Data Protection & Privacy

Contributing editor
Wim Nauwelaerts

2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2018

Contributing editor
Wim Nauwelaerts
Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Sixth edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Introduction 5
Wim Nauwelaerts
Hunton & Williams

EU overview 9
Wim Nauwelaerts and Claire François
Hunton & Williams

Safe Harbor and the Privacy Shield 12
Aaron P Simpson
Hunton & Williams

Australia 14
Alex Hutchens, Jeremy Perier and Eliza Humble
McCullough Robertson

Austria 20
Rainer Knyrim
Knyrim Trieb Attorneys at Law

Belgium 28
Wim Nauwelaerts and David Dumont
Hunton & Williams

Brazil 36
Ricardo Barretto Ferreira and Paulo Brancher
Azevedo Sette Advogados

Chile 42
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
García Magliona & Cía Abogados

China 47
Vincent Zhang and John Bolin
Jincheng Tongda & Neal

France 55
Benjamin May and Clémentine Richard
Aramis

Germany 63
Peter Huppertz
Hoffmann Liebs Fritsch & Partner

India 69
Stephen Mathias and Naqeeb Ahmed Kazia
Kochhar & Co

Ireland 75
Anne-Marie Bohan
Matheson

Italy 84
Rocco Panetta and Federico Sartore
Panetta & Associati

Japan 93
Akemi Suzuki and Tomohiro Sekiguchi
Nagashima Ohno & Tsunematsu

Lithuania 99
Laimonas Marcinkevičius
Juridicon Law Firm

Luxembourg 106
Marielle Stevenot and Audrey Rustichelli
MNKS

Mexico 113
Gustavo A Alcocer and Abraham Díaz Arceo
Olivares

Poland 119
Arwid Mednis and Gerard Karp
Wierzbowski Eversheds Sutherland

Portugal 126
Helena Tapp Barroso, João Alfredo Afonso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Russia 133
Ksenia Andreeva, Anastasia Dergacheva, Vasilisa Strizh and Brian Zimbler
Morgan, Lewis & Bockius LLP

Serbia 140
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore 145
Lim Chong Kin and Charmian Aw
Drew & Napier LLC

South Africa 159
Danie Strachan and André Visser
Adams & Adams

Spain 168
Alejandro Padín, Daniel Caccamo, Katiana Otero, Francisco Marín and Álvaro Blanco
J&A Garrigues

Sweden 174
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland 181
Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

Turkey 189
Ozan Karaduman and Bentley James Yaffe
Gün + Partners

United Kingdom 195
Aaron P Simpson
Hunton & Williams

United States 202
Lisa J Sotto and Aaron P Simpson
Hunton & Williams

Portugal

Helena Tapp Barroso, João Alfredo Afonso and Tiago Félix da Costa

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Portugal has a dedicated data protection law governing personal data processing issued in 1998 (Law No. 67/98 of 26 October 1998 (the DPA)). A previous data protection law had been issued in 1991 (Law No. 10/91) dedicated to the protection of personal data processed by automated means. This initial law was based on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), adopted by the Council of Europe. The DPA currently in force implements the provisions of 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 PII and on the free movement of such information. Currently (July 2017) there is no specific legislation based on the EU General Data Protection Regulation (GDPR).

Portugal has relevant national constitutional privacy provisions, as article 35 of the Portuguese Constitution (on the use of computerised data) sets forth the main relevant principles and guarantees that rule PII protection.

International instruments relevant for PII protection have also been adopted in Portugal, as is the case of the following:

- the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108);
- the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) of which article 8 is specifically relevant for PII protection; and
- the Charter of Fundamental Rights of the European Union (ie, articles 7 and 8).

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The National Commission for the Protection of Data (CNPD) is the authority responsible for overseeing the DPA in Portugal.

The CNPD (its members or delegated staff) have powers to require information on PII processing activities from public or private bodies and hold rights of access to the computer systems supporting PII processing, as well as to all documentation relating to the processing and transmission of PII, within the scope of its duties and responsibilities.

These include, among others, the responsibility to:

- supervise and monitor compliance with the laws and regulations regarding privacy and PII;
- exercise investigative powers related to any PII processing activity, including PII transmission;
- exercise powers of authority, particularly those of ordering the blocking, erasure or destruction of PII or imposing a temporary or permanent mandatory order to ban unlawful PII processing;
- issue public warnings or admonition towards PII owners failing to comply with PII protection legal provisions;
- impose fines for breaches of the DPA or other specific data protection legal provisions; and
- report criminal offences to the Public Prosecution Office in the context of the DPA and pursue measures to provide evidence thereon.

3 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of data protection law can lead to both administrative sanctions or orders and criminal penalties.

The administrative fines applicable to data protection law breaches under the DPA currently range between €498.79 and €4,987.97. The amounts are doubled in certain aggravated breach cases, depending on the occurrence of legally specified breach circumstances (eg, if the breach involves special categories of PII).

Sector-specific legislation for the protection of PII in the electronic communication business activity (applicable, for example, to PII owners that are telecom operators and internet service providers) foresees much higher administrative fines for data protection law breaches (which may go up to a maximum of €5 million).

Criminal offences are punished with imprisonment of up to two years or a 240 day-fine (the relevant day-fine amount being fixed by the judge within a range between €5 and €500, depending on the financial situation and personal and family expense level of the offender), both of which can be aggravated to double the amount.

Administrative sanctions and orders are applied by the CNPD, which also has powers to order ancillary administrative measures such as temporary or permanent data processing bans or PII blockage, erasure or total or partial PII destruction, among others.

Criminal offences are subject to prosecution by the Public Prosecutor and their application must be decided by the criminal courts.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Portuguese DPA applies to both public and private entities.

An application exemption is foreseen for PII processing carried out by natural persons in the course of purely personal or domestic activities.

The provisions of the DPA also apply to the processing of personal data regarding public security, national defence and state security, without prejudice, however, to special rules contained in international law instruments to which Portugal is bound, as well as specific domestic laws on the relevant areas.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The DPA generally covers these subjects, to the extent they involve processing of PII. A number of such issues are also covered by specific laws and regulations.

Video surveillance and surveillance cameras for defined purposes are the object of specific laws, as is the case, among others, of:

- Law No. 1/2005 of 10 January 2005 (subsequently amended and republished by Law No. 9/2012 of 23 February 2012) on the installation in public areas and use of surveillance through video cameras, by national security forces (for protection of public buildings, including premises with interest for defence and security, people and asset security, crime prevention, driving infraction prosecution, prevention of terrorism and forest fire detection) and Decree-Law No. 207/2005 of 29 November 2005 specifically on electronic surveillance on the roads (eg, cameras and radars) by traffic police and other security forces; and
- Law No. 34/2013 of 16 May 2013 on the licensing of private security agencies and their activity, which contains relevant provisions on the use of video surveillance cameras (and Regulation No. 273/2013 of 20 August 2013).

The Portuguese Labour Code (2009) also contains a number of provisions on employee privacy, including provisions on monitoring and surveillance; namely, excluding the possibility of surveillance equipment being used by the employer to control employee performance (articles 20 to 22) and consultation requirements with employee work councils for certain types of processing.

The retention of PII by electronic service providers is regulated by Law No. 32/2008 of 17 June 2008 (see question 6 for additional information).

Law No. 41/2004 of 18 August 2004 as amended by Law 46/2012 of 29 August 2012 (see question 6 for additional information), which governs the processing of personal data and privacy in the electronic communications sector, contains specific provisions on unsolicited communications for marketing purposes.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

In Portugal some sector-specific or purpose-specific provisions for the protection of PII may be found in specific laws or regulations. A relevant example of these are the rules specifically applicable to the electronic communications (telecom) sector contained in Law 41/2004 of 18 August 2004, which implemented Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, or E-privacy Directive) as amended by Law 46/2012 of 29 August 2012, implementing Directive 2009/136/EC (which also amended the E-privacy Directive) and Commission Regulation (EU) No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under the above referred Directive 2002/58/EC.

The provisions of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC have also been implemented in Portugal through Law No. 32/2008 of 17 June 2008 on the retention and transfer of such PII for the purposes of the investigation, detection and prosecution of serious crime by competent authorities.

Other specific scope or sector acts may also be referred to, as is the case of Law No. 12/2005 of 26 January 2005 (as amended) and Decree-law No. 131/2014 of 29 August 2014, both on personal genetic and health information.

7 PII formats

What forms of PII are covered by the law?

In Portugal the DPA covers PII processed by totally or partially automatic means as well as PII contained in manual filing systems or intended to integrate such systems.

8 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The Portuguese DPA covers PII processing carried out in the context of the activities of an establishment of the PII owner located in Portuguese territory or in a place where Portuguese law applies by virtue of international public law.

The DPA also applies to processing carried out by a PII owner established outside the European Union area but who makes use of automated or non-automated means for processing located in Portuguese territory, with the exception of means or equipment located in Portugal to serve the purposes of mere transit of PII through the country.

The DPA covers video surveillance and other forms of PII collection, processing and broadcast consisting of sound or image, whenever the owner is located in Portugal or uses a network access provider established in Portuguese territory.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners?

Although the DPA includes a number of provisions that refer to processors or processing services, the main direct legal obligations contained in the DPA are applicable to PII owners.

Although administrative penalties and criminal infractions refer primarily to PII owners (while applicable to the breach of specific PII owner legal duties) penalties are not exclusively applicable to the same entities (eg, unauthorised access to PII, tampering or destruction of PII and others is not restricted to a PII owner action).

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Portuguese DPA requires that the holding of PII is legitimised on specific grounds.

In the case of non-sensitive data, the following grounds legitimise processing:

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

11 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

More stringent rules apply in the case of 'sensitive data'.

Sensitive data refers to PII that reveals:

- philosophical or political beliefs;

- political party or trade union membership;
- religious beliefs;
- private life (privacy);
- racial or ethnic origin;
- health or sex life (including genetic PII); and
- suspicion of illegal activities, criminal or administrative offences and decisions applying criminal penalties, security measures, administrative fines or additional conviction measures.

As a rule, the processing of sensitive PII is prohibited. However, under express legal disposition or upon prior authorisation granted by the CNPD, processing of sensitive PII is permitted (and may, therefore, be lawfully grounded) provided one of the following legitimation grounds for the processing occurs:

- explicit consent is obtained from the individual;
- processing is essential for the accomplishment of a task carried out in the public interest and in the exercise of a legal or statutory role vested in the PII owner;
- processing is required for the protection of vital interests belonging to the individual, in cases where same individual is physically or legally incapable of providing consent;
- PII covered by processing has been clearly made public by the individual, provided same individual's statements allow consent to be clearly inferred; and
- processing is required for legal proceedings or in order to exercise legal rights in court proceedings.

In the case of PII relating to health or sex life, including genetic data, processing is also legitimate when grounded on medical purposes (preventative medicine, medical diagnosis, provision of medical care and management of healthcare services).

The processing of information consisting of the suspicion of illegal activities or criminal or administrative offences is allowed on the grounds of pursuing the legitimate purposes of the PII owner, provided the latter are not overridden by the individual's fundamental rights and freedoms.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The law requires owners of PII to notify individuals whose data they hold of the following information, at the time of collection of the PII, (except where the individuals already hold such information):

- the PII owner's identity and, where applicable, that of the owner's representative;
- the purposes of the PII processing; and
- other relevant information, including, at least, the following:
  - the PII recipients or category of recipients;
  - the statutory or voluntary nature of responses on PII required from the individual (and the consequences of not providing a response);
  - information that PII may circulate on the network without security measures and may be at risk of being seen or used by unauthorised third parties, when the PII is collected on an open network; and
  - the existence and conditions for the exercise of the individual's rights of access to PII and correction thereof.

Where the PII is not obtained by the PII owner directly from the individual, notification should take place at the time the first processing operation takes place or, if disclosure to third parties is envisaged, at the time disclosure first takes place.

13 Exemption from notification

When is notice not required?

Notice requirement may be waived by the CNPD or a specific legal provision based on state security grounds or criminal activity prevention or investigation purposes. Waiving may also occur in the case of PII processing performed for statistical or research purposes when notification proves to be practically impossible or to involve a disproportionate effort. The same applies if the law explicitly provides for the PII registry or disclosure to be made.

Notice is not required if processing is carried out solely for journalistic purposes or for literary or artistic expression purposes.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

PII owners must offer individuals whose PII they hold the rights of access, amendment (and updating) and objection.

The right of access comprises the individual's entitlement to obtain, without restrictions, excessive delay or expense:

- confirmation of whether PII is being processed (including the purpose of processing, the categories of PII addressed by the processing activities and the recipients or categories of recipients of PII);
- communication in an intelligible form of the PII undergoing processing and of on any available information as to the source of such PII;
- knowledge on the logic involved in any automated processing of the relevant PII;
- rectification, erasure or blocking of PII if processing does not comply with the provisions of the DPA (in particular due to the incomplete or inaccurate nature of PII being processed); and
- notice to third parties to whom the PII has been disclosed of any such rectification, erasure or blocking, except where notice proves not to be possible.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

PII processed must be relevant, accurate and, where necessary, kept up to date in relation to the purpose for which it is held.

The PII owner is required to take adequate measures to ensure that PII that is inaccurate or incomplete, in light of the processing purpose, is erased or corrected.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The amount of PII that may be held is limited to that which is strictly adequate, relevant and not excessive in relation to the purpose for which it is collected and further processed.

The DPA does not specify allowed retention periods, the general rule being that the PII may not be held for longer than is necessary for the specific purposes for which it was collected and further processed.

There are certain guidelines and decisions issued by the CNPD that indicate, for specific purposes, the length of time the authority considers certain categories of PII may be held. Additionally, all authorisation and registration procedures filed with the CNPD will specify the length of time the PII owner is allowed to hold the relevant PII.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

As a rule, the finality principle has been adopted. PII may only be collected for specific, express and legitimate purposes and may not be subsequently used for purposes that are incompatible with same.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The CNPD may authorise, on an exceptional basis, the use of PII for purposes that differ from those that determined its collection subject, in any case, to the legally applicable PII quality and processing lawfulness principles.

Security

19 Security obligations

What security obligations are imposed on PII owners and service providers that process PII on their behalf?

The DPA requires PII owners to put in place appropriate technical and organisational measures that, taking into account the state of the art and the cost required for their implementation, are appropriate to protect PII against:

- accidental or unlawful destruction;
- accidental loss or alteration;
- unauthorised disclosure or access (particularly where processing of the PII involves its transmission over a network); and
- any other unlawful forms of processing.

The level of security required must be appropriate in view of the risks represented by the relevant processing activity and the nature of the processed PII.

When the PII owner chooses to resort to processors, he or she is subject to electing processors that offer sufficient guarantees in respect to the implementation of such technical and organisational measures. It stands upon the PII owner to ensure that the processor complies with the appropriate measures.

When sensitive PII is processed the owner must implement measures that are appropriate to:

- control entry to the premises where such sensitive PII is processed;
- prevent same PII from being read, copied, altered, removed, used or transferred by unauthorised persons;
- guarantee that no unauthorised PII input or PII input knowledge, alteration or elimination occurs;
- keep the access of authorised persons to sensitive PII to the limits of authorised processing;
- guarantee recipient entity verification when same PII processing includes transmission; and
- guarantee that logs or other types of registration are kept to allow sensitive PII input control.

The DPA requires that systems guarantee logical separation between PII relating to health and sex life, including genetic information and other PII.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The law does not include any general obligation to notify the supervisory authority or individuals of data breaches.

There is a sector-specific requirement to do so in the electronic communications sector. In this case, data breaches must be notified by the PII owner to the CNPD, without undue delay.

Also in the electronic communications sector, if the data breach is likely to adversely affect individuals (ie, the telecom service subscribers or users), the PII owners must additionally notify the individuals, also without undue delay. The data breach is deemed to affect PII individuals negatively in cases where the data breach may cause identity fraud or theft, physical or reputational damage connected or relevant humiliation.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

In Portugal and under the DPA the appointment of a data protection officer is not mandatory.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

There are no specific general requirements for PII owners to maintain internal records or establish internal processes or documentation, as such.

There are, nevertheless, requirements that may result in a certain level of record maintenance. In the case of sensitive PII processing, for example, the PII owner is required to put in place appropriate measures to ensure that it is possible to check a posteriori (typically through a log system) for a given period (which may be set in specific regulations or guidelines) on any PII inputs, on the user that performed the input and the time and date when it took place.

Registration and notification

23 Registration

Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?

The PII owner is required to notify the CNPD or obtain prior processing authorisation from same entity before any PII processing activities are initiated. This is not a PII owner registration but a PII processing registration or authorisation system, which is required on the basis of each specifically intended processing purpose.

The processing of sensitive PII or of PII relating to credit or solvency information on individuals, the interconnection of PII not provided for in a legal instrument and the use of PII for purposes other than those that determined its collection requires prior authorisation from the authority and may be performed only after such authorisation has been granted. Other PII processing is subject to registration only; therefore, processing may start as soon as the notification is served by the PII owner.

The CNPD has issued limited scope decisions that exempt PII owners from obtaining prior authorisation or from serving registration notification. These include, among others, the processing of specific categories of employee PII for payroll purposes or the processing of client PII for invoicing purposes.

24 Formalities

What are the formalities for registration?

Both the notification (processing registration) and the prior authorisation request must be completed online (an e-notification system is in place). A fee is payable in all cases (the registration fee being currently in the amount of €75 and the authorisation filing fee €150).

Both procedures involve filling in general or specific processing purpose forms that require specific information on the intended PII processing operations, entities and conditions involved to be provided to the CNPD.

Processors must be identified by the PII owner as well as any third-party recipients of the PII. Additionally, the following information must be provided by the PII owner when filing the request with the authority:

- name and address of the PII owner and of his representative, if any;
- specific purposes for the PII processing;
- list of the categories of PII to be processed;
- period of time the owner foresees PII needs to be held;
- PII interconnections, if any, and specific grounds or need that justify such interconnection;
- form and circumstances foreseen for the individuals to exercise the rights of access and correction in which the data subjects may be informed of or may correct the personal data relating to them;
- information on any proposed PII transfers to third countries and grounds on which transfer will occur; and
- general description of technical and operational security measures to enable a preliminary assessment to be made of the respective adequacy to ensure security of processing.

Additional information is provided in certain specific processing purpose cases (eg, in the case of PII processing resulting from video camera surveillance information, additional information must be provided on the surveillance system features, number of cameras, etc).

There is no requirement for registration or authorisation periodical renewal, but any changes to the processing, the PII owner, the processor or to other relevant information provided in the notification form should be the object of an amendment form submitted by the PII owner to the authority.

25 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

The DPA provides that the conduct of a PII owner of intentionally omitting PII processing notification with the CNPD may give rise to a criminal offence punished with imprisonment up to one year or a 120 day-fine and up to two years or a 240 day-fine in the case of sensitive PII.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Refusal must be grounded on the authority concluding that the terms of the intended PII processing are not in line with the legal requirements resulting from the DPA. The CNPD may issue a decision with a limited scope authorisation (eg, excluding certain categories of PII from the authorisation or limiting the period during which the PII may be kept by the owner or imposing other limitations to the intended processing).

If the applicable fee is not paid, submitting the form will be ineffective.

27 Public access

Is the register publicly available? How can it be accessed?

The CNPD register (mainly authorisation decisions) is open to public consultation, free of charge, on the authority's website (www.cnpd.pt/bin/registo/registo.htm), although the information available is not complete.

28 Effect of registration

Does an entry on the register have any specific legal effect?

Each entry on the register must specify the purpose of processing. Registration is required for each processing activity, per processing purpose.

An entry on the register does not cause the PII owner to be subject to specific or additional obligations (eg, no notification to individuals or any other entities results from such entry). Because registration is required as a formality that must be completed prior to the relevant PII processing taking place, once the notification is served, processing may begin.

In the case of processing acts or activities that require authorisation (refer to question 23), processing may take place only after the CNPD issues the authorisation decision.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the Portuguese DPA, entities providing outsourced processing services qualify as 'processors'. The processor must only act on instructions from the PII owner, unless he or she is required to act by law.

The PII owner must ensure that the processors it selects provide sufficient guarantees that the required technical and organisational security measures are carried out. Compliance by the processors with the relevant measures must be ensured by the PII owner.

The PII owner and the processor must enter into a contract or be mutually bound by an equivalent legal act, in writing. The relevant instrument is required to bind the processor to act only on instructions from the owner and must foresee that the relevant security measures are also incumbent on the processor.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Disclosure of PII is generally subject to all the processing principles, restrictions and notification requirements contained in the DPA. The individuals must be notified at the time of collection or before disclosure takes place for the first time to the categories of entities to which disclosure of PII will be made. Disclosure, as is the case with all other processing acts, must be based on one of the legitimate processing grounds. This may be, in certain cases, the individual's consent.

Health and sex life PII can be disclosed only to health professionals or other professionals also subject to the same secrecy duties.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The transfer of PII to another European Union member state and European Economic Area (EEA) member countries is not restricted.

Transfer of PII outside these territories is restricted. In this case, transfer is permitted only when it is compliant with the DPA requirements and when the state to which PII is transferred ensures an adequate level of protection assessed in the light of all the circumstances surrounding PII transfer, with special consideration being given to the nature of PII to be transferred, the purpose and duration of the proposed processing, the country of final destination, the rules of law in force in the state in question (both general and sector rules) and the professional rules and security measures that are complied with in such country.

The PII may flow from Portugal to non-EU or non-EEA member states that have been comprised by an adequacy decision issued by the European Commission, acknowledging such country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. Transfer may also be made under contracts that follow the standard form model clauses approved by the European Commission.

The Portuguese authority does not accept 'Binding Corporate Rules' for the transfer of PII. In 2015 the CNPD issued a guideline decision stating that entities within a single corporate group may enter into intragroup agreements compatible with the approved standard form model clauses.

In addition, transfer to the US may be done under the EU–US Privacy Shield framework following the adoption, on 12 July 2016, of the European Commission decision on the EU–US Privacy Shield.

Transfer may also take place, subject to the authority's prior authorisation, if a derogation case applies. Derogations include, among others specified by law:

- the individual having given his or her unambiguous consent to the proposed transfer; or
- the transfer being necessary for:
  - a contract between the individual and the PII owner or the implementation of precontractual measures taken at the individual's request;
  - a contract between the PII owner and a third party, in the interest of the individual;
  - legal proceedings; or
  - the protection of vital interests of the individual.

32 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

All PII processing requires prior notification with the Portuguese authority or prior authorisation (see questions 23 and 24). In the case of cross-border transfers to non-EU or non EEA member states, the PII owner must indicate to the authority that the PII will be the object of a cross-border transfer and the framework that allows such transfer (eg, standard model clauses approved by the European Commission, EU–US Privacy Shield, Intragroup Agreement).

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions that apply to transfers outside the EU and EEA between PII owners apply equally in the case of transfers of PII to service providers (processors).

Onward PII transfers depend on the rules that apply in the PII importer jurisdiction, without prejudice of the case of transfers made under agreements compliant with the approved standard contractual clauses model and intragroup agreements that cover onward data transfers.

Rights of individuals

34 Access

Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals are granted the right to access their personal information held by PII owners. The DPA does not contain specific provision on formalities for the exercise of this right of access, but it does establish that the access entitlement is not to be subject to restrictions, excessive delay or expense. (See question 14 for an indication of the entitlements comprised in the individuals' right of access.)

When notifying the individuals whose PII they hold, the owners of PII must include information on the existence and conditions for the exercise of the individual's rights of access to PII and correction thereof (see question 12).

35 Other rights

Do individuals have other substantive rights?

Individuals are entitled to require the correction of inaccurate information from the PII owner as well as the update of information held.

Individuals also have the right to object at any time to the processing of information relating to them:

- on justified grounds; or
- in any case, and free of charge, if information is meant for the purposes of direct marketing or any other form of research.

Additionally, individuals are entitled to the right not to be subject to a decision that produces legal effects concerning them or significantly affecting them which is based solely on automated processing of information intended to evaluate certain personal aspects relating to same individual.

Correction, removal and information blocking rights are also granted to the individuals when the information held by the PII does not comply with the provisions set out in the DPA, including cases where the information is incomplete or inaccurate.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

In the event an individual suffers damage as a result of an act or omission purported by the PII owner in breach of the DPA, same individual is entitled to compensation for damage claimable through the courts. Compensation for serious injury to feelings may be also claimed.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights to claim monetary damage and compensation are exercisable through the judicial system and not directly enforced by the supervisory authority.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Under the DPA, the Portuguese authority may authorise notification exemptions for specific categories of processing, which, taking into account the categories of PII to be processed, are unlikely to adversely affect the rights and freedoms of the individuals, for speed, economy and efficiency reasons.

The authority has issued six exemption decisions covering PII processing for the following purposes:

- payroll management;
- library users' management;
- invoicing and client, services and goods provider contact management;
- employee and independent contractor administrative management;
- registration of entries and exits in buildings; and
- management of club or association dues.

Each exemption decision specifies not only the purposes of the processing, but also the PII information or category of PII information comprised by the notification exemption, the relevant individuals to whom the PII relates, the recipients or categories of recipients to whom the PII may be disclosed and the length of time the PII may be stored by the owner.

The notification exemption only applies within the strict limits of each authorisation (ie, the purposes, categories of PII information, categories of individuals and recipients and within the time frame limits foreseen).

Supervision

39 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

PII owners can appeal against orders issued by the CNPD to the courts. In the case of decisions issued by the authority applying penalties for administrative misdemeanour, the PII owners may appeal to the criminal courts. To appeal from decisions on authorisation or registration proceedings the competence lies on the administrative courts.

Specific data processing

40 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Portugal has adopted legislation implementing article 5.3 of Directive 2002/58/EC, as amended by Directive 2009/136/EC (E-Privacy Directive). The implementation came into effect on 30 August 2012.

The use of cookies requires the individuals' consent, upon having been provided with clear and comprehensive information on the use of cookies as well as on the categories of PII processed and purposes thereof.

There has been no explicit provision on the nature of the consent, neither has the authority issued formal guidelines on its understanding, but the system implemented in Portugal tends to be seen as an opt-in solution.

41 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing is only allowed in respect of individuals who have given their prior explicit consent. This rule does not apply to users that are not individuals (legal persons). In this case, unsolicited communications for direct marketing purposes may be sent except where the recipient, being a legal person, expresses its opposition.

Unsolicited communications for direct marketing purposes by means of electronic mail also apply to SMS, EMS, MMS and other kinds of similar applications.

These rules do not exclude the possibility of a PII owner, having obtained the electronic contact of its customers, in the context of the sale of its products or services, using such contact details for direct marketing of its own products or similar ones. In this case, the PII owner must only provide its customers with the possibility of objecting, free of charge and in an easy manner, to such use. This possibility must be given both at the time of collection of the PII and on the occasion of each marketing message sent to the customer.

All direct marketing messages must identify the PII owner and indicate a valid contact point for the recipient to object to future messages being sent.

All entities sending unsolicited communications for direct marketing purposes must keep an updated list of individuals that have given their consent to receive such communications, as well as a list of customers that have not objected to receiving it.

42 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific rules of guidance issued by the Portuguese authority on the use of cloud computing. The general DPA rules on PII transfers and on the use of processors by the PII owners will fully apply in the case of cloud computing services contracted by the owner.

Helena Tapp Barroso **htb@mlgts.pt**
João Alfredo Afonso **joaoafonso@mlgts.pt**
Tiago Félix da Costa **tfcosta@mlgts.pt**

Rua Castilho, 165
1070-050 Lisbon
Portugal

Tel: + 351 21 381 74 00
Fax: +351 21 381 74 94
www.mlgts.pt

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law