global-data-privacy/portugal)*
- *Global Handbook on Employment Litigation: Procedures, Remedies and Best Practices - Portugal - L&E Global, 2016 (www.mlgts.pt/xms/files/Publicacoes/Artigos/2016/L_E_Global_Annual_Publication_2016.pdf).*
- Data Transmission and Privacy, Portugal, Center for International Legal Studies, Kluwer, Boston, 1994 (*https://books.google.pt/books?id=bMU6DOAnV-sC&pg=PA435&lpg=PA435&dq=Data+Transmission+and+Privacy,+%E2%80%98Portugal%E2%80%99,+Center+for+International+Legal+Studies&source=bl&ots=vRk-SMdzrx&sig=tWdjSX3s6GMNEoeav45vSj5GQa0&hl=pt-PT&sa=X&ved=0ahUKEwiv-4Lu6vLVAhUJtRoKHXPUAwIQ6AEIKTAA#v=onepage&q=Data%20Transmission%20and%20Privacy%2C%20%E2%80%98Portugal%E2%80%99%2C%20Center%20for%20International%20Legal%20Studies&f=false*).

João Alfredo Afonso, Partner

Morais Leitão, Galvão Teles, Soares da Silva & Associados – Sociedade de Advogados
T +351 213 817 426
F +351 213 817 494
E joaoafonso@mlgts.pt W www.mlgts.pt

Professional qualifications. Portugal, Law Degree, Law Faculty of the Portuguese Catholic University, 1998

Areas of practice. Corporate and commercial (corporate law, mergers, acquisitions and joint ventures), personal data privacy and protection.

Languages. Portuguese, English, French and Spanish

Professional associations/memberships. Portuguese Bar Association, 2000.

Publications

- *Data Protection Impact Assessments under the GDPR: questions unanswered? - Data Protection Leader (www.mlgts.pt/xms/files/Publicacoes/Artigos/2017/DPL_Data_Protection_Impact_Assessments_under_the_GDPR_questions_unanswered_MAIO2017.pdf).*
- *Gaming Global Guide: Portugal 2017 - Thomson Reuters (www.mlgts.pt/xms/files/Publicacoes/Artigos/2017/TR_Gaming_Global_Guide_Gaming_in_Portugal_Overview.pdf).*
- Shared liquidity in Portugal: Regulation notified to the European Commission - Online Gambling Lawyer *(www.mlgts.pt/xms/files/Publicacoes/Artigos/2017/OGL_February_2017_pg6-7.pdf).*
- Issues preventing the launch of operations in Portugal - Draft regulations issued on betting exchanges and liquidity *(www.mlgts.pt/xms/files/Publicacoes/Artigos/2016/WOGLR_March_2016_pg_14.pdf).*

Tiago Félix da Costa, Partner

Morais Leitão, Galvão Teles, Soares da Silva & Associados – Sociedade de Advogados
T +351 210 091 783
F +351 213 817 494
E tfcosta@mlgts.pt W www.mlgts.pt

Professional qualifications. Portugal, Law Degree, Law Faculty of the University of Lisbon, 2002; Postgraduate Studies in Corporate Law, Management Institute/Portuguese Bar Association, 2004; Master's Degree in Law, Law Faculty of the Portuguese Catholic University, 2009; Advanced Training Course on Data Protection Compliance in the EU, European Institute of Public Administration – EIPA, 2017

Areas of practice. Litigation and arbitration (civil and commercial litigation, constitutional law, criminal litigation, misdemeanour litigation and compliance); personal data privacy and protection.

Languages. Portuguese, English and French

Professional associations/memberships. Portuguese Bar Association, 2004.

Publications. *Litigation in Portugal - Chambers Legal Practice Guides, 2014* (*www.mlgts.pt/xms/files/Publicacoes/Artigos/2014/Chambers_Legal_Practice_Guides_Litigation_2014.pdf*).