CHAPTER 50

PORTUGAL

Magda Cocco
Joana Almeida e Sousa*

* Joana Almeida e Sousa participated in prior versions of this chapter when she was associated with Vieira de Almeida & Associados.

Entry in the European Union	*Capital*	*Official Language*	*Political System*	*Population*	*Currency*
1986	Lisbon	Portuguese	Republic	10.6 million	Euro

LOCATION

Portugal—officially, the Portuguese Republic—is the westernmost country of Europe. It is located in the southwest corner of Europe and looks out from the Iberian Peninsula onto the Atlantic Ocean. It is bordered on the north and east by Spain. Portugal includes the Madeira and Azores archipelagos.

GOVERNMENT & LEGAL SYSTEM

Portugal is a democratic republic ruled by the Constitution of 1976, which has been revised numerous times since its adoption. Its sovereign bodies are: the President, the Parliament, the Government, and the Courts.

The President, elected for a five-year term by universal suffrage, has a supervising, non-executive role. The Council of State is the presidential advisory body. The Prime Minister is the head of government and is appointed by the President. Taking into account the results of the general election for the Parliament, the Prime Minister in turn appoints the other ministers to form the Council of Ministers, and he prepares the program of the government.

The legislative branch is unicameral. The Assembly of the Republic is composed of deputies who are elected every four years. It has both exclusive and non-exclusive legislative powers. The non-exclusive legislative powers may be delegated to the Government by the Parliament for specific purposes.

The Portuguese legal system is a civil law system. Consequently, the main legal rules are laid out in codes or other written laws. The judicial branch is comprised of the Supreme Court, District Courts Appeals, and the Constitutional Tribunal.

MEMBERSHIP

Portugal has been a member of the United Nations since 1955 and of the European Union since 1986. It joined the North Atlantic Treaty Organization (NATO) in 1949 and the Organization for Economic Cooperation and Development (OECD) in 1961. Portugal joined the Council of Europe in 1976.

ECONOMY

The economy of Portugal is based on industries such as textiles, clothing, footwear, cork and wood products, beverages, porcelain, and glass. Metalworking, petrochemicals, and mechanical engineering are the main heavy industries. Services, particularly tourism, are playing an increasingly important role.[1]

§ 50.01 INTERNATIONAL TREATIES AND AGREEMENTS

[A] United Nations

As part of its membership in the United Nations, Portugal has ratified several conventions, *inter alia*:

- The Universal Declaration of Human Rights, which establishes the right to be protected by law against the arbitrary interference with privacy;
- The Resolution on the use of biometrics in passports, identity cards, and travel documents, and the Resolution on the use of Personal Data for Political Communication, both having stated strict rules on data protection;
- The Convention on the Rights of the Child;
- The International Covenant on Civil and Political Rights; and
- The International Covenant on Economic, Social and Cultural Rights.

[B] European Union

Portugal is a member of the European Union, having, therefore adopted all treaties arising from this membership. In this context, Portugal has signed the European Social Charter and the Supplemental Agreement between the Europol Police Office and the United States of America on the Exchange of Personal Data and Related Information. This Protocol was signed following the authorization given to Europol by the Council of the European Union to enter into negotiations to reach an agreement on the exchange of personal data with the United States.

[1] Sources for this section http://europa.eu; http://www.state.gov.

[C] Council of Europe

As a member of the Council of Europe, Portugal has ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, its additional Protocol regarding supervisory authorities and transborder data flows, as well as the European Convention for the Protection of Human Rights and Fundamental Freedoms.

[D] Organization for Economic Cooperation and Development (OECD)

Portugal is also a member of the Organization for Economic Cooperation and Development (OECD). In this connection, it has signed the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. It has also signed the Monteux Declaration that explains the document, "The Protection of Personal Data and privacy in a globalized world: a universal right respecting diversity," which establishes several principles, such as the principles of data security, responsibility, independent supervision and legal sanction and adequate level of protection in the case of transborder flows of personal data, among others.

§ 50.02 CONSTITUTION

Part I of the Constitution of the Portuguese Republic addresses the fundamental rights and duties of the Portuguese people and contains several sections dealing with privacy.[2] The protection of the privacy of the home and correspondence is set forth in Article 34 and Article 35 establishes the foundations of the protection of personal data.

[A] Privacy of the Home and Correspondence

Article 34 declares that an individual's home and the privacy of his correspondence and other means of private communication are inviolable. It prohibits entering into the home of any person without his consent except by order of the competent judicial authority and in the cases, and

[2] An unofficial translation of the Constitution of the Portuguese Republic is available at: http://www.wipo.int.

according to the forms, laid down by law. It also prohibits any interference with correspondence or telecommunications, apart from the cases laid down by law in connection with criminal procedure.

[B] Protection of Personal Data

The protection of personal data is addressed in Article 35, which deals with the use of data processing. Compared to other constitutions, this provision is especially lengthy and detailed. Article 35 (Use of Computers) was brought into the Constitution of the Portuguese Republic in 1997. Article 35 provides the following:

1. Every citizen shall possess the right of access to all computerized data that concern him, to require that they be corrected and updated, and to be informed of the purpose for which they are intended, all as laid down by law.
2. The law shall define the concept of personal data, together with the terms and conditions applicable to its processing by automatic means and its linkage, transmission and use, and shall guarantee its protection, particularly by means of an independent administrative body.
3. Computers shall not be used to process data concerning philosophical or political convictions, party or trade union affiliations, religious beliefs, private life or ethnic origins, except with the express consent of the data subject, with authorization provided for by law and with guarantees of non-discrimination, or for the purpose of processing statistical data that cannot be individually identified.
4. Third-party access to personal data shall be prohibited, except in exceptional cases provided for by law.
5. The allocation of a single national number to any citizen shall be prohibited.
6. Everyone shall be guaranteed free access to public-use computer networks, and the law shall define both the rules that shall apply to crossborder data flows and the appropriate means for protecting personal data and such other data as may justifiably be safeguarded in the national interest.

7. Personal data contained in manual files shall enjoy the same protection as that provided for in the previous paragraphs, as laid down by law.

§ 50.03 DATA PROTECTION LAW

The primary data protection law of Portugal is the Act on the Protection of Personal Data,[3] Act 67/98 of October 26, 1998 (Data Protection Act). This law is based on the 1995 Data Protection Directive of the European Union.[4] The Data Protection Act replaces the 1991 Act on the Protection of Personal Data with regard to Automatic Processing, which was enacted in order to implement the requirements of the 1995 Data Protection Directive.

Chapter IV of the Data Protection Act establishes the *Comissão Nacional de Protecção de Dados* or CNPD (National Data Protection Commission).[5] Articles 21 to 32 of the Data Protection Act detail the extensive powers of the CNPD.

[A] Protected Information

The Data Protection Act is applicable to the processing of personal data. More stringent provisions govern the processing of "sensitive data."

[1] Personal Data

According to the Data Protection Act, "personal data" is any information of any type, including sound and image, relating to an identified or identifiable natural person ("data subject"). An "identifiable person" is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific

[3] An unofficial translation of the Data Protection Act is provided at: http://www.cnpd.pt/english/index_en.htm.

[4] Directive 95/46/EC of the European Parliament and of the Council dated October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. For more on the 1995 EU Data Protection Directive, see Chapter 6.

[5] The website of the National Data Protection Commission is available in English at: http://www.cnpd.pt/english/index_en.htm.

to his physical, physiological, mental, economic, cultural or social identity.[6]

[2] Sensitive Data

Personal data concerning any of the following is considered "sensitive data": philosophical or political beliefs, political party or trade union membership, religion, private life and racial or ethnic origin, and data concerning health or sex life, including genetic data. The processing of sensitive data is prohibited, unless an exception applies, as explained below in this chapter.

[B] Obligations of the Data Controller

[1] Definitions

The Data Protection Act defines numerous requirements for entities that have access to personal data. It distinguishes controllers and processors. A "controller" is a natural or legal person, public authority, agency, or any other body that determines the purposes and means of the processing of personal data.[7] A "processor" is any natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the controller.[8]

The "processing of personal data" is a broad concept, which consists in any operation or set of operations that are performed upon personal data, whether wholly or partly by automatic means, such as collection, recording, organization, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

[2] Collection Limitation

In order to be lawful, the collection of personal data must be carried out according to the requirements provided in the Data Protection Act.

[6] Data Protection Act, Article 3(a).
[7] Data Protection Act, Article 3(d).
[8] Data Protection Act, Article 3(e).

There are different rules for personal data in general, and for personal data that are considered "sensitive data."

[a] Personal Data

Personal data may be collected only if (i) the relevant data subject has clearly and unambiguously given his consent or (ii) the processing is necessary in order to carry out one of the following purposes:[9]

- The performance of a contract to which the data subject is a party, or to take steps at the request of the data subject before entering into a contract, or a declaration of his intent to negotiate an agreement;
- Compliance with a legal obligation to which the data controller is subject;
- The protection of the vital interests of the data subject if the data subject is physically or legally incapable of giving his consent;
- The performance of a task carried out in the public interest or in the exercise of public authority vested in the data controller or in a third party to whom the data are disclosed; or
- The pursuit of the legitimate interests of the data controller or the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests of the data subject for fundamental rights, freedoms and guarantees.

[b] Sensitive Data

The processing of sensitive data is prohibited unless an exception applies.[10] For example, the processing of sensitive data may be lawful if the relevant consent is obtained from the data subject and an authorization is granted by the National Data Protection Commission.[11]

Further, the processing of sensitive personal data is permitted when one of several conditions are met, such as if healthcare data are required

[9] Data Protection Act, Article 6.
[10] Data Protection Act, Article 7(1).
[11] Data Protection Act, Article 7(2).

for preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services. However, in this case, the data may be processed only by a health professional that is bound by an obligation of professional secrecy or by another person who is subject to an equivalent obligation of secrecy.[12]

The processing of sensitive data is also permitted when one of the following conditions applies:

- When it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally unable of giving his consent;
- When it is carried out with the data subject's consent in the course of its legitimate activities by a foundation, association or non-profit seeking body with a political, philosophical, religious, or trade union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
- When it relates to data which are manifestly made public by the data subject, provided his consent for their processing can be clearly inferred from his declarations;
- When it is necessary for the establishment, exercise, or defense of legal claims and is exclusively carried out for that purpose.

[3] Purpose Limitation

The Act requires that data be collected for specified, explicit, and legitimate purposes. Data may not be further processed in a way that is incompatible with these purposes.[13] Nevertheless, in exceptional cases, the National Data Protection Commission may authorize the use of personal data for a purpose different from the purpose for which the data were initially collected.

[12] Data Protection Act, Article 7(4).
[13] Data Protection Act, Article 5(1)(b).

[4] New Purpose

If the data controller intends to process the collected data for a different purpose than initially intended—i.e., a purpose that was not specified in the corresponding notification to the National Data Protection Commission or in the notice of data collection—the data controller must request the authorization of the National Data Protection Commission before carrying out the processing of the information for such new purpose.

[5] Data Quality and Accuracy

Article 5 details the requirements for the quality of the data, and the lawfulness of their processing. The principles outlined in Article 5 are similar to those that are set forth in Article 6 of the 1995 EU Data Protection Directive.[14] Personal data must be:[15]

- Processed lawfully and with respect for the principle of good faith;
- Collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes;
- Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- Accurate and, when necessary, kept up to date. Adequate measures must be taken to ensure that data that are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; and
- Kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which they were collected or for which they are further processed.[16]

[14] *See* Chapter 6, "1995 EU Data Protection Directive."
[15] Data Protection Act, Article 5(1).
[16] Data Protection Act, Article 5(1).

[C] Rights of the Data Subject

The Data Protection Act provides data subjects with a range of rights that is substantially similar to those that are outlined in the 1995 Data Protection Directive. These rights include, for example, the right of information, right of access, and right of erasure.

[1] Right to Information

The Data Protection Act requires the data controller to provide the data subject with certain information on the terms of the processing. Whenever data are collected, the data controller must provide the following information to the data subject (except when such information was already provided):[17]

- The identity of the controller and of its representative, if any;
- The purposes of the processing;
- Other information such as: (i) the recipients or categories of recipients, (ii) whether replies are mandatory or voluntary and the consequences of failure to reply, or (iii) the existence of a right of access and right of rectification.

Furthermore, the documents supporting the collection of personal data must contain the above information.

If the data are not collected directly from the data subject, the data controller or its representative must provide the data subject with the information referred to above (i) when the data are recorded or (ii) if the disclosure of the data to third parties is envisaged. This disclosure must occur no later than the time when the data are first disclosed.

If the data are collected on an open network, the data subject must be informed that his or her data may be circulating in the network without security measures and may be at risk of being seen and used by unauthorized third parties.[18]

[17] Data Protection Act, Article 10(1).

[18] Data Protection Act, Article 10(4).

[2] Consent

Under the Data Protection Act, in order to process any personal data, the unambiguous consent of the data subject should be previously obtained,[19] unless an exception applies. Different rules and restrictions apply. The collection and processing of personal data is less restricted than the collection and processing of "sensitive data."[20]

[3] Right of Access

Article 11 of the Data Protection Act grants individuals the right to access personal information about them. Specifically, a data subject has the right to obtain from the data controller, without constraint, at reasonable intervals, and without excessive delay or expense:

- A confirmation as to whether or not data relating to her are being processed and information as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
- Communication in an intelligible form of the data undergoing the processing, and of any available information as to their source;
- Knowledge of the logic involved in any automatic processing of the data concerning her.[21]

The National Data Protection Commission has issued some guidelines concerning the right of access to health data of deceased data subjects.

[4] Right of Rectification

If access to the data pursuant to the right of access described above has revealed that the data were incorrect, the data subject may wish to

---

[19] Data Protection Act, Article 6.

[20] For the detailed rules on consent and other restrictions on the collection and processing of personal data and sensitive data, *see* Data Protection Act, Articles 6 and 7. *See also, supra*, in this chapter, the obligations of data controllers regarding the collection of personal data.

[21] Data Protection Act, Article 11.

have the data corrected. Article 11 grants the data subject the right to obtain from the data controller, without constraint, within a reasonable term and without excessive delay or expense, the rectification, erasure or blocking of data, whenever the relevant processing does not comply with the Data Protection Act, in particular due to the incomplete or inaccurate nature of the data.

In addition, Article 11 grants the data subject the right to have the data controller notify all third parties to whom the data have been disclosed before the rectification, erasure, or blocking, unless such notification proves impossible.

[5] Right of Opposition

[a] Right to Object to the Processing of Data

Article 12 of the Data Protection Act addresses the right of the data subject to object to the processing of his data. There are two standards. One applies to the processing of data in general, and the other applies to the processing of data for direct marketing purposes.

With respect to the general processing of the data, the data subject has the right to object, at any time, on compelling legitimate grounds relating to his particular situation, to the processing of data relating to him.[22] Where there is a justified objection, the processing instigated by the controller may no longer involve these data, unless otherwise provided by law and, at least, in the cases where data processing is needed for the accomplishment of a mission of public interest or the pursuit of the legitimate interests of the data controller or the third party to whom the data are disclosed. There is an exception when these interests are overridden by the interests of the data subjects that are protected by the fundamental rights, freedoms and guarantees.

[b] Right to Object to Direct Marketing

Article 12(b) grants individuals the right to object to the use of their personal data for direct marketing purposes or any other form of research.

[22] Data Protection Act, Article 12.

In this case, the data subject has the right to object, on request and free of charge, to the processing of personal data relating to him that the data controller anticipates will be processed for direct marketing purposes or for any other form of research. The data subject has the right to be informed before personal data are disclosed for the first time to third parties for direct marketing purposes or for use on behalf of third parties. In addition, the data subject must expressly be offered the right to object to such disclosure or uses, free of charge.[23]

[D] Content of the Notice

Article 10 grants the data subject the Right of Information. The data subject has the right to be informed of:[24]

- The identity of the controller and of its representative, if any;
- The purposes of the processing;
- The recipients, or categories of recipients, of the data;
- What replies are mandatory or optional, and the possible consequences of failure to reply;
- The existence and conditions of the right of access and the right to rectify, provided that they are necessary, taking into account the specific circumstances of collection of the data in order to guarantee that the relevant information will be processed fairly.

If data are collected on an open network, the data subject must be informed that his data may be circulating on the network without security measures and may be at risk of being seen and used by unauthorized third parties.

[E] Security and Protection of the Data

Articles 14 to 17 of the Data Protection Act address the requirements for the protection of the security and confidentiality of the processing.

[23] Data Protection Act, Article 12.
[24] Data Protection Act, Article 10.

The law distinguishes general security measures and special security measures.

[1] Security of Processing

Under Article 14, the data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, change, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures must ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. The measures must also take into account the state of the art and the cost of their implementation.

[2] Special Security Measures

Article 15 specifies special security measures for the handling of sensitive data. More stringent requirements apply to the processing of sensitive personal data. If the data to be processed concern philosophical or political beliefs, political party or trade union membership, religion, racial or ethnic origin, health or sex life, or are genetic data, or data relating to individuals suspected of illegal activities, criminal and administrative offenses and decisions applying penalties or fines, the data controller is required to take appropriate measures in order to:[25]

- Prevent unauthorized persons from entering the premises used for processing such data (control of entry to the premises);
- Prevent data media from being read, copied, modified, or removed by unauthorized persons (control of data media);
- Prevent unauthorized input, disclosure, modification, or elimination of personal data input (control of input);
- Prevent automatic data processing systems from being used by unauthorized persons by means of data transmission facilities (control of use);

[25] Data Protection Act, Article 15.

- Guarantee that only authorized persons may access data covered by the authorization (control of access);
- Guarantee the control of the entities to whom personal data may be transmitted by means of data transmission facilities (control of transmission);
- Guarantee that it is possible to control *a posteriori* when and by whom the data were input (control of input);
- Prevent the unauthorized reading, copying, modification, or erasure of data while the data are being transmitted or transported (control of transport).

The National Data Protection Commission may waive the existence of certain security measures by taking into account the nature of the entities responsible for processing and the type of premises in which it is carried out. However, the data controller must guarantee that the fundamental rights, freedoms, and guarantees of the data subjects are respected.

The systems must guarantee logical separation between health, sex life, and genetic data, and other personal data. This rule applies especially to the processing of data by hospitals.

The National Data Protection Commission may determine that the transmission of sensitive data[26] over a network must be encoded whenever the circulation of these data over a network may jeopardize the fundamental rights, freedoms and guarantees of the relevant data subjects.[27]

[3] Penalties

Entities that fail to comply with any of the security requirements described immediately above may be punished with a minimum fine of EUR 498.80 and a maximum fine of EUR 4,987.98.[28]

---

[26] That is, data concerning philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data, and relating to individuals suspected of illegal activities, criminal and administrative offenses and decisions applying penalties.

[27] Data Protection Act, Article 15.

[28] Data Protection Act, Articles 37 and 38.

[4] Responsibility for the Data; Accountability

When processing is carried out on its behalf, the data controller must choose a data processor that provides sufficient guarantees with respect to the use of technical and organizational security measures that will govern the processing. The data controller must ensure that the data processor complies with these measures.[29]

If processing is carried out by a data processor, the data processor and data controller must enter into a written contract or legal act binding the data processor.[30] This agreement must stipulate that the data processor shall act only on instructions from the data controller and that the data controller's obligations to use appropriate technical and organizational measures to protect the data shall be incumbent on the data processor.[31] The agreement must define the security requirements and the measures to be used in order to protect personal data against accidental or unlawful destruction, accidental loss, modification, unauthorized disclosure, or access.

[5] Recipient of Personal Data

Any person who acts under the authority of the data controller or the data processor, including the data processor himself, and who has access to personal data must not process the data except under instructions from the data controller, unless required to do so by law.[32]

[F] Transfer of Information to a Third Party

Chapter III of the Data Protection Act focuses on the transfer of personal information. As required by the 1995 Data Protection Directive, the Act distinguishes transfers that are made within the European Union from transfers that are made outside the region.

[29] Data Protection Act, Article 14(2).
[30] Data Protection Act, Article 14(3).
[31] Data Protection Act, Article 14(3).
[32] Data Protection Act, Article 16.

[1] Within the Region

Personal data may be freely moved within Portugal and transferred to another EU Member State;[33] however, data subjects must be informed if the data are transferred to a third party. A notification to the National Data Protection Commission to inform the data transfer must be made, although, in general, an authorization from the National Data Protection Commission will not be necessary. Nevertheless, note that whenever there is a transfer of data within the European Union between a data controller to another data controller, in which the latter (recipient of such data) will process the data for its own purposes, an authorization will be issued by the National Data Protection Commission, as this transfer of data will be deemed as a communication of data to a third party.

[2] Out of the European Union

For transfers outside the European Union, the Act distinguishes countries that offer an adequate level of protection from the other countries that do not offer the referred adequate level of protection. There are more complex requirements where the receiving party is located in a country that does not offer an adequate level of protection.

[a] Country with Adequate Level of Protection

The transfer of personal data that are undergoing processing (or are intended for processing) to a country that is not a member of the European Union, may only take place subject to compliance with the Data Protection Act and provided that the country to which the data are transferred ensures an adequate level of protection.[34]

The adequacy of the level of protection of a country that is not a member of the European Union is assessed in light of the circumstances surrounding a data transfer or set of transfers.[35] It is for the National Data Protection Commission or the European Commission to decide whether a

[33] Data Protection Act, Article 18.
[34] Data Protection Act, Article 19(1).
[35] Data Protection Act, Article 19(2).

country that is not a member of the European Union ensures an adequate level of protection.[36]

The European Commission has already approved the transfer of data to some countries that it has considered to offer an adequate level of protection. The referred approved territories are the following: Argentina, Canada, Faroe Islands, Guernsey, Jersey, Isle of Man, Israel, and Switzerland.

[b] Country Without Adequate Level of Protection

A transfer of personal data to a country that does not ensure the required "adequate level of protection" may be allowed by the National Data Protection Commission if the data subject has given his consent unambiguously to the proposed transfer, or if that transfer:[37]

- Is necessary for the performance of an agreement between the data subject and the data controller, or for the implementation of pre-contractual measures taken in response to a request by the data subject;
- Is necessary for the performance or conclusion of an agreement concluded or to be concluded between the data controller and a third party, in the interest of the data subject; or
- Is necessary or legally required on important public interest grounds, or for the establishment, exercise of defense of legal claims; or
- Is necessary in order to protect the vital interests of the data subject; or
- Is made from a register that, according to laws, is intended to provide information to the public and that is open to consultation by the public or by any person who can demonstrate legitimate interest.

The National Data Protection Commission may authorize a transfer, or a set of transfers, to a country that does not ensure an adequate level of protection, if the data controller guarantees adequate safeguards with

[36] Data Protection Act, Article 19(3).
[37] Data Protection Act, Article 20(1).

respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise. This guarantee can be achieved through appropriate contractual clauses.[38] This authorization is granted by the National Data Protection Commission according to its own procedures and the decisions of the European Commission. Typically, the National Data Protection Commission follows the decisions of the European Commission on these matters.[39]

The National Data Protection Commission has issued an Opinion in 2004 in order to clarify the interpretation of Articles 19 and 20 of the Data Protection Act concerning the transfer to countries outside the European Union. This Opinion states that the transfer of personal data to those countries is allowed, and will not be subject to the National Data Protection Commission prior authorization, if:

- There is a decision of the European Commission finding that a country offers an adequate level of protection;
- Any of the exemptions foreseen in the Article 20 of the Data Protection Act is fulfilled; or
- The transfers of personal data are made under the adoption of the standard contractual clauses approved by the European Commission.

[c] Standard Contractual Clauses

The European 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 (data controller to data controller).
- Decision 2004/915/EC on standard contractual clauses for the transfer of personal data to third parties (data controller to data controller set II).

[38] Data Protection Act, Article 20(2).
[39] Data Protection Act, Article 20(4).

- Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries (data controller to data processor).

If the parties have adopted the standard contractual clauses approved by the European Commission, the National Data Protection Commission will only confirm whether the transfer of personal data is made in accordance with these clauses.[40]

Standard Contractual clauses may not be amended but the parties are free to include any other clauses on business related issues provided that they do not contradict the model clauses.

[d] Safe Harbor

If a data importer that is based in the United States has self-certified to its adherence to the Safe Harbor Principles agreed between the European Union and the U.S. Department of Commerce, the data exporter located in Portugal has the assurance that the company to whom the data are transferred has the adequate level of protection as required by the Data Protection Act.

Notwithstanding the above, whenever the data are transferred to a data processor, the National Data Protection Commission considers that the relation between the data importer and the data exporter (the data controller) must also be ruled by a written agreement.[41]

[e] Binding Corporate Rules

The National Data Protection Commission does not accept Binding Corporate Rules to allow transferring personal data throughout the multinational organization or group of companies.

[f] Other Mechanisms to Transfer Data to a Country Without Adequate Level of Protection

The European Decisions approving Standard Contractual Clauses do not prevent national Data Protection Authorities authorizing other

[40] Data Protection Act, Article 20(5).

[41] Data Protection Act, Article 14.

contractual arrangements for the export of data out of the European Union based on national law, as long as these authorities are satisfied that the contracts in question provide adequate protection for data privacy. The National Data Protection Commission recognizes the validity of other contractual arrangements for the export of data, provided that such contracts contain specific rules on data protection and comply with the requirements set by the Data Protection Act.

Some Member States (such as the United Kingdom) allow the self-assessment approach for legitimizing transfers of data from member states to third countries. Under this mechanism the data exporter should consider and make a judgment as to whether, in the particular circumstances of a transfer, the transfer is made to a country that can ensure an adequate level of protection. This approach is not admitted by the Data Protection Act.

[G] Notification and Registration with Local Authorities

The Data Protection Act identifies different levels of requirements for notification and request for authorization, which depend on the nature of the data and the nature of the processing. A notification is sufficient in most cases. For most sensitive data, an authorization may be required.

The National Data Protection Commission has implemented an electronic notification procedure, allowing the data controllers to only notify the data processing operations carried out.

[1] Obligation to Notify the National Data Protection Commission

The data controller or its representative, if any, must notify the National Data Protection Commission before carrying out any processing intended to serve a single purpose or several related purposes.[42] Subject to this notification, the data controller must pay a fee of EUR 75 to the National Data Protection Commission.

The non-automatic processing of personal data regarding philosophical or political beliefs, political party or trade union membership, religion, racial or ethnic origin, and the processing of data concerning

[42] Data Protection Act, Article 27(1).

health, sex life, or genetics requires notification of the National Data Protection Commission whenever these data are processed in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his consent.[43]

[2] Exemption

The National Data Protection Commission may authorize the exemption from notification for specific categories of processing operations that are unlikely to affect adversely the rights and freedoms of the data subjects. This decision must be made based on the nature of the data, efficiency, or economics criteria.[44]

In the use of such powers, the National Data Protection Commission has issued some decisions related to notification exemptions, which concern:

- The processing of employees' salaries, contributions and allowances;
- The management of databases and registries of libraries and archives;
- The management and invoicing of customers and suppliers;
- The management of employees and service providers;
- The registers of entrance in and exit from a building;
- The databases of associations.

These exemptions are only applicable whenever all requirements foreseen in the decisions are met.

In addition, there is no obligation to file a notification if the sole purpose of the processing is to keep a register that is intended to provide information to the public and that may be reviewed by the public in general or by any person who proves to have a legitimate interest. This processing is also exempt from notification (for example, the real estate registry).[45]

---

[43] Data Protection Act, Article 27(5).
[44] Data Protection Act, Article 27(2).
[45] Data Protection Act, Article 27(4).

[3] Prior Checking

There are cases where there is an additional concern about the processing of certain data because of the high level of sensitivity associated with these data. In these cases, the data controller must obtain an authorization from the National Data Protection Commission. This procedure is called "prior checking."[46] Whenever the data processing is subject to prior authorization from the National Data Protection Commission, the applicable fee is EUR 150.

The authorization of the National Data Protection Commission is required for the processing of:[47]

- Sensitive data when not foreseen in a legal provision;
- Personal data relating to individuals suspected of illegal activities, criminal and administrative offenses and decisions applying penalties, security measures, fines and additional penalties; or
- Personal data relating to the credit and solvency of the data subjects.

The authorization of the National Data Protection Commission is also required for the combination of personal data and the use of personal data for purposes that do not give rise to their collection.[48] A "combination of personal data" is defined as a form of processing that consists of the possibility of correlating data in a database with data in another database that is kept by another or other data controllers or that is kept by the same controller for other purposes.[49]

A legal ruling may authorize the processing of data that would otherwise be subject to the prior checking process. In this case, the authorization of the National Data Protection Commission is not required. For example, there is no need for an authorization if the processing is intended for preventive medicine, medical diagnosis, the provision of care or treatment, or the management of health care services. However, the data must be processed by a health professional who is subject to the

[46] Data Protection Act, Article 28(1).
[47] Data Protection Act, Article 28(1).
[48] Data Protection Act, Article 9.
[49] Data Protection Act, Article 3(1).

obligation of professional secrecy. In this case, if all the conditions are met only is a notification required.[50]

[H] Privacy Official

Unlike other European Member States, such as France or Germany, the Data Protection Act of Portugal does not provide for the appointment of a data protection official within an organization.

[I] Enforcement

The law distinguishes different levels of penalties. These levels depend upon the nature of the violation. The penalties range from a fine of a few hundred Euros to prison terms.

[1] Misdemeanors

The most usual penalties are those that apply when an entity negligently fails to comply with the obligation to notify the National Data Protection Commission regarding the processing of personal data, or that provide false information or comply with the obligation to notify without complying with the request of some information, or that, despite having been notified by the National Data Protection Commission, continue to allow access to open data transmission networks to data controllers who fail to comply with the provisions of the Data Protection Act.

Such offenses are punishable with the following fines:

- In the case of a natural person, a fine between EUR 249.40 and EUR 2,493.99;
- In the case of a legal person or an organization without legal personality, a fine of EUR 1,496.40 to EUR 14,963.94.

Such limits are doubled whenever the processing of the relevant data was subject to prior checking by the National Data Protection Commission and authorization under Article 28 of the Data Protection Law.[51]

[50] Data Protection Act, Article 7(4).

[51] Data Protection Act, Article 37.

In addition, whenever the entities fail to comply with certain provisions of the Data Protection Act these offenses are punishable with a fine between EUR 498.80 and EUR 4,987.98. This includes, for example, failure to comply with the obligation to (i) provide the data subject's rights to be informed, to have access to the data or to object to the processing; (ii) adopt special security measures when processing sensitive data; and (iii) guarantee that the processor only acts under the instructions of the data controller, among others.

Such fines are doubled whenever the entities fail to comply with the provisions regarding the conditions to legitimize the data processing, the processing of sensitive data, the data relating to people suspected of illegal activities, criminal and administrative offenses, combination of personal data and transfer of personal data out of the European Union.

[2] Crime

Any person who intentionally does not comply with obligations listed below may be liable to up to one year's imprisonment or a fine of up to 120 days.[52] Examples of non-compliance include:[53]

- Failure to notify or apply for authorization before carrying out any processing operation that requires notification or authorization;
- Providing false information in the notification or in applications for authorization to process personal data, or making modifications that are not permitted by the applicable notification or authorization instrument;
- Misappropriation or use of personal data in a form that is incompatible with the purpose for the collection or with the notification or authorization instrument;
- Promoting or carrying out an illegal combination of personal data;

[52] When the Act provides for a fine of "a number of days up to 120 days," this fine will correspond to a certain amount—between EUR 5 and EUR 500 per day. The relevant court will determine the number of days and the amount applicable to a certain case.

[53] Data Protection Act, Article 43.

- Failure to comply, within the delay determined by the National Data Protection Commission, with the obligations provided for in the Data Protection Act or in other data protection legislation;
- Continuing to allow access to open data transmission networks to data controllers who fail to comply with the provisions of the Data Protection Act after being notified by the National Data Protection Commission not to do so.

The limits of the above-mentioned penalty may be doubled whenever sensitive data are being processed, such as data relating to people suspected of illegal activities, criminal and administrative offenses or the processing of personal data relating to credit, and the solvency of the data subjects.[54]

Moreover, the Data Protection Act states that if any person accesses personal data when prohibited from doing so and without due authorization, this person will be liable to up to one year's imprisonment or a fine of up to 120 days.[55] These criminal proceedings may only take place whenever a complaint is submitted before the competent authorities.

The Act allows the upper limit of the penalty to be increased to twice the amount whenever access:

- Is achieved by means of the violation of technical security rules;
- Allows the agent or third parties to obtain knowledge of the personal data; or
- Provides the agent or third parties with a benefit or material advantage.[56]
    - Any person who without authorization erases, destroys, damages, deletes, or changes personal data, making them unusable or affecting their capacity for use shall be punished by up to two years imprisonment or a fine up to 240 days. These limits are doubled if the damage caused is particularly serious. The negligence is also punishable up to one-year imprisonment or with a fine up to 120 days. The Data Protection Act also provides that any person who does not

[54] Data Protection Act, Article 43(2).
[55] Data Protection Act, Article 44.
[56] Data Protection Act, Article 44(3).

interrupt, cease or block the processing of personal data after being notified to do so, shall be subject to a penalty corresponding to the crime of "qualified non-compliance."[57] The Data Protection Act provides additionally that the same penalty applies to any person who after being notified to do so,[58] without just cause refuses to provide the cooperation specifically required of him according to Article 24 of the Data Protection Act (which refers to the cooperation with the National Data Protection Commission by providing it with all the information requested in order to carry out its responsibilities);

- Does not erase or totally or partially destroys the personal data; or
- Does not destroy the personal data after the period for keeping such data provided for in Article 5 has elapsed.

Any person bound by professional secrecy according to the law who without just cause and without due consent reveals or discloses personal data, shall be liable to up to two years' imprisonment or a fine of up to 240 days.[59] The penalty may be increased by half the maximum if the agent: (i) is a civil servant or equivalent, according to penal law; (ii) acts with the intention of obtaining a material advantage or other unlawful gain; or (iii) adversely affects the reputation, honor, and esteem or the privacy of another person. A person guilty of negligence shall be liable for up to six months' imprisonment or a fine of up to 120 days.

Any attempt to commit the crimes provided for in the above-mentioned provisions shall always be liable for punishment.[60]

In addition to the fines and penalties applied, the following additional penalties may be ordered:[61] (a) temporary or permanent prohibition of processing, blocking, erasure or total or partial destruction of data; (b) publication of the conviction; (c) public warning or censure of the data controller.

---

[57] Data Protection Act, Article 46(1).
[58] Data Protection Act, Article 46(2).
[59] Data Protection Act, Article 47.
[60] Data Protection Act, Article 48.
[61] Data Protection Act, Article 49.

[J] Private Right of Action

Individuals may report directly to the National Data Protection Commission any non-compliance with the Data Protection Act, by any entity that is subject to the Act. The National Data Protection Commission, in turn, will prosecute the non-compliant organization or entity.

The National Data Protection Commission is responsible for assessing the claims, complaints, or applications of individuals. It may conduct an investigation and may have access to data undergoing processing. It also has the power to collect all the information necessary for the performance of its supervisory duties.

In exercising its functions, the National Data Protection Commission must issue mandatory decisions against which challenges or appeals may be lodged with the *Tribunal Central Administrativo* (Central Administrative Court).[62]

[K] Data Protection Supervisory Authority

The Portuguese data protection supervisory authority is *Comissão Nacional de Protecção de Dados* or CNPD[63] (National Data Protection Commission). The National Data Protection Commission has extensive powers, such as the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law.[64] It also has the power to enforce the Data Protection Act, and to assess fines and penalties as described above.

In addition, the National Data Protection Commission has an important role in connection with the creation of laws and other legal instruments. The National Data Protection Commission must be consulted on any legal provisions and on legal instruments that relate to the processing of personal data and that are in preparation in the European Community or international institutions.[65]

---

[62] Data Protection Act, Article 23(3).

[63] The CNPD website is located at www.cnpd.pt.

[64] Data Protection Act, Article 22.

[65] Data Protection Act, Article 22(2).

§ 50.04 EMPLOYEE INFORMATION

There are no special rules applicable to the processing of employee information. The Data Protection Act is the primary source of rules with respect to the processing of personal information. However, the National Data Protection Commission has created some guidelines concerning health and security at the workplace and preventive and curative medicine regarding control in the use of alcohol and drugs by employees.

[A] Protected Information

All information collected by the employer concerning the employee is subject to the rules laid down in the Data Protection Act and no special rules apply. Employers must notify, or request authorization from the National Data Protection Commission, when applicable, the following forms of processing:

- Management of human resources;
- Recruitment of human resources;
- Healthcare at the workplace; and
- Preventive and curative health care regarding control in the use of alcohol and drugs by employees.

Additionally, in some cases, the processing of data concerning disciplinary sanctions, disciplinary procedures, as well as the guidelines concerning the use of e-mail or Internet must be notified or may be subject to the prior authorization of the National Data Protection Commission.

Moreover, the National Data Protection Commission has created some guidelines concerning health and security at the workplace. These guidelines define how the data processing and the notifications or the authorizations to the National Data Protection Commission must be prepared. In 2010, the National Data Protection Commission issued Opinion No. 840/2010, of October 11, 2010, which updated the above-mentioned guidelines concerning security and health at the workplace, due to the new Portuguese Labor Code (Law No. 7/2009), which came into force in 2009. The information protected in this context is:

- Personal data;
- Health data (such as medical results concerning healthcare at the workplace, medical details and diseases, absence records and/or records concerning accidents, complementary medical exams);
- Employee data;
- Data concerning the risk of professional diseases at the workplace and professional diseases.

The processing of data concerning sexual life and personal habits is admitted only if related to any kind of specific pathology and/or to any other health data. With respect to data relating to race or ethnic origin, the National Data Protection Commission has determined that the processing of such data in the context of healthcare at the workplace is excessive, inadequate, and not relevant. Data related to drugs and alcohol consumption, may be processed only in special circumstances, for instances considering the activity that is carried out by the employee (i.e., bus drivers or chemistry industry employees).

The National Data Protection Commission has also issued Opinion No. 890/2010, of November 15, 2010, concerning the processing of personal data with the purpose of preventive and curative medicine in the context of control in the use of alcohol and drugs by employees. The information protected in this context is:

- Personal data (employees and healthcare professionals' identification data);
- Health data related to the use of alcohol and drugs, including therapeutic treatments;
- Health data related to the control exams (such as the substances under control, the conditions, the frequency and the dates of the exams, the results of the control—and the results of an eventual rebuttal—and the proceedings adopted if the result of the exams is positive).

This processing of personal data is subject to the prior authorization of the National Data Protection Commission and the personal information mentioned above may only be collected for the purpose of preventive and curative medicine. In addition, only healthcare professionals may have access to, and process the health data. When sensitive data are processed,

the employer may not have access to the results of the exams. Employers may only have access to the information regarding whether an employee is able or not able to perform his or her responsibilities at work. These data may only be retained for one year.

[B] Required Notices

The notice to be given in the context of the processing data relating to human resources, recruitment of personnel, healthcare at the workplace, and preventive and curative medicine regarding control in the use of alcohol and drugs by the employees is not subject to any special requirement. Therefore, the employee has the right to be informed of:

- The identity of the data controller;
- The purposes of the processing;
- The recipients or categories of recipients;
- Mandatory and optional replies, as well as the possible consequences of failure to reply;
- The existence and conditions of the right of access and the right to rectify provided they are necessary, taking into account the specific circumstances of collection of the data in order to guarantee the relevant information will be processed fairly.

If the data are collected on an open network, the data subject must be informed that her data may be circulating on a network without security measures, and may be at risk of being seen and used by unauthorized third parties.

[C] Required Protective Measures

The employers must adopt special measures whenever their processing includes data revealing trade union membership, privacy, or health. In these cases, security measures must be adopted as required in Article 15 of the Data Protection Act:[66]

[66] Data Protection Act, Article 15.

- Control of entry to the premises;
- Control of data media;
- Control of input;
- Control of use;
- Control of access;
- Control of transmission;
- Control of transport.

Taking into consideration the nature of the entities responsible for processing and the type of premises in which it is carried out, the National Data Protection Commission may waive the requirement for certain security measures, subject to guaranteeing respect for the fundamental rights, freedoms and guarantees of the data subjects.[67]

[D] Former Employees and Retirees

The processing of the personal data of former employees or retirees is subject to the rules referred to above. Usually the processing of such data is notified to the National Data Protection Commission or requires the prior authorization of the National Commission.

§ 50.05 CHILDREN INFORMATION

There is no specific data protection law concerning children information. The general provisions of the Data Protection Act, or other laws that apply to specific types of personal data would apply to them in the same way as they would apply to adults. However, pursuant to the general rules set forth in the Portuguese Civil Code, children under eighteen (18) are not able to, by themselves, give an informed consent and therefore the legal representative of these children must give such consent, if necessary.

[67] Data Protection Act, Articles 6(a), 8, 15(2).

§ 50.06 COMMERCIAL COMMUNICATIONS

While some provisions of the Data Protection Act address the use of personal data in connection with direct marketing, the main law that addresses privacy and data protection issues in the context of commercial communications, and unsolicited commercial messages of the Decree-Law No. 7/2004, of January 7, 2004 as amended by the Decree-Law No. 62/2009, of March 10, 2009 (Electronic Commerce Law).[68] This law is based primarily on the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000. However, some of its provisions also implement the requirements of the 2002 EU Directive on Privacy and Electronic Communications.[69] The issue of unsolicited communications is addressed in Article 22 of the law.

[A] Restrictions on Direct Marketing Under the Data Protection Act

Article 12(2) of the Data Protection Act, grants the data subject three rights regarding the use of personal data in connection with direct marketing. These include:

- The right to object, on request and free of charge, to the processing of personal data relating to him or her when the controller anticipates to process these data for the purposes of direct marketing or any other form of research;
- The right to be informed before personal data relating to him or her are disclosed for the first time to third parties for the purposes of direct marketing, or for use on behalf of third parties; and
- The right to object to such disclosure or uses, free of charge.

[68] Available at: http://www.anacom.pt/render.jsp?contentId=164733.

[69] For more information on the 2002 EU Directive on Privacy and Electronic Communications, see Chapter 7.

[B] Restrictions to Direct Marketing Under the Electronic Commerce Law

[1] Prohibited Message Types

Article 22 of the Electronic Commerce Law regulates the use of messaging capabilities for direct marketing purposes when the receipt of a message is independent of the intervention of the recipient. The types of regulated messages include, for example, messages sent, or calls made, through automatic calling machines, facsimile machines, e-mail, short message service, or multimedia message service.[70]

[2] Basic Rule

The basic rule is that the use of automatic calling machines, facsimile machines, e-mail, short message service or multimedia message service, for direct marketing purposes, is permitted only when the data subject has given his or her prior consent.[71]

The prohibition does not apply to messages sent to legal entities. However, recipients of such messages are entitled to take advantage of the opt-out system laid out in the Law.[72]

[3] Exception for Preexisting Relationship

The supplier of a product or service is permitted to send advertising with respect to its products and services to customers to whom it has previously sold these products or services, and only if the advertisement pertains to the same products or services as those that the customer originally purchased.[73]

[4] Means of Opting Out

The customer must explicitly be given the opportunity to object to such messaging and there must not be any charges for the recipient in

[70] Electronic Commerce Law, Article 22(1).
[71] Electronic Commerce Law, Article 22(1).
[72] Electronic Commerce Law, Article 22(2).
[73] Electronic Commerce Law, Article 22(3).

addition to the telecommunication service cost.[74] The recipient must be granted access to the appropriate means that allow her to refuse future communications, at any time, freely and without a cause.[75]

[5] Content of the Commercial Message

Each unsolicited communication must indicate an address and an electronic technical means, easy to identify and to use so that the recipient of the service can refuse future communications.[76]

In addition, the law prohibits the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the person on whose behalf the communication is made.[77]

[6] Maintenance of an Opt-Out List

The entities that send direct marketing messages must maintain, on their own or through the entities that represent them, an updated list of persons who have expressed their wish not to receive such advertising communications.[78]

The *Direcção General do Consumidor* or DGC (General Consumer Directorate) is responsible for maintaining an updated national list of individuals who have expressed their wish not to receive such advertising communications.[79] This list is updated when individuals send a request to be added to the "opt-out list" through an electronic application form available through the website of the General Consumer Directorate.[80]

Entities that send messages for direct marketing purposes must consult the opt-out list, which is updated every quarter by the General Consumer Directorate and is made available upon request.[81] The law prohibits sending advertising communications by electronic means to persons included in the opt-out list.[82]

---

[74] Electronic Commerce Law, Article 22(3).
[75] Electronic Commerce Law, Article 22(4).
[76] Electronic Commerce Law, Article 22(6).
[77] Electronic Commerce Law, Article 22(5).
[78] Electronic Commerce Law, Article 22(7).
[79] Electronic Commerce Law, Article 22(8).
[80] Electronic Commerce Law, Article 22(9).
[81] Electronic Commerce Law, Article 22(10).
[82] Electronic Commerce Law, Article 22(11).

§ 50.07 ELECTRONIC COMMUNICATIONS

The processing of data concerning phone calls, location data and other related kind of data is regulated by the Data Protection Act and by Law No. 41/2004[83] and Law No. 32/2008.[84]

Law No. 41/2004 concerns the processing of personal data and the protection of privacy in the electronic communications sector. It transposes the 2002 EU Directive on Privacy and Electronic Communications into the laws of Portugal.[85]

Law No. 32/2008 concerns the retention of data from, or processed in the context of, electronic communications available to the public, for the investigation, detection and control of serious crimes against the security of the Country and others such as terrorism, violent crimes, organized crimes, kidnapping, abduction and the taking of hostages. The law transposes the 2006 EU Data Retention Directive into the Portuguese legal framework.[86] Implementing Order No. 469/2009 sets out the technical and security conditions of the electronic communications for the purposes of the communication of the traffic and location data concerning a natural person and the legal person to the competent authorities provided in Law No. 32/2008, when required by a judicial order.

[A] What Is Prohibited

The laws define different types of prohibitions that depend on the type of communication. The laws distinguish telephone communications, traffic data, and location information.

[1] Phone Calls

Law No. 41/2004 prohibits listening, tapping, storage, or other kinds of interception or surveillance of communications and the related traffic data by persons other than users without the prior and explicit consent of

[83] http://www.anacom.pt/render.jsp?contentId=227522.

[84] http://www.anacom.pt/render.jsp?contentId=820279.

[85] For more on the 2002 EU Directive on Privacy and Electronic Communications, see Chapter 7.

[86] For more information on the 2006 EU Data Retention Directive, see Chapter 8.

the users concerned. There are exceptions to this prohibition under applicable law, such as in the context of a criminal investigation.

The National Data Protection Commission issued Opinion No. 629/2010, of September 13, 2010 in order to clarify that the processing of data regarding the record of phone calls is subject to the prior and explicit consent of the data subject and prior authorization from this Commission.

[2] Traffic Data

Law No. 41/2004 requires that traffic data relating to subscribers and users that have been processed and stored by the entities providing electronic communications networks and/or services be erased or made anonymous when no longer needed for the transmission of the communication.[87] Traffic data may be processed for billing purposes.

Law No. 32/2008 requires the retention of traffic data for the investigation, detection and prosecution of serious crimes in a separated and blocked folder.[88] The data must be retained for one year[89] after which the data must be erased.

[3] Location Information

Law No. 41/2004 requires that location data other than traffic data relating to subscribers or users of public communications networks or publicly available electronic communications services, be processed anonymously. However, it permits the processing of location data to the extent, and for the duration, necessary for the provision of a value-added service. In this case, the user must have given his prior consent.

According to Law No. 32/2008, the location information must be retained for the investigation, detection, and prosecution of serious crimes. The data must be kept in a separated and blocked folder[90] for one year, after which the data must be erased.[91]

---

[87] Law No. 41/2004, Article 6(1).
[88] Law No. 32/2008, Article 3(3).
[89] Law No. 32/2008, Article 6.
[90] Law No. 32/2008, Article 3(3).
[91] Law No. 32/2008, Article 6.

[B] Requirements

There are also different requirements that depend on the type of information. The laws distinguish telephone communications, traffic data, and location information.

[1] Phone Calls

Under Law No. 41/2004, the prohibition of the listening, tapping, storage, or other kinds of interception or surveillance of communications and the related traffic data by persons other than users does not apply to any legally authorized recording of communications and the related traffic data. This is only the case if the listening, tapping, storage or other activity has been carried out in the course of lawful business practice in order to provide evidence of a commercial transaction, or of any other communication that was made in the scope of a business relationship. In addition, the data holder must have been informed of the recording and must have given his consent.[92] Moreover, Law No. 41/2004 authorizes the recordings of communications by, and for public services intended to provide for emergency help.

Law No. 32/2008 requires providers of public electronic communications services or of public communications networks to retain data related to electronic communications for the investigation, detection, and prosecution of serious crimes. These data must be retained in a separated and blocked folder only accessible to specially authorized persons. The providers of publicly available electronic communications services, or of public communications networks, must adopt security measures that will ensure the protection and confidentiality of the data against loss and unauthorized access.

The data must be transmitted to the competent authorities when required by a judicial order. This transmission must be done through electronic communication and be subject to the technical and security measures that are be set forth by government regulation.

[92] Law No. 41/2004, Article 4(3).

[2] Traffic Data

Law No. 41/2004 allows the processing of traffic data in connection with billing and payments. Only the processing of specified traffic data necessary for billing the subscriber or computing the interconnection charges is permitted, namely:[93]

- Number or identification, address and type of subscriber;
- Total number of units to be charged for the accounting period, as well as the type, starting time and duration of the calls made and/or the data volume transmitted;
- Date of the call or service and called number;
- Other information concerning payments such as advance payment, payments by installments, disconnection, and reminders.

However, the processing of traffic data is only permitted up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.[94]

Companies providing electronic communications services may process the traffic data relating to subscribers and users to the extent and for the duration necessary for marketing electronic communications services or providing value-added services. The subscriber or user to whom the data relate must have given his prior consent. The subscriber may withdraw his consent at any time.[95]

The processing of traffic data must be restricted to employees who are responsible for handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.[96]

---

[93] Law No. 41/2004, Article 6(2).
[94] Law No. 41/2004, Article 6(3).
[95] Law No. 41/2004, Article 6(4).
[96] Law No. 41/2004, Article 6(5).

The above-mentioned restrictions do not affect the ability of courts or other competent entities to have access to traffic data, pursuant to the rules set forth in the relevant legislation, namely in cases concerning interconnection or billing disputes.[97]

Law No. 32/2008 requires that the traffic data be retained only for the investigation, detection, and prosecution of serious crimes.[98] These data must be retained in a separated and blocked folder only accessible to specifically authorized persons. The providers of publicly available electronic communications services or of public communications networks must adopt security measures that will ensure the protection and confidentiality of the data against loss and unauthorized access.[99]

Data must be transmitted to the competent authorities when required by a judicial order.[100] The transmission of the data to the competent authorities must be done through electronic communication and will be subject to technical and other security measures that are to be set forth by government regulation.

Implementing Order No. 469/2009 requires the adoption of the following measures when communicating data within Law No. 32/2008:

- The judge must request the communication of the data through a specific electronic application that includes the corresponding judicial order authorizing such communication of data;
- Each communication must bear an electronic signature;
- Each communication must be encrypted;
- Each request of communication of data must be registered;
- The computer application must be audited.

[3] Location Information

The entities with legal competence to deal with emergency calls may record, process and transmit the location data for responding to such calls.[101]

---

[97] Law No. 41/2004, Article 6(7).
[98] Law No. 32/2008, Article 3(1).
[99] Law No. 32/2008, Article 7.
[100] Law No. 3/2008, Article 9.
[101] Law No. 41/2004, Article 7(2).

The processing of location data is also permitted to the extent and for the duration necessary for the provision of a value-added service, if the prior consent of the subscribers or users has been given.[102]

Companies providing publicly available electronic communications services must, *inter alia*, inform the users or subscribers, before obtaining their consent, of the type of location data that will be processed, of the duration and purposes of the processing and whether the data will be transmitted to a third party for providing the value added service.[103]

Entities that provide publicly available electronic communications services must give subscribers and users, using a simple means and be free of charge, the possibility:[104]

- To withdraw their previous consent at any time for the processing of location data referred to in the preceding paragraphs; and
- To temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

The processing of location data must be restricted to employees of entities that provide electronic communications networks and/or publicly available services, or third parties that provide the value-added service. This processing must be restricted to what is necessary for the purposes of the referred activity.[105]

Law No. 32/2008 requires that the location data be retained only for the investigation, detection, and prosecution of serious crimes. These data must be retained in a separated and blocked folder only accessible to specially authorized persons.[106] The providers of publicly available electronic communications services or public communications networks must adopt security measures that will ensure the protection and confidentiality of data, against loss and unauthorized access.[107]

Data must be transmitted to the competent authorities when required by a judicial order.[108] The transmission of the data to the competent

[102] Law No. 41/2004, Article 7(3).
[103] Law No. 41/2004, Article 7(4).
[104] Law No. 41/2004, Article 7(5).
[105] Law No. 41/2004, Article 7(6).
[106] Law No. 32/2008, Article 7(2).
[107] Law No. 32/2008, Article 7.
[108] Law No. 32/2008, Article 9.

authorities must be done through electronic communication and will be subject to technical and security measures that are to be set forth by government regulation.

[C] Enforcement; Lawsuits; Penalties

The National Data Protection Commission initiates, examines, and rules on breach proceedings. In addition, it may assess fines on grounds of non-compliance with legal requirements concerning the recording of communications and the related traffic data, and location data.[109]

The violation of the obligation of confidentiality, the prohibition of interception or surveillance of communications and the related traffic data may be fined from EUR 1,500 to EUR 25,000 for individuals and from EUR 5,000 to EUR 5,000,000 for legal persons.

Failure to comply with the conditions concerning the processing and storage of traffic data and location data exposes to a fine from EUR 500 to EUR 20,000 for individuals and from EUR 2,500 to EUR 2,500,000 for legal persons.

Law No. 32/2008 contains fines for the violation of the duty to retain information, or the violation of the duty to retain information for the specified period of time of one year, the violation of the duty to transmit information to the competent authorities, and the violation of the duty to provide the data to the specially authorized people. These violations are punishable with a fine between EUR 1,500 to EUR 50,000 for individuals, and between EUR 5,000 to EUR 10,000,000 for legal entities.[110]

The violation of the rules related to the protection and security of the data, blocking the data and the prohibition of access by persons who are not specially authorized to do so, may expose the violator to up to two years of imprisonment or a fine up to EUR 240. The penalty is doubled if the crime is perpetrated through violation of technical measures, or if the crime has made personal data available to third parties, or has brought economic advantage to third parties.[111]

[109] Law No. 41/2004, Article 15.
[110] Law No. 32/2008, Article 12.
[111] Law No. 32/2008, Article 13(2).

§ 50.08 WHISTLEBLOWING

The Portuguese legal system does not have any specific law concerning whistleblowing procedures. Nevertheless, the National Data Protection Commission has issued Opinion No. 765/2009, on September 21, 2009, on the rules applicable to the data processing related to internal whistleblowing schemes. In general terms, the National Data Protection Commission follows the orientations of the Article 29 Working Party on this matter (Opinion 1/2006):

- These schemes, which are subject to the prior authorization of the National Data Protection Commission, may only be adopted in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking, and financial crime.
- Promotion of identified and confidential reports as against anonymous reports, in compliance with the data protection essential requirement that data should only be collected fairly.
- As to the rights of an incriminated person, from a data protection point of view, the data controller must assure the data subjects' rights of information, access, and rectification.
- Data processed by a whistleblowing scheme shall be deleted: (i) within 6 months of completion of the investigation of the facts, (ii) in case of a legal proceeding, data shall be kept until the conclusion of these proceedings, (iii) data related to alerts found to be unsubstantiated should be deleted without delay.

The preliminary management and review of the reports shall be conducted by an independent auditing entity. This entity may be (i) a specific internal organization or (ii) a third independent party, in which case the rules related to the employment of a data processor and transfer of data shall apply.

§ 50.09 SECURITY BREACH DISCLOSURE LAWS

The Portuguese legal system does not have any specific law concerning security breach disclosures.

Nevertheless, with the approval of the Directive 2009/136/CE in November of 2009, which amends the so-called "ePrivacy Directive," all

telecommunications operators will be obliged to immediately notify the relevant entities and individuals of the occurrence of a security breach.

This Directive is to be transposed to the Portuguese legal framework by May 2011.

§ 50.10 OTHER LAWS PROTECTING PERSONAL DATA

Numerous other laws address the protection of personal data. For example:

- Decree-Law No. 35/2004, of February 21, 2004 (concerning the processing of personal data in the context of video surveillance), amended by the Decree-Law No. 198/2005, of November 10, 2005 and Law No. 38/2008, of August 8, 2008.
- Law No. 1/2005, of January 10, 1995 (concerning the processing of personal data in the context of video surveillance).
- Law No. 51/2006, of August 29, 2006 (concerning the processing of personal data in the context of video surveillance).

law. These fines range from several hundred Euros to over half a million Euros. The law distinguishes different forms of infringements.

On February 16, 2011, Spain adopted amendments to its current data protection law, which can be found at http://www.congreso.es/public_oficiales/L9/CONG/BOCG/A/A_060-18.PDF. These amendments define new types of violations, and new sanctions. Complete up-to-date detailed information will be provided in Supplement #6.

[1] Types of Infringement

Infringements are classified as minor, serious, and very serious. The following are deemed as "minor infringements."[59]

- Failure to respond, for formal reasons, to a request by a data subject for the rectification or cancellation of personal data subject to processing, when that request is justified in law.
- Failure to provide the information requested by the Data Protection Agency in the exercise of the functions assigned to it by law, with regard to non-substantive aspects of data protection.
- Failure to request the entry of the file of personal data in the General Data Protection Register, where this does not amount to a serious infringement.
- Collection of personal data on data subjects without providing them with the information set out in Article 5 of Organic Law 15/1999.
- Failure to respect the duty of secrecy set out in Article 10 of Organic Law 15/1999, where this does not amount to a serious infringement.

The following are deemed "serious infringements":[60]

- Creating files in public ownership, or initiating the collection of personal data for such files, without the authorization published in the *Boletín Oficial del Estado* or the corresponding official gazette;

[59] Organic Law 15/1999, Articles 33.1 and 44.2.
[60] Organic Law 15/1999, Articles 33.1 and 44.3.

- Creating files in private ownership, or initiating the collection of data for such files, for purposes other than the legitimate purposes of the undertaking or body;
- Collecting personal data without obtaining the explicit consent of the data subjects, where it has to be obtained;
- Processing personal data or subsequently using them in infringement of the principles and guarantees laid down in Organic Law 15/1999, and failure to respect the protection laid down by the implementing provisions, where this does not amount to a very serious infringement;
- Preventing or hindering the exercise of the rights of access and objection, and refusing to provide the information asked for;
- Maintaining incorrect personal data or failure to rectify or cancel such data when legally obliged if the citizens' rights protected by Organic Law 15/1999 are affected;
- Breach of the duty of secrecy for personal data incorporated into files containing data on the commission of administrative or criminal offenses, public finance, financial services, provision of creditworthiness and credit services, as well as other files containing a set of personal data sufficient to obtain an assessment of the personality of the individual;
- Maintaining files, premises, programs or hardware containing personal data without the security required by regulations;
- Failure to send the Data Protection Agency the notifications laid down in Organic Law 15/1999 or in its implementing provisions, and not providing it, on time, with any documents and information due to it or that it may require to this end;
- Impeding inspections;
- Failure to enter a file of personal data in the General Data Protection Register when this has been required by the Director of the Data Protection Agency;

- Failure to comply with the duty of information laid down in Articles 5, 28 and 29 of Organic Law 15/1999, when the data have been obtained from a person other than the data subject.
- The following are deemed "very serious infringements";[61]
- The misleading or fraudulent collection of data;

[*Next page is 58-27.*]

[61] Organic Law 15/1999, Article 44.4.