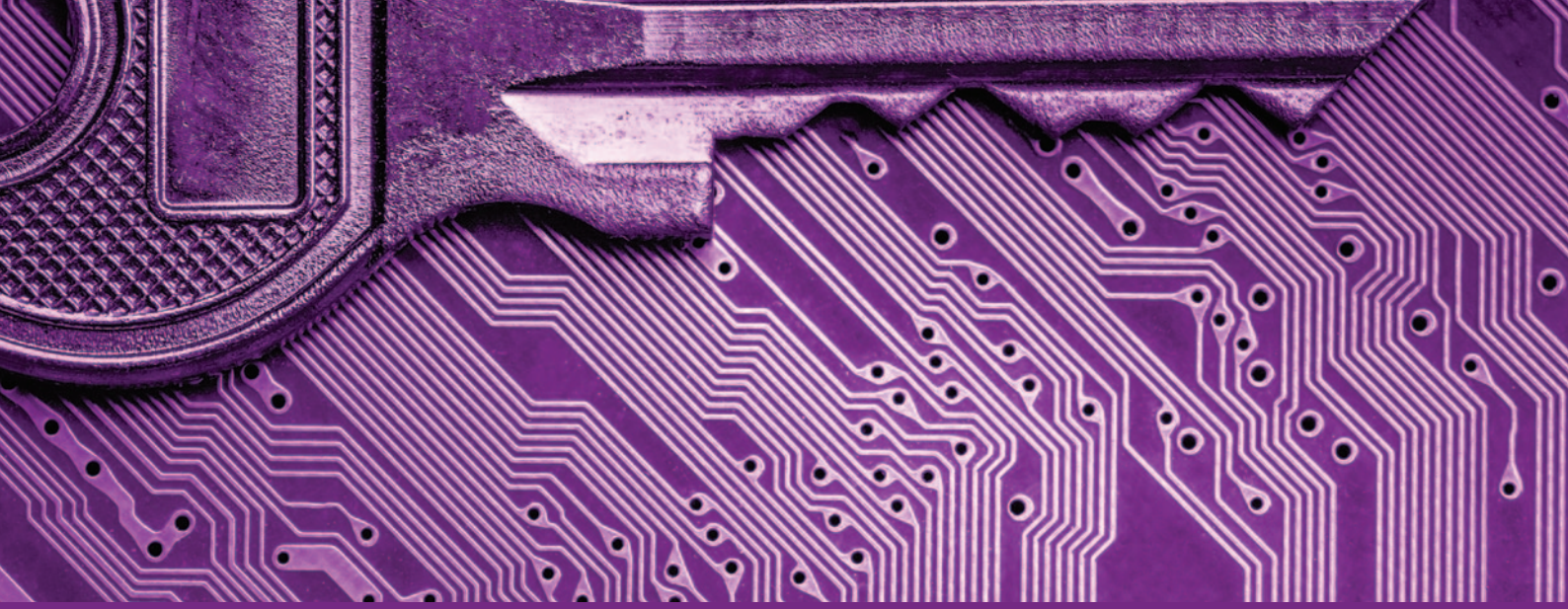

ICLG

The International Comparative Legal Guide to:

Data Protection 2019

6th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Ashurst Hong Kong
Assegaf Hamzah & Partners
BEITEN BURKHARDT
Bird & Bird
Christopher & Lee Ong
Çiğdemtekin Çakırca Arancı Law Firm
Clyde & Co
Cuatrecasas
Deloitte Legal Shpk
DQ Advocates Limited
Drew & Napier LLC
Ecija Abogados
FABIAN PRIVACY LEGAL GmbH
GANADO Advocates
Herbst Kinsky Rechtsanwälte GmbH
Herzog Fox & Neeman
Infusion Lawyers
Integra Law Firm
KADRI LEGAL
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys At Law
Lee & Ko
LPS L@w
Lydian
Matheson
Mori Hamada & Matsumoto
Morri Rossetti e Associati Studio Legale e Tributario
Nyman Gibson Miralis
OLIVARES
Osler, Hoskin & Harcourt LLP
Pestalozzi Attorneys at Law
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Rothwell Figg
S. U. Khan Associates Corporate & Legal Consultants
Subramaniam & Associates (SNA)
thg IP/ICT
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg global legal group

global legal group

Contributing Editor
Tim Hickman &
Dr. Detlev Gabel,
White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Nicholas Catlin

Senior Editors
Caroline Collingwood
Rachel Williams

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

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
June 2019

ISBN 978-1-912509-76-8
ISSN 2054-3786

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Continued Overleaf

global legal group

Country Question and Answer Chapters:

Portugal

Sónia Queiróz Vaz

Cuatrecasas

Ana Costa Teixeira

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the main data protection legislation in the EU has been Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR"). The GDPR repealed Directive 95/46/EC (the "Data Protection Directive") and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

Although Law no. 67/98 of 26 October ("Data Protection Act"), which transposed the Data Protection Directive, is still in force, it will be revoked once the new data protection law is approved by the Portuguese Parliament and enters into force.

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

There are other laws in Portugal, which impact data protection, for example:

- Constitution of the Portuguese Republic – Article 35 (use of computerised data);
- Law no. 46/2012 of 29 August – transposed the part of Directive 2009/136/EC amending Directive 2002/58/EC of the European Parliament and of the Council of 12 July, on the processing of personal data and the protection of privacy in the electronic communications sector, introducing the first amendment to Law no. 41/2004 of 18 August;
- Regulation no. 1093/2016, of 14 December, which regulates the use of drones;
- Decree-Law no. 298/92, of 31 December, General Regime of Credit Institutions and Financial Companies; and
- Law no. 83/2017, of 18 August, containing measures to combat money laundering and the financing of terrorism.

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

The Portuguese health, labour, banking and insurance sectors are subject to additional and specific statutory restrictions in relation to data protection.

1.4 What authority(ies) are responsible for data protection?

The Data Protection Act has created the *Comissão Nacional de Protecção de Dados* – the Portuguese Data Protection Authority ("CNPD") – as the empowered body to supervise and monitor the compliance with laws and regulations within personal data protection.

2 Definitions

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

- "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**" means the natural or legal person, public authority, agency or 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 such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law.
- "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**" means an individual who is the subject of the relevant personal data and who is an identifiable person who can be identified, directly or indirectly, in particular with reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

- "**Sensitive Personal Data**" is personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  No further definitions are applicable.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in the EU and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in the EU, but is subject to the laws of a Member State by virtue of public international law, is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

4 Key Principles

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

- **Transparency**

  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data in a concise, transparent, intelligible and easily accessible form (using clear and plain language).
- **Lawful basis for processing**

  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations; or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

  Please note that businesses require stronger grounds to process special categories of personal data. Processing of these data is only permitted under certain conditions, of which the most relevant are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.
- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) must be able to rely on a lawful basis as set out above.
- **Data minimisation**

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- **Proportionality**

  The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.
- **Retention**

  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Other key principles – please specify

- **Accuracy**

  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **Data security**

  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**

  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

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

- **Right of access to data/copies of data**

  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii)

information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to be determine that period); (vi) information about the existence of the rights to access, to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

Additionally, the data subject may request a copy of the personal data being processed.

Data access must be exercised before the controller or, if applicable, the processor. This right comprises three exceptions:

a. medical data, whose access must be exercised only by a doctor appointed by the data subject;

b. police data, whose access is made through the CNPD; and

c. the data for journalistic use and/or artistic or literary purposes, whose access must be performed also through the CNPD.

- **Right to rectification of errors**

  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**

  Data subjects have the right of erasure of their personal data (the "right to be forgotten") if: (i) the data is no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data has been processed unlawfully; (v) erasure is necessary for compliance with EU law or national data protection law; or (vi) the personal data has been collected in relation to the offer of information society services.

- **Right to object to processing**

  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**

  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**

  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers provided that:

  a. the processing is based on consent or on a contract; and

  b. the processing is carried out by automated means.

- **Right to withdraw consent**

  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**

  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**

  Data subjects have the right to lodge complaints concerning the processing of their personal data with the CNPD, if the data subjects live in Portugal or the alleged infringement occurred in the Portuguese jurisdiction.

Other key rights – please specify

- **Right to basic information**

  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Prior to the GDPR, the controller was obliged to notify or to file an authorisation request before the CNPD before carrying out a personal data processing operation. While that obligation produced administrative and financial burdens, it did not contribute to improving the protection of personal data. With the GDPR, this obligation has been abolished and replaced with effective procedures and mechanisms (data protection impact assessment ("DPIA")), which focus on the processing operations that are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope, context and purposes. Recently, the CNPD published a list of personal data processing activities subject to DPIA in addition to those already exemplified in the GDPR.

Nevertheless, the GDPR sets forth new obligations to notify the competent supervisory authority, for example in the case of a personal data breach.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable; please see question 6.1 above.

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

This is not applicable; please see question 6.1 above.

6.4 Who must register with/notify the data protection authority (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 is not applicable; please see question 6.1 above.

6.5 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)?

This is not applicable; please see question 6.1 above.

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

This is not applicable; please see question 6.1 above.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable; please see question 6.1 above.

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

This is not applicable; please see question 6.1 above.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable; please see question 6.1 above.

6.10 Can the registration/notification be completed online?

This is not applicable; please see question 6.1 above.

6.11 Is there a publicly available list of completed registrations/notifications?

Yes. The notifications and authorisations granted by the CNPD before the entry into force of the GDPR are available on the CNPD website.

6.12 How long does a typical registration/notification process take?

This is not applicable; please see question 6.1 above.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances, including where:

a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

b. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c. the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

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

Infringements of the following provisions shall be subject to administrative fines of up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings, provided that the Data Protection Officer is easily accessible from each establishment.

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

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the

minimum tasks required by the Data Protection Officer, which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on DPIAs and the training of staff; (iv) co-operating with the data protection authority; and (v) acting as the authority's primary contact point for issues related to data processing.

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

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer. In Portugal, an official notification form has been approved by the CNPD and can be filed directly online.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the "WP29") (now the European Data Protection Board (the "EDPB")) recommended in its 2017 guidance on Data Protection Officers that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf, is required to enter into an agreement with the processor which sets out the subject matter for the processing, its duration, its nature and purpose, the types of personal data and categories of data subjects and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing, including in electronic form. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules of regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Under Law no. 41/2004 of 18 August (following the amendment of Law no. 46/2012 of 29 August), sending unrequested communications for direct marketing purposes requires the express prior consent of the subscriber or user ("opt-in"). 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. Nevertheless, if the above-mentioned communications refer to products or services similar to those which the data subject has already purchased from the controller, prior consent is not required, provided that he/she is able to oppose to such communications, both at the time of collection and at the time of sending each message ("opt-out").

Although the "opt-in" rule does not apply to legal entities, Law no. 41/2004 also sets forth the right to "opt-out" for these entities.

With the GDPR, the consent acquires a new relevance, namely in the marketing sector. As such, any organisation that wants to collect data must communicate clearly to the data subject what that data is going to be used for. The data subjects will need to give their consent to that use and the consent needs to be clear, "informed, specific, unambiguous, and revocable". Data subjects also need to be informed about their right to withdraw consent.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

It is incumbent upon the Directorate General of Consumers ("DGC") to keep up to date a national list of legal persons that expressly object to the receipt of unsolicited communications for direct marketing purposes. The entities that promote the sending of communications for direct marketing purposes are obliged to consult the list, updated monthly by the DGC, which is available on request.

Where the prior express consent of the subscriber (data subject) has been collected, such consent overrides the need to consult the above-referenced list.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not, including the following circumstances where the controller or processor are not established in the EU: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

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

Although the CNPD is not very proactive in the execution of its supervision and monitoring powers, following a complaint, they are quick to open investigations and issue decisions.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, user-friendly and must specifically cover the controller's name, the purposes of the processing and the types of processing activity. As such, if the consent collected by the controller does not specifically cover third parties (with whom the controller may share consent) and the specific purposes for which these third parties will process the personal data shared, the sharing and/or acquisition of data for marketing purposes is unlawful.

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

The CNPD and ICP-ANACOM are empowered to issue fines of up to €5 million 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 for each day up to a maximum of €3 million (30 days' delay).

When applicable, according to the GDPR a fine of up to €20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, can be issued.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Law no. 41/2004 of 18 August (following the amendment of Law no. 46/2012 of 29 August), which implements Article 5 of the ePrivacy Directive, determines that the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Law no. 41/2004 of 18 August does not distinguish between different kinds of cookies. In order to determine whether the prior informed consent of users is required or not, the WP29 guidance on "cookie consent exemption" must be taken into consideration.

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

To date, the CNPD has not taken any enforcement action in relation to cookies.

10.4 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 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 for each day up to a maximum of €3 million (30 days' delay).

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the "EEA") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a "layered approach" should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules ("BCRs").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the USA is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.

In Portugal, the CNPD has issued the Decision 765/2009, on the principles applicable to whistle-blower hotlines. According to this Decision the whistle-blowing of irregular acts is also restricted to the prevention and/or repression of irregularities such as corruption, banking and financial crime and matters affecting accounts, internal account controls and auditing.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

In its Decision 765/2009, the CNPD repudiates the anonymity. Instead, the controller should adopt a confidentiality regime in order to prevent the risks of slanderous complaints and discrimination.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

In Portugal, these notifications took place before the entry into force of the GDPR.

However, a DPIA must be undertaken with assistance from the Data Protection Officer when there is systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

Yes: only for the purpose of protection of persons and goods.

14 Employee Monitoring

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

The CNPD has issued Recommendations on the monitoring of use of phone calls, email and internet access by employees at the workplace, as follows:

a. **Phone**

The controller (employer) shall define the level of tolerance regarding the use of telephones and the forms of control adopted. In cases where monitoring of phone calls takes

place, data other than that which is strictly necessary to achieve the purpose of the control shall not be processed.

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

b. **Email and internet**

The controller shall set up clear and precise rules on the use of the email and internet for private purposes.

These rules shall be submitted to the opinion of the data subjects (employees) and their representatives, being expressly publicised. It is advisable that the controller allows the data subjects to use, in moderate and reasonable terms, the new technological means made available to them.

c. **Principles for the use of email**

Even when controllers prohibit the use of emails for private purposes, they are not entitled to open the emails addressed to the data subjects. Non-intrusive control methods must be previously defined and disclosed to the data subjects.

The control shall be punctual and towards the areas or activities that present a greater "risk" for the business.

d. **Principles on internet access**

Permanent and systematic control of internet access shall not be undertaken. 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.

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

There are situations where a data subject will not have a real choice because of an imbalance of power in their relationship with the controller (e.g., between an employer and employee). As such, employers should (by default) avoid reliance on consent as a lawful basis for processing; for instance, (i) execution of the contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or (ii) carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The level of use of phone, email and internet at workplace, 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 an Internal Regulation, which shall be submitted to the work councils and publicised (namely, by posting it in the headquarters and in all other workplaces, in order to allow the employees to obtain full knowledge of it).

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Depending on the security risk this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident and a process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

15.2 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) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach, without undue delay (and in any case within 72 hours of first becoming aware of the breach), to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach, including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach, including attempts to mitigate possible adverse effects.

In Portugal, an official notification form has been approved by the CNPD and can be filed directly online.

15.3 Is there a legal requirement to report data breaches to affected data subjects? 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) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Investigative Powers	The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out a review of certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks, and to access the premises of the data including any data processing equipment.	N/A
Corrective Powers	The data protection authority has a wide range of powers, including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw certification, and to impose an administrative fine (as below).	N/A
Authorisation and Advisory Powers	The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and authorise certificates, contractual clauses, administrative arrangements and BCRs as outlined in the GDPR.	N/A
Imposition of administrative fines for infringements of specified GDPR provisions	The GDPR provides for administrative fines which can be €20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year.	N/A
Non-compliance with a data protection authority	The GDPR provides for administrative fines which will be €20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year, whichever is higher.	N/A

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes. No court order is required.

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

On October 2018, the CNPD fined Barreiro-Montijo Hospital Centre ("Hospital") in the amount of €400,000, based on its policies regarding access to databases, which allowed technicians and physicians to consult patients' clinical files without proper authorisation. This action was based on the fact that professionals working in the area of social services had access to patients' personal data files which should have been exclusively reserved to physicians. The CNPD concluded that the Hospital had no internal rules for the creation of accounts or for granting different levels of access to clinical information.

The following (three) infractions were identified: violation of the principle of data integrity and confidentiality; violation of the principle of data minimisation which should prevent indiscriminate access to clinical data of patients; and the inability of the Hospital, as controller, to ensure the confidentiality and integrity of the data. The first two infringements were punished with a fine of €150,000 each, with a further €100,000 fine handed down for the third.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

We are not aware of any such cases.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Portuguese businesses typically respond that they are subject to EU personal data protection obligations, namely those regarding confidentiality and the impossibility to share data without legitimate grounds. In Portugal, there is a conflict between the data protection law and e-discovery demands, which is strengthened by the differences between the different judicial systems. In these cases, the reply to foreign e-discovery requests is always limited by compliance with Portuguese and EU legislation on data protection.

17.2 What guidance has/have the data protection authority(ies) issued?

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

a. Furnishing adequate notice to affected Portuguese individuals.

b. Ensuring the underlying legitimacy of the collection and processing (and, frequently, international transfer) of personal data.

c. Maintaining appropriate limitations or controls on the scope of the data collection exercises.

d. Abiding by international data transfer rules.

18 Trends and Developments

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

Portuguese courts have been deciding that the images captured by CCTV are admissible as proof in a disciplinary proceeding and in the subsequent legal action, provided that the requirements arising from the legislation on data protection have been met, and that the purpose of their placement was not solely to control workers' professional performance.

According to the Portuguese legislation, the employer may not use remote monitoring equipment in the workplace for controlling the worker's professional performance. However, the use of this equipment is acceptable whenever it has as its purpose the protection and security of people and goods, or when particular requirements inherent to the nature of the activity justify such use.

The most relevant decision in this matter is a ruling from the Court of Appeal of Oporto, of October 2018, that considered as a legitimate proof for disciplinary means the visualisation of CCTV images that were collected at the workplace. Since CCTV has been duly authorised by the CNPD for protecting people and goods, and the worker had knowledge that her workplace was under video surveillance, the Court ruled that it is permissible to view, in a court hearing, images from video surveillance collected at the workplace as proof for disciplinary purposes.

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

The following topics are being looked at closely:

a. The implementation of the new national data protection law that will complement the GDPR in Portugal.

b. The protection of students' personal data online (*viz.* the publication of evaluations).

c. The implementation and enforcement of the GDPR – the CNPD has published several documents to guide controllers and processors in this process.

Sónia Queiróz Vaz

Cuatrecasas
Praça Marquês de Pombal, nº 2
1250-160 Lisboa
Portugal

Tel: +351 21 355 38 00
Email: sonia.queiroz.vaz@cuatrecasas.com
URL: www.cuatrecasas.com

Having joined Cuatrecasas in 2008, Sónia Queiróz Vaz is now a Senior Associate coordinating the firm's Intellectual Property, Media and Data Protection department in Portugal.

Sónia has advised on projects involving the evaluation and verification of compliance with obligations relating to personal data and privacy protection, has helped map how personally identifiable information is processed, and has defined strategies for implementing the requirements of the General Data Protection Regulation.

She is experienced in drafting and negotiating agreements for the exploitation of intellectual property rights (particularly, licensing and transfer rights) in many fields (including broadcasting, publishing and merchandising). She has extensive expertise in the commercial exploitation of software and audiovisual products domestically and internationally.

Sónia has also provided legal advice on projects concerning consumer rights, industrial property rights, advertising rights and social communication rights.

She has been a member of the Portuguese Bar since 2000.

Education:

- 3rd Consumer Law and Alternative Consumer Dispute Resolution Course, Universidade Nova de Lisboa, 2016.
- Information Technology Course, Instituto Nacional da Propriedade Industrial, Lisbon, 2016.
- Course on IP and Competition Law, Católica Global School of Law, 2016.
- Postgraduate Course in Information Society Law, Universidade Nova de Lisboa Law School, 2001.
- Law Degree from the University of Lisbon Law School, 2000.

Ana Costa Teixeira

Cuatrecasas
Praça Marquês de Pombal, nº 2
1250-160 Lisboa
Portugal

Tel: +351 21 355 38 00
Email: ana.costa.teixeira@cuatrecasas.com
URL: www.cuatrecasas.com

Ana Costa Teixeira has been an Associate Lawyer at Cuatrecasas since 2008.

Ana focuses her practice on the areas of intellectual property, advertising and media law, new technologies law (computer law) and data protection law, providing advice, in particular, on conflicts relating to intellectual and industrial property rights, unfair competition and advertising, and distribution and licence agreements.

Previously, she worked at Almeida Sampaio & Associados.

She has been a member of the Portuguese Bar Association since 2002.

Ana has also been a teacher at IADE, on the subject of Legal Protection of Trademarks and Branding and Trademark Management (Postgraduate Course), since 2011.

Education:

- Law Degree, University of Lisbon Law School, 2002.
- Postgraduate Course in Administrative Litigation, School of Law of the Catholic University, 2006.
- Summer Course on Industrial Property, University of Lisbon Law School, 2008.

CUATRECASAS

Cuatrecasas is a leading Iberian law firm with its main offices in Portugal and Spain and an international presence in 10 other countries. We have nearly 1,000 lawyers in 27 offices worldwide, organised by legal practice areas and multidisciplinary teams with expertise in specific commercial and industrial sectors. In Portugal, we have offices in Lisbon and Porto and a total of over 140 lawyers.

Different regions become connected through the firm's client-tailored model that offers the best team for each particular case, depending on the jurisdiction, speciality area and complexity required.

Sixteen offices on the Iberian Peninsula coordinate with the firm's teams in Beijing, Bogotá, Brussels, Casablanca, London, Luanda, Maputo, Mexico City, New York, São Paulo and Shanghai, thus optimising efficiency of resources and client proximity, and benefiting from the different time zones. The international desks (covering Africa, Latin America, China, France, Germanic countries and the Middle East) and over 20 country-specific groups guarantee a comprehensive approach to the legal advice from Spain and Portugal.

In continental Europe, Cuatrecasas has developed a non-exclusive network with three other leading law firms – Chiomenti in Italy, Gide in France and Gleiss Lutz in Germany – allowing it to offer clients an integrated service in complex cross-border transactions.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com