ICLG

The International Comparative Legal Guide to:

Data Protection 2015

2nd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

A.G. Erotocritou LLC
Adsuar Muñiz Goyco Seda & Pérez-Ochoa, P.S.C.
Affärsadvokaterna i Sverige AB
Brinkhof
Cuatrecasas, Gonçalves Pereira
Dittmar & Indrenius
ECIJA ABOGADOS
ELIG, Attorneys-at-Law
Eversheds
Gilbert + Tobin
Gorodissky & Partners
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams LLP
Juridicon Law Firm
Jurisconsul
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio
& Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

GLG
Global Legal Group

GLG
Global Legal Group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Head of Business Development
Dror Levy

Sales Director
Florjan Osmani

Commercial Director
Antony Dine

Account Directors
Oliver Smith, Rory Smith

Senior Account Manager
Maria Lopez

Sales Support Manager
Toni Hayward

Sub Editor
Amy Hirst

Senior Editor
Suzie Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
May 2015

ISBN
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Chapter 22

Portugal

Cuatrecasas, Gonçalves Pereira

Leonor Chastre

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Portugal is, essentially, regulated by Law 67/98 of October 26 ("Data Protection Act"), which transferred into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

1.2 Is there any other general legislation that impacts data protection?

There are a few more laws in Portugal which impact data protection, e.g.:

- Constitution of the Portuguese Republic - Article 35 (use of computerised data).
- Act 2/94 of 19 February - establishes the control and verification mechanisms for the Schengen Information System (SIS).
- Law 46/2012 of 29 August transposes the part of Directive 2009/136/EC amending Directive 2002/58/EC of the European Parliament and of the Council of 12 July, concerning the processing of personal data and the protection of privacy in the electronic communications sector, introducing the first amendment to Law 41/2004, of 18 August, and the second amendment to Law 7/2004, of 7 January.

1.3 Is there any sector specific legislation that impacts data protection?

The Portuguese health, bank and insurance sectors are subject to additional and specific statutory restrictions in relation to data protection due to their sensitive nature.

1.4 What is the relevant data protection regulatory authority(ies)?

Data Protection Law has created the *Comissão Nacional de Protecção de Dados* - Portuguese Data Protection Authority - ("CNPD") as the empowered body to supervise and monitor the compliance with laws and regulations within the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in Portuguese law.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  "Personal Data" means any information of any type, irrespective of the type of medium involved, including sounds and images, relating to an identified or identifiable natural person ("data subject").
- **"Sensitive Personal Data"**

  Article 7 of the Data Protection Law defines "Sensitive Personal Data" as any personal data revealing one's philosophical or political beliefs, political affiliations or trade union membership, religion, private life and racial or ethnic origin and also data concerning health or sex life, including genetic data.
- **"Processing"**

  "Processing" means any operation or set of operations which is performed upon personal data, whether wholly or partly by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- **"Data Controller"**

  "Data controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by laws or regulations, the controller shall be designated in the Act establishing the organisation and functioning or in the statutes of the legal or statutory body competent to process the personal data concerned.
- **"Data Processor"**

  "Data processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
- **"Data Owner"**

  The term "Data Owner" is not used and there is no analogous concept in the Data Protection Act.

- **"Data Subject"**

  "Data Subject" means an identifiable person who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

- **"Pseudonymous Data"**

  The term "Pseudonymous Data" is not used and there is no analogous concept in the Data Protection Act.

- **"Direct Personal Data"**

  The term "Direct Personal Data" is not used and there is no analogous concept in the Data Protection Act.

- **"Indirect Personal Data"**

  The term "Indirect Personal Data" is not used and there is no analogous concept in the Data Protection Act.

- **"Personal Data Filing System"**

  "Personal Data Filing System" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

- **"Third Party"**

  "Third Party" means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

- **"Recipient"**

  "Recipient" means a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a law shall not be regarded as recipients.

- **"The Data Subject's Content"**

  "The Data Subject's Consent" means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

- **"Combination of Data"**

  "Combination of Data" means a form of processing which consists of the possibility of correlating data in a filing system with data in a filing system or systems kept by another or other controllers or kept by the same controller for other purposes.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  The processing of personal data shall be carried out transparently and in strict respect for privacy and for other fundamental rights, freedoms and guarantees.

- **Lawful basis for processing**

  The Data Protection Act governs each of the collection, holding, use, disclosure, access and correction of personal information by CNPD entity.

- **Purpose limitation**

  The persons who are reported shall only be those who perform management acts regarding accounting, internal control of accounting, auditing, and the fight against corruption and banking and financial crime.

  Therefore, the majority of employees cannot be a data subject under this system, as they do not perform management functions or acts.

- **Data minimisation**

  This is not applicable in Portugal.

- **Proportionality**

  Under the Data Protection Act, the CNPD ensures that the personal information is accurate, up-to-date, complete and relevant.

- **Retention**

  In accordance with the Portuguese Data Protection Authority's decision, the personal data shall be deleted:

  (i) immediately, when they are revealed to be incorrect or unreasonable;

  (ii) within six months from the closing of the investigations, when no disciplinary or judicial proceeding will take place; or

  (iii) immediately after the end of the judicial or disciplinary proceeding, under a restricted access information system.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  The data must be available for immediate access, with no excessive costs, by the Data Subject. Furthermore, the right of access must be exercised before the Data Controller or, if applicable, the Data Processor.

  This right comprises three exceptions:

  (i) medical data, including genetic data, access to which must be exercised only by a Doctor appointed by the Data Subject;

  (ii) police data, access to which is through the CNPD; and

  (iii) the data for journalistic use and/or artistic or literary purposes, access to which must be performed through the CNPD.

- **Correction and deletion**

  The Data Subject has the right to demand that his data are updated and exact. He also has the right to demand that his data are eliminated from the processing for marketing purposes. The Data Subject may exercise this right by contacting the Data Controller or Data Processor.

- **Objection to processing**

  The Data Subject may oppose the processing of his data for Direct Marketing, for Company Marketing and also that his data is communicated to third parties.

- **Objection to marketing**

  The Data Subject can oppose the processing of personal data for marketing purposes. To do so, it's necessary to send a letter to the company concerned, expressing your right to object to receiving more mail and wait a reasonable time for the company to withdraw from the listing of mailings. In case the receiving of mail persists from the same company, the Data Subject should complain to the CNPD.

  If the Data Subject does not wish to receive, in general, this type of mail, it is possible to request that its name and address are included in the designated "Robinson lists", in charge of the Direct Marketing Association.

- **Complaint to relevant data protection authority(ies)**

  Although the right to submit a complaint to the CNPD is not foreseen as a specific right of the data subject, Portuguese law determines that any individual (including the data subject) may have recourse to administrative and legal means to guarantee the compliance with legal provisions in the area of data protection.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

The authorisation of the CNPD is required for:

(a) the processing of sensitive personal data and that relating to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties;

(b) the processing of personal data relating to credit and the solvency of the data subjects;

(c) the combination of personal data not provided for in a legal provision; and

(d) the use of personal data for purposes not giving rise to their collection.

The processing referred above may be authorised by legal ruling, in which case it does not require the authorisation of the CNPD.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

The registrations/notifications are made per processing purpose.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

This Act shall apply to the processing of personal data wholly or partly by automatic means, and to the processing other than by automatic means of personal data which form part of manual filing systems or which are intended to form part of manual filing systems.

This Act shall not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity.

This Act shall apply to the processing of personal data carried out:

(a) in the context of the activities of an establishment of the controller on Portuguese territory;

(b) outside national territory, but in a place where Portuguese law applies by virtue of international public law; and

(c) by a controller who is not established on European Union territory and who for purposes of processing personal data makes use of equipment, automated or otherwise, situated on Portuguese territory, unless such equipment is used only for purposes of transit through the territory of the European Union.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

As for the filing requirements, the CNPD has an official form that must be submitted in Portuguese with the following information:

- Identity of the controller and its representative.
- Main software features.
- The purposes of the processing.
- Third party entity responsible for the processing (if applicable).
- All the personal data that will be collected in each register; it is also necessary to indicate if sensitive data is to be collected as well as data concerning the suspicion of illegal activities, criminal and/or administrative offences, as well as data regarding credit and solvability.
- Grounds of legitimacy of the collection and a brief description of the data collection method used.
- Means and methods available for updating the data.
- Means of communication of data to other entities and their identification (if applicable).
- Any transfers of data to third countries, listing the reasons, grounds and the measures adopted in each transfer.

5.5 What are the sanctions for failure to register/notify where required?

The Data Protection Law foresees several Administrative Offences, for which fines vary from €250 to up to €15,000.

If the Data Controller does not notify the CNPD of the processing, or if the notification is inaccurate, then it will be liable to be fined at:

- a minimum of €250 and a maximum of €2,500 – if the Data Controller is a natural person; or
- a minimum of €1,500 and a maximum of €15,000 – if the Data Controller is a Corporate Entity.

Please note that these fines may be increased to up to the double of their amount, if the data being processed required previous authorisation.

5.6 What is the fee per registration (if applicable)?

The notification procedure involves the payment of a notification fee of 75 Euros or 150 Euros, depending on whether the processing is, respectively, a simple register or is subject to prior authorisation.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

The registrations/notifications only need to be renewed if and when any change in the following information occurs:

- Controller of the file and his representative, if any.
- Categories of personal data processed.
- Purposes of the data and categories of body to whom they might be disclosed.
- Form of exercising the right of access and rectification by the data subject.
- Combinations of personal data processing.
- Transfers of data to third countries.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

Prior authorisation is mandatory when:

(i) there are sensitive data;

(ii) personal data relates to persons suspected of illegal activities, criminal and administrative offences;

(iii) data relates to credit and solvency of the data subjects;

(iv) data is combined with other databases owned by a different controller; or

(v) data is collected without disclosing its purpose.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

In order to obtain prior approval it is necessary to file a legalisation form, pay the corresponding fees (in the amount of 150 Euros) and deliver the form to the CNPD. The filing and delivery of the legalisation form can be performed online.

Portuguese law does not foresee any timeframe for the issuance of the authorisations. According to our experience, except for purposes of video surveillance, phone call recordings, medicine at work and control of the use of telephone, e-mail and internet at work (which are handled more quickly), a decision from the CNPD should not be expected in less than six months.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

There is no legal requirement in Portugal for organisations to appoint a Data Protection Officer.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not applicable in Portugal.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

This is not applicable in Portugal.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in Portugal.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

This is not applicable in Portugal.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable in Portugal.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, e-mail, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

The Law No. 41/2004, of 18 August on the protection and processing of personal data in e communications was recently amended by Law no. 46/2012, of 29 August, which transposed the 2009/136/EC Directive.

In relation to individuals, the sending of unrequested communications for direct marketing purposes is subject to express prior consent of the subscriber or user (that is, the "opt in" rule applies). This includes the use of automated calling and communication that do not rely on human intervention (automatic call devices), facsimile or electronic mail, including SMS, EMS, MMS and other similar applications.

This does not apply to legal entities and accordingly unrequested direct marketing communications are allowed. Nevertheless, the "opt out" rule applies and legal entities may refuse future communications and enroll in the non-subscribers list.

This does not prevent the supplier of a product or service that has obtained its customers' data and contacts, under the lawful terms of the Data Protection Law and in connection with the sale of a product or service, to use such data for direct marketing of its own products or services similar to those transacted, provided it ensures the customers concerned, clearly and explicitly, with the opportunity to object to the use of such data, free of charge and in an easy manner:

- at the time of the respective collection; and
- on the occasion of each message in case the customer has not initially refused such use.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The sending of electronic mail for purposes of direct marketing disguising or concealing the identity of the entity on whose behalf such communication is made, as well as the non-indication of valid means of contact to which the recipient may send a request to stop these communications or the encouragement of recipients to visit websites that violate these provisions, is strictly forbidden.

7.3 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The violation of these rules is an administrative offence, punishable with fines ranging from 5,000 Euro to 5,000,000 Euro, for legal entities.

7.4 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

The Law requires that companies obtain prior consent for placing cookies on users' equipment except when the cookie is used solely for the purpose of carrying out the transmission of a communication over an electronic communications network or is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

The Law also requires prior explicit consent for direct marketing; companies and representatives must maintain a log of an up-to-date list of individuals who have given explicit consent to receive direct marketing communications. The log must also contain a list of customers who do not object to receiving direct marketing messages when opt-out is considered legally sufficient, for example when provided by contractual terms. Companies offering electronic communications services are now obliged to notify the CNPD in the event of a personal data breach without undue delay.

7.5 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

At this point, the local regulatory Authority (CNPD) has not yet issued any guidelines regarding the definition of "consent", namely if implied consent suffices and if the continuous use of a website implies consent. In view of Portuguese practice and the restrictive approach taken by the DPA, the implied consent shall not be enough and continuous use of a website shall only be regarded as consent provided clear and evident information is given. The use of a confirmation procedure is advisable.

7.6 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

To date, the Data Protection Authority has not taken any enforcement action in relation to cookies.

7.7 What are the maximum penalties for breaches of applicable cookie restrictions?

The CNPD and ICP-ANACOM are empowered to issue fines of up to 5 million Euro and to seize any equipment, devices, or materials used to commit the infraction. Delays in complying with any orders or requests from the CNPD or ICP-ANACOM may also attract a fine of up to 100,000 Euro for each day up to a maximum of 3,000,000 Euro (30 days' delay).

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

Without prejudice to the tax or customs decisions of the Community, personal data may move freely between Member States of the European Union.

The transfer to a State which is not a member of the European Union of personal data which are undergoing processing or are intended for processing may only take place subject to compliance with this Act and provided the State to which they are transferred ensures an adequate level of protection.

The adequacy of the level of protection of a State which is not a member of the European Union shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the State in question and the professional rules and security measures which are complied with in that country.

It is for the CNPD to decide whether a State which is not a member of the European Union ensures an adequate level of protection.

By means of the Ministry of Foreign Affairs the CNPD shall inform the European Commission of cases where it considers that a State does not ensure an adequate level of protection.

The transfer of personal data identical to those the European Commission has considered do not enjoy adequate protection in the State to which they are to be sent shall be prohibited.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

A transfer of personal data to a State which does not ensure an adequate level of protection within the meaning of Article 19, of Law 67/98 may be allowed by the CNPD if the data subject has given his consent unambiguously to the proposed transfer or if that transfer:

(a) is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;

(b) is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party;

(c) is necessary or legally required on important public interest grounds, or for the establishment, exercise of defence of legal claims;

(d) is necessary in order to protect the vital interests of the data subject; or

(e) is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

Without prejudice to the above paragraph the CNPD may authorise a transfer or a set of transfers of personal data to a State which does not ensure an adequate level of protection within the meaning of Article 19, provided the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise, particularly by means of appropriate contracts. The authorisations provided for shall be granted or derogated by the CNPD according to its own procedures and the decisions of the European Commission clauses.

By means of the Ministry of Foreign Affairs the CNPD shall inform the European Commission and the competent authorities of the other Member States of the European Union of the authorisations it grants.

Whenever there are specimen contractual clauses approved by the European Commission according to its own procedures, because they provide the adequate guarantees referred, the CNPD shall authorise the transfer of personal data made under such clauses.

A transfer of personal data which is necessary for the protection of State security, defence, public safety and the prevention, investigation and prosecution of criminal offences shall be governed by special legal provisions or by the international conventions and agreements to which Portugal is a party.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

For data transfers performed within the EU/EEA countries, it is only required to notify the CNPD and data processing may commence immediately thereafter.

Transfers to non EU/EEA countries can only take place if the recipient country ensures an adequate level of protection. In any case it is mandatory to start an authorisation procedure with the CNPD and data processing can only commence upon the authorisation issuance.

Exceptionally, transfers performed according to the standard Model Clauses or to Safe Harbor Certificate holders are possible. In such cases, data processing can be done immediately after filing with the CNPD.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

The CNPD has issued Decision No. 765 /2009 on the principles applicable to the processing of personal data for the purposes of internal communication of irregular management and financial acts (whistleblower hotlines).

The Portuguese DPA has considered that the legitimate purpose in this matter is the management of whistle-blowing of irregular acts, in order to prevent and/or repress irregularities such as corruption, banking and financial crime and matters affecting accounts, internal account controls and auditing.

In order to obtain the mandatory prior authorisation for the processing, the Data Controller must prove that it is necessary for the execution of legitimate purposes, provided that no fundamental rights of the data subject prevail.

The Data Controller must be individually identified, and the Portuguese DPA will only admit co-controllers where there is a case of absolute impossibility to determine individually the responsibility for the processing. The data controller is, therefore, considered as the company which adopts internal procedures and ensures means that allow the whistle blowing and subsequent investigations of behaviours contrary to the law or company's policies, and ultimately decides if the complaint will be sent for disciplinary or judicial proceeding. Hence, the data controller must establish the rules applicable to the communication and processing of complaints, appointing those people or bodies which are especially responsible for the collection and processing of complaints – they must be in a limited number, with technical education and subject to strict confidentiality obligations contracted.

The data processor, if any, must assume, by means of contract the liability of not using the data for other purposes than those authorised, to guarantee the confidentiality of data, respect the deadline for its preservation and record, and to destroy all physical or electronic records of personal data in the term of the contract with the data controller.

Nonetheless, the data controller is still bound by an obligation of result regarding the protection of quality or safety of personal data.

In this matter, the company must ensure that an agreement in the above conditions is entered into with the Data Processor (contractor), if that is the case.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

Anonymous whistleblowers are not allowed by the Portuguese Data Protection Authority, so as to prevent the risks of slanderous complaints and discrimination. Instead, a confidentiality regime should be adopted by the data controller.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

See the answers to questions 9.1 and 9.2 above.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Yes. A specific form must be filed and delivered to the CNPD.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

According the Recommendations of the Portuguese DPA regarding the monitoring of employees in the workplace the monitoring of phone calls, e-mail and Internet access, is permitted as follows:

Phone calls

The employer shall define with accuracy the level of tolerance regarding the use of the telephones and the forms of control adopted. However one should not think, in a simple manner, that employees could be prevented from responding to needs strictly private that correspond to the way our society is structured.

In case monitoring of phone calls take place, other data than that which is strictly necessary to achieve the purpose of the control shall not be processed. The processing shall be limited to the user identification, his/her rank/function in the corporation, the number called, the type of call (local, regional or international), the continuance of the call and cost.

Undue access to communications, the use of any tapping device, storage, interception and surveillance of the communications by the employer is forbidden.

In the cases foreseen by law that require the recording of phone calls, in order to document a business declaration and prove its validity and efficacy, this "interception" can only occur with the prior consent of the users, or legal provision.

Use of e-mail and Internet access

The employer shall set up clear and precise rules on the use of e-mail and Internet access for private purposes, which shall be based

on the principles of adequacy, proportionality, mutual collaboration and reciprocal trust.

These rules shall be submitted to the opinion of the employees and their representatives, being expressly publicised, in order to assure good information about the level of tolerance and about the consequences of non-compliance with the rules.

It is advisable that the employer allows the employees to use, in moderate and reasonable terms, the new technological means made available to them.

The system administrator is bound to the obligation of professional secrecy and cannot disclose to third parties the employees' private information that comes to his knowledge within the scope of monitoring.

Specific principles for the use of e-mail

Even in the case of the employer prohibiting the use of e-mails for private purposes, this doesn't give the employer the right to open, automatically, the e-mails addressed to the employee.

The monitoring powers of the employer shall be made compatible with the rights of the employees, in order to assure that intrusions can be avoided. The employer shall therefore choose non-intrusive control methods, according to the principles previously defined and being of the employees' knowledge.

The employer shall not undertake a permanent and systematic monitoring of the employees' e-mail. The control shall be punctual and towards the areas or activities that present a greater "risk" for the business.

The specific professional secrecy for some employees (i.e. medical secrecy or protection of the sources in journalism) shall be preserved.

The level of exigency and accuracy in relation to the monitoring of received and sent e-mails shall be clearly distinctive. Also the reasons for opening the mailbox of the employee in case of a long absence (holidays or illness) shall be clearly expressed and completed with the employee's prior knowledge.

The monitoring of e-mails shall mainly aim to guarantee the security of the system and its performance. The employer may also adopt the necessary procedures – always with the knowledge of the employees – to filter certain files that may not be professional e-mails (.exe Files, mp3 or image files). The detection of a virus does not justify the reading of the e-mails received.

Eventual monitoring for prevention or detection of commercial secrets disclosure shall be directed exclusively for the employees with access to those secrets and only when there are strong suspicions.

The access to the employee's e-mail shall be the last recourse to be used by the employer, and it should be done in the presence of the employee concerned. The access shall be limited by watching the addresses of the recipients, the subject, the date and hour. The employee – if it is the case – may specify the existence of e-mails of A private nature and object to their reading by the employer. In the face of this opposition, the employer shall refrain from viewing the content of the e-mail.

Principles on Internet access

A certain level of tolerance shall be admitted in relation to Internet access for private purposes, in particular if it occurs out of the working hours.

The employer shall not undertake a permanent and systematic control of Internet access. It shall be done in a global way, not individualised, in relation to all access inside the corporation, with reference to the time of the web connection. It is admissible that the employer processes data about the most acceded websites, but without identifying the place of origin of the access.

Whenever there are reasons of costs and productivity involved, the monitoring shall be done through the counting of the time of connection, independently of the sites visited. If excessive and disproportionate use is verified, the employee shall be warned in respect to his level of use. The control of the time spent daily on the Internet and the websites consulted by the employee shall only occur in exceptional circumstances, in particular when the employee, after the warning, doubts of the employer's indications and wishes to confirm such accesses.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Whenever there is personal data processing for the purpose of monitoring employees, the Data Protection Act's provisions are applicable. The DPA will evaluate all aspects of the data processing – data quality, conditions of processing legitimacy, balancing all the interests involved, assessing the means used by employees and how the right to information is provided, and will set the measures to safeguard the individual freedom of the employees.

The employer shall – before starting any kind of processing – inform the employee about the conditions, under which the means of the corporation may be used for private purposes or the level of tolerance admitted; about the existence of the processing, its purpose, the control methods adopted, the data processed and its storage, as well as the consequences for the misuse of the means of communications made available to the employee.

The data processing and the means of control shall be adequate for the business management, for the development of the productive activity and be compatible with the rights and duties of the employees, and not abusive or disproportionate in relation to the level of protection of the employee's private sphere.

10.4 The employer shall privilege generic monitoring methodologies, avoiding the individual consultation of personal data. To what extent do works councils/ trade unions/employee representatives need to be notified or consulted?

The level of use of the corporation means for private purposes, the delimitation of the conditions for the data processing and the definition of the forms of monitoring adopted shall be included in internal Rules of Procedure, which shall be submitted to the workers council and approved by the Labour Inspection Board.

The employer shall publicise the content of the Rules of Procedure, namely by posting it in the corporation's headquarters and in all other working places, in order to allow the employees to have full knowledge of it.

The employer, as data controller, has to notify the Data Protection Authority of this data processing, sending information the RoP and specifying the ways used to disclose the conditions of the data processing to the employees.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, it does not.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The CNPD has not yet ruled on this issue.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The CNPD has not yet ruled on this issue.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The CNPD has not yet ruled on this issue.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art measures and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Where processing is carried out on his behalf the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.

The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the obligations referred to in section 1 shall also be incumbent on the processor.

Proof of the will to negotiate, the contract or the legal act relating to data protection and the requirements relating to the measures referred to shall be in writing in a supporting document legally certified as affording proof.

Law 41/2004, of 18 of August on the protection and processing of personal data in e-communications was recently amended by Law No. 46/2012, of 29 August, which transposed Directive 2009/136/EC.

Now, companies that offer electronic communications services accessible to the public shall, without undue delay, notify the CNPD of a personal data breach. When the personal data breach may affect negatively the subscribers or users of personal data, companies providing electronic communications services accessible to the public should also, without undue delay, notify the breach to the subscriber or user so that they can take the necessary precautions.

For these purposes, a negative effect on the personal data of privacy exists when the breach may result namely in theft or identity fraud, physical harm, significant humiliation or damage to reputation.

Regardless, if a person/entity is affected by the breach of the Data Protection Law, he/she is entitled to file a claim to the CNPD and/or file a civil lawsuit to seek compensation for damages.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Portuguese law does not foresee any requirements to report data breaches. Nevertheless it foresees a generic duty of cooperation from the private and public bodies, according to which such parties must provide all the information requested by the CNPD. The duty to cooperate shall be insured in particular when in order to exercise its functions in full the CNPD has to examine the computer system and personal data filing systems and all documentation relating to the processing and transmission of personal data.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

The Portuguese law does not foresee any requirements to report data breaches to individuals. Nevertheless, if the data are collected on open networks the data subject shall be informed, except where he is already aware of it, that personal data relating to him may be circulated on the network without security measures and may be at risk of being seen and used by unauthorised third parties.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Power to supervise and monitor compliance with the laws and regulations in the area of personal data. Investigative powers and may have access to data undergoing processing and powers to collect all the information necessary for the performance of its supervisory duties.	Deliberating on the application of fines (administrative sanctions).	This is not applicable.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

According to our experience, although the CNPD is not very proactive in the execution of its supervision and monitoring powers, following a complaint the CNPD is very quick in the beginning of the investigations and in the issuance of decisions.

Also, the CNPD is very strict in the interpretation of the personal data protection laws and regulations and in the protection of the data subjects' rights.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within Portugal respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

In Portugal, this issue is only raised in big group companies. In these cases the reply to foreign e-discovery requests is always limited by compliance with the Portuguese law and regulations on data protection.

15.2 What guidance has the data protection authority(ies) issued?

Although the CNPD has not furnished any specific guidelines on this issue, the implications of e-discovery exercises are relatively easy to identify:

- Furnishing adequate notice to affected Portuguese individuals.
- Ensuring the underlying legitimacy of the collection and processing (and, frequently, international transfer) of personal data.
- Maintaining appropriate limitations or controls on the scope of the data collection exercises.
- Abiding by international data transfer rules.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In its Resolution No 7680/2014, dated 28 October 2014, the Portuguese Data Protection Authority (*Comissão Nacional de Protecção de Dados* (CNPD)) analyses the implications, in terms of employees' data protection and privacy, of geolocation devices in motor vehicles, on the one hand, and in smart mobile devices, on the other, in the scope of employment relations and it establishes the criteria and circumstances under which the processing of personal data concerning geolocation is admissible.

The installation of geolocation devices on the equipment in question may enable the employer to achieve legitimate goals, relating, among others, to achieving efficiency and quality of services, the optimisation of resources or the protection of assets, provided they are not used as a means of locating the whereabouts of the employer or as a tool of monitoring his or her professional performance, which is clearly forbidden by the law (see Article 20 of the Employment Code).

The data relating to the location of the employee, as well as the record of moves and other associated data, constitute information concerning identified or identifiable physical persons, which, because they relate to the private life of the employees, fall within the concept of sensitive data.

The consent of the employee is viewed as unnecessary by the CNPD in order to legitimise the processing of the personal data in question, on account of the situation of imbalance of power that exists in employment relations that does not guarantee that the consent is given freely, which constitutes an essential condition in the light of the Data Protection Law. Accordingly, the processing of sensitive data can only legitimately occur on the basis of a legal provision. Without prejudice to the fact that geolocation in the employment context is not expressly provided for in any provision of the national legal system, since geolocation devices are pieces of technological equipment that monitor the employees remotely, the CNPD considers that the same constitutes remote surveillance, for which reason the Labour Code and the General Law on Public Service Work establish the necessary and indispensable legal provision on which the legitimacy of the data processing must be based.

With regard to its purpose, the CNPD considers admissible the processing of data relating to geolocation, in the case of motor vehicles, for the following purposes: (i) management of fleets on external services (in the areas of activity of external/home technical assistance, distribution of goods, passenger transport, transport of goods and private security); and (ii) protection of goods, in the case of transport of hazardous materials (namely flammable or toxic materials, hazardous waste, weapons, munitions and explosives, medicinal products or drug precursors) and the transport of high-value material (the CNPD has set 10,000 euros as the maximum limit of the value of the cargo carried).

Where the specific purpose of the installation of geolocation devices is to file criminal complaints in case of theft, although the geolocation data are automatically recorded, the employer cannot have access to the data unless the vehicle is stolen.

In the case of portable phones or computers, the CNPD does not permit the employer to monitor the geolocation of those equipments, and the employer cannot have access to such information, even if the same is available from the operators, nor can the employer install applications on the smart mobile devices activating GPS sensors.

Where the processing of these data indicates the committing of a crime, such information can be used as grounds for the corresponding criminal complaint. In the cases in which such occurs, the employer may also use such information in the scope of disciplinary proceedings, where those facts constitute, in and of themselves, a breach of the duties of the employee. The CNPD considers that this guarantees the protection of the legitimate interests of the employer, whilst ensuring that there is no deviation from the purpose, and that the personal data are not used to control the performance of the employee.

In addition to the aspects listed above, the Resolution under consideration analyses other relevant matters, namely the category of personal data that may be processed and the periods of time during which data can be retained, the processing of the information

internally and externally, intercommunication and communication of personal data to third parties, transparency and the rights of the data subjects and the security measures to be implemented, for which reason the reading of this text should not dispense with the perusal of the entire Resolution.

16.2 What "hot topics" are currently a focus for the data protection regulator?

- The new Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
- Geolocalisation in the work place.
- Video surveillance using drones.
- Control of the use of information technologies in the workplace.

Leonor Chastre
Cuatrecasas, Gonçalves Pereira
Praça Marquês de Pombal 2
1250-160
Lisboa
Portugal

Tel: +351 21 350 2997
Fax: +351 21 3549784
Email: leonor.chastre@cuatrecasas.com
URL: www.cuatrecasasgoncalvespereira.com

Leonor Chastre graduated from University of Lisbon Law School and, among others, has a post-graduate degree in IP Law from the University of Lisbon Law School. She also completed a training course about Chinese Culture and Civilization and the History of Macau.

She is also a lecturer for the post-graduate course in Privacy and Data Protection at the Catholic University of Lisbon.

Leonor Chastre is recognised as an IP Law Specialist Lawyer by the Portuguese Bar Association. She is the IP, Media and IT Partner of Cuatrecasas, Gonçalves Pereira.

Leonor Chastre advises on Intellectual Property, Information Technologies and Data Protection, Arbitration and Corporate Law. Some projects coordinated by her and involving her team in the last few years include key industrial investments, namely in Communications and IT areas, some of the largest international groups in Electronic Communications, Audiovisual, IT and Data Protection.