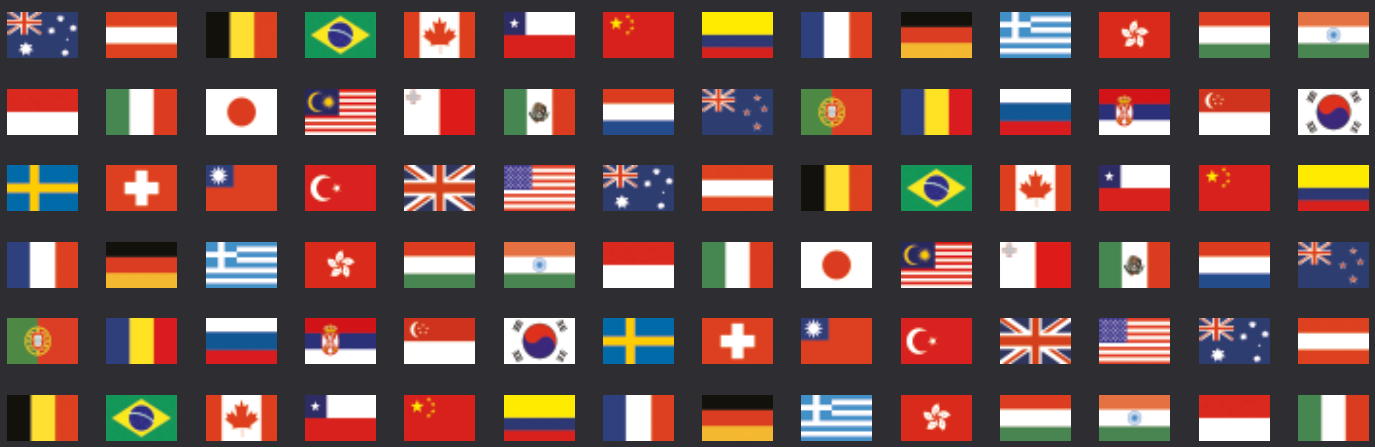
Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto



LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Ninth edition
ISBN 978-1-83862-322-7

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

Data Protection & Privacy

2021

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY®
Getting The Deal Through

London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Portugal

Helena Tapp Barroso and Tiago Félix da Costa

Morais Leitão, Galvão Teles, Soares da Silva & Associados

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 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?

The legislative framework for the protection of PII applicable in Portugal is currently (as from 25 May 2018) that resulting from the direct application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)).

National legislation providing for specific rules in the context of the GPDR – Law 58/2019 of 8 August, entered into force on 9 August (the DPA). This act repealed the previous dedicated Portuguese data protection law governing personal data processing that had been issued in 1998 (Law No. 67/98 of 26 October 1998). 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. The 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 and 1998 law transposed the provisions of Directive 95/46/EC.

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 108;
- the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights (ECHR)), 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).

Data protection authority

2 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 supervisory authority responsible for overseeing the application of the data protection rules and principles 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 transfer;
- exercise investigative powers related to any PII processing activity, including PII transmission;
- exercise powers of authority, particularly those 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.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Cooperation between the supervisory authorities applicable to the Portuguese supervisory authority is currently subject to the provisions of chapter VII of the GDPR on cooperation and consistency, pursuant to article 51(2), which states:

> *Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.*

Breaches of data protection

4 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 covering data protection law breaches under the GDPR apply. The DPA provides for specific rules in the context of the GPDR, including a complete chapter on administrative sanctions that contains provisions setting ranges of fines (minimum and maximum) and classifying infringements according to their nature and gravity, in line with article 83 of the GDPR. Different ranges are set for infractions incurred by individuals, small and medium enterprises (SMEs) and large undertakings (as defined in Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises).

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) foresee administrative fines for data protection law breaches which may go up to a maximum of €5 million.

Criminal offences are punished with fines or imprisonment ranging from six months to four years.

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

Exempt sectors and institutions

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

All sectors and types of organisations are covered by the General Data Protection Regulation (GDPR) and the Law 58/2019 of 8 August (the DPA) in their scope, therefore covering personally identifiable information (PII) processing by both public and private entities.

There is an application exemption for PII processing carried out by natural persons in the course of purely personal or domestic activities, under the GDPR.

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

The provisions of the DPA do not apply to the personal data files kept under the responsibility of the Portuguese Intelligence System (SIRP) – a public entity that reports directly to the prime minister and their cabinet, and is responsible for providing support to policy-makers on the evaluation of threats to the national interest, internal and external security, and the maintenance of the independence, unity and integrity of the Portuguese State – which is subject to specific legislation.

Communications, marketing and surveillance laws

6 | 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.

A number of issues are 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. 51/2006 of 29 August 2006 on the setting up and operation of electronic surveillance systems on the roads for accident and incident prevention and management by highway concessionaires;
- 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 the 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 (subsequently amended and republished by Law No. 46/2019 of 8 July 2019 and Ordinance No. 273/2013 of 20 August 2013, subsequently amended, namely by Ordinance No. 106/2015 of 13 April).

Other laws

7 | 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 the ePrivacy Directive) as amended by Law 46/2012 of 29 August 2012, implementing Directive 2009/136/EC (which also amended the ePrivacy 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 reform of ePrivacy legislation currently taking place in the European Union in line with the new rules in force under the GPDR will, no doubt, bring changes in this area to local legislation.

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.

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. In the context of the coronavirus pandemic, specific provisions were also issued on the possibility of employee temperature measuring by employers.

The retention of PII by electronic service providers is regulated by Law No. 32/2008 of 17 June 2008.

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

PII formats

8 | What forms of PII are covered by the law?

The legislation applicable in Portugal covers PII processed by totally or partially automatic means as well as PII that forms part of a (manual) filing system or is intended to form part of such systems (GDPR). PII refers to any information relating to an identified or identifiable natural person. The GDPR does not apply, as a rule, to the personal data of deceased persons but it foresees that member states may provide for

rules regarding the processing of personal data of deceased persons. The DPA includes a provision foreseeing that PII relating to deceased individuals is protected in accordance with the provisions of the GDPR and those of same DPA when consisting on special categories of data foreseen in article 9 of the GDPR (genetic PII, biometric PII, PII concerning health, data concerning the individual's sex life or sexual orientation, PII revealing political opinions, trade union membership, religious or philosophical beliefs and racial or ethnic origin) or when it refers to private life PII or communication (traffic) data.

Extraterritoriality

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

The 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.

Also covered is processing carried out by a PII owner established outside Portuguese territory affecting individuals (whose PII they process) who are in Portugal, where the processing activities are related to the offering of goods or services to such Individuals in Portugal, irrespective of whether payment is required, or the monitoring of their behaviour as far such behaviour takes place within the Portuguese territory. The DPA provisions also apply to the processing of PII registered in Portuguese consulates regarding Portuguese individuals residing outside Portugal.

The GDPR territorial scope, as defined in article 3, nevertheless fully applies.

Covered uses of PII

10 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? Do owners', controllers' and processors' duties differ?

All processing of PII is covered regardless of whether it is processed by those who control or own PII of by those who provide PII processing services to owners. A significant number of duties apply both to controllers and processors, although some of the duties differ, in the sense that they apply to PII owners or, controllers, to use the GDPR terminology.

All specific processor and controller duties resulting from the GDPR apply directly in Portugal. Administrative penalties and criminal infractions apply to the latter, while entities that process personal data on behalf of the controller (when in breach of specific processor legal duties or duties applicable to both processor and controller).

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 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?

The provisions contained in the General Data Protection Regulation (GDPR), particularly those in articles 6 and 9 on the requirement that the holding of personally identifiable information (PII) be legitimised on specific grounds, fully apply.

In line with article 6 of the GPDR, PII processing shall be lawful only if and to the extent that at least one of the following applies:

- the individual has given free, informed and unambiguous consent to the processing of his or her personal data for one or more specific purposes;
- processing of the PII is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the latter prior to entering into a contract;
- PII processing is necessary for compliance with a legal obligation to which the PII owner (controller) is subject;
- PII processing is necessary in order to protect the vital interests of the individual or of another natural person;
- PII processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- PII processing is necessary for the purposes of the legitimate interests pursued by the owner (controller) or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual that require protection of personal data, in particular where the individual is a child.

Legitimate processing – types of PII

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

More stringent rules apply in the case of the 'special categories of data' indicated in article 9 of the General Data Protection Regulation (GDPR). This refers to the processing of genetic PII, biometric PII, PII concerning health, data concerning the individual's sex life or sexual orientation, PII revealing political opinions, trade union membership, religious or philosophical beliefs and racial or ethnic origin, 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 special categories of PII is prohibited with the exceptions provided for in article 9 of the GPDR. Currently, Law 58/2019 of 8 August (the DPA) does not provide for any additional exceptions, that being also the case of the New DPA.

In the case of PII relating to health or sex life, including genetic data, processing is also legitimate on medical grounds (preventive 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.

Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of the official authority or when the processing is authorised by EU or Portuguese law providing for appropriate safeguards for the rights and freedoms of individuals. Any comprehensive register of criminal convictions shall be kept only under the control of the official authority.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 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?

Law 58/2019 of 8 August (the DPA) required owners of personally identifiable information (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.

Information requirements provided for in articles 13 and 14 of the General Data Protection Regulation (GDPR) are now applicable and supersede, as may be applicable, those that were contained in the DPA.

Exemption from notification

14 | When is notice not required?

Notice requirement shall not apply:

- where and insofar as the individual already has the information (article 13(4) of the GDPR) and where personal data has not been obtained from the data subject;
- when notice proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in article 89(1) of the GDPR;
- insofar as notification is likely to render impossible or seriously impair the achievement of the objectives of that PII processing. In such cases the owner shall take appropriate measures to protect the individual's rights and freedoms and legitimate interests, including making notice publicly available;
- obtaining or disclosure is expressly laid down by EU or Portuguese law and provides appropriate measures to protect the individual's legitimate interests; or
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or Portuguese law, including a statutory obligation of secrecy.

Control of use

15 | 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, rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability as provided for in the GDPR.

The right of access comprises the individual's entitlement to obtain from the owner confirmation as to whether or not PII concerning him or her is being processed, and, where that is the case, access to the PII and to all the information provided for in article 15(1)(a) to (h) and (2) of the GDPR.

The right of access also entitles the individual to obtain from the owner a copy of the PII undergoing processing.

Data accuracy

16 | 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.

Amount and duration of data holding

17 | 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, it does, nevertheless, foresee that wherever legal provisions provide for specific retention periods (which, in a number of cases are set-forth as minimum document our information record and retention periods) these will be taken into account by PII owners to set the applicable PII retention periods, the general rule remaining 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, which, although issued prior to the GDPR may also still be taken into account in the present legal context.

Finality principle

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

The finality principle has been adopted in the DPA (same principle had been previously adopted before the GDPR). Under the GPDR, this is reinforced in light of the principles relating to the processing of personal data provided for in article 5 of the GDPR. PII may only be collected for specific, express and legitimate purposes and may not be subsequently used for purposes that are incompatible with the same.

Use for new purposes

19 | 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?

Prior to the GDPR, the general data protection legislation provided that the National Commission for the Protection of Data (CNPD) could authorise, on an exceptional basis, the use of PII for purposes that differ from those that determined its collection, subject to the legally applicable PII quality and processing lawfulness principles. Currently, this is ruled by the GDPR, particularly by the provisions of article 6(4).

The DPA also contains a provision that states that the processing by PII owners that are public entities, for the use of PII for purposes that differ from those that determined its collection is only admitted on an exceptional basis and must be duly grounded on processing being necessary for the performance of a task carried out in the public interest that cannot be satisfied other than with the processing of such PII for that purpose.

SECURITY

Security obligations

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

Under article 32 of the General Data Protection Regulation (GDPR), the owner and the service provider are subject to implementing appropriate technical and organisational measures (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of individuals) to ensure a level of security for personally identifiable information (PII) appropriate to the risk. The adequateness of the measures must be assessed taking into account security and in particular of the risks that are presented by the PII processing, particularly from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to PII transmitted, stored or otherwise kept.

Examples of possible measures are also provided by the GDPR under article 32(2), specifically:

- the pseudonymisation and encryption of PII;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to PII in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Law 58/2019 of 8 August (the DPA) provides that the government will identify, through appropriate regulation the minimum-security measures and technical requirements that must be adopted by PII controllers and processors when processing health and genetic data, including minimum measures on:

- differentiated PII access permissions, based on a 'need to know' principle and the segregation of roles;
- requirements for prior authentication of access to such PII; and
- guarantee that logs or other types of electronic registration are kept to allow such data access traceability.

Regulation has been issued indication minimum-security measures and technical requirements, in some cases mandatory and in other cases, recommended as best practices, for public entities.

Notification of data breach

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

Prior to the GDPR there was no general obligation to notify the supervisory authority or individuals of data breaches as this was a sector-specific requirement for data breaches in the electronic communications sector, which remain. Under the sector specific rules, the National Commission for the Protection of Data (CNPD) must be notified of data breaches by the PII owner without undue delay. In addition, if the breach was likely to adversely affect individuals (ie, telecom service subscribers or users), PII owners were also required to notify the individuals concerned, also without undue delay. In the latter case, a data breach is deemed to affect PII individuals negatively where it may cause identity fraud or theft, physical or reputational damage, or humiliation.

Under the GDPR and the current DPA, the data breach notification obligations to the supervisory authority and communication of a personal data breach to the data subject are provided for under articles 33 and 34 respectively, fully apply. Therefore, a general obligation to notify the supervisory authority (ie, the CNPD) of data breaches has been applicable since 25 May 2018.

Under the current rules, PII breaches must be reported by the PII owner to the CNPD without undue delay and within 72 hours after having become aware of the breach. Only if a PII breach is unlikely to risk harm to the rights and freedoms of the data owners will the reporting requirement be waived. In such cases, the PII owner must still keep a record of the breach and the risk assessment that justified it not reporting the PII breach.

The CNPD has provided PII owners with specific online forms for data breach notification.

When the PII breach is likely to result in a high risk to the rights and freedoms of the affected individuals, the PII owner shall also communicate the breach to same individuals without undue delay.

INTERNAL CONTROLS

Data protection officer

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

In Portugal, before the General Data Protection Regulation (GDPR), the appointment of a data protection officer was not required. Since 25 May 2018, under the GDPR, it is mandatory for certain personally identifiable information (PII) owners (controllers) and processors to appoint a data protection officer (DPO). This is the case for all public authorities and bodies (irrespective of what data they process), and for owners (or processors) that, as a core activity, monitor individuals systematically and on a large scale, or process special categories of personal data on a large scale.

Law 58/2019 of 8 August (the DPA) includes a broad list of entities that qualify as public authority or body for the purposes of being subject to the duty of designating a DPO.

Record keeping

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

Prior to the GDPR, there were no specific or general mandatory requirements for PII owners or processors to maintain internal records or establish internal processes or documentation of the PII processing operations, purposes or activities pursued. In fact, the previous system was based on a prior recording of PII processing activities with the supervisory authority (National Commission for the Protection of Data (CNPD)). This has not been the case, ever since the GDPR applied. All PII owners employing 250 or more persons, shall maintain a record of processing activities under their responsibility. Smaller PII owners, nevertheless, shall also keep such record when carrying out PII processing that is likely to result in a risk to the rights and freedoms of individuals, or is not occasional, or includes special categories of PII (sensitive data referred to in article 9(1)) or PII relating to criminal convictions and offences. The same requirement applies to PII processors.

New processing regulations

24 Are there any obligations in relation to new processing operations?

Under article 25(1) of the GDPR, the PII owner shall, both at the time of the determination of the means for processing the PII and at the time of the processing itself, implement appropriate technical and organisational

measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of individuals. This must be done taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing.

The requirements to carry out a prior assessment of the impact of the envisaged processing operations on the protection of PII under article 35 of the GDPR fully apply in Portugal. The Portuguese supervisory authority has specified the list of PII processing operations likely to result in a high risk and which, therefore, require prior data protection impact assessment. The following are among those listed:

- health PII processing with the aid of an implant;
- PII processing involving large-scale profiling;
- biometric PII processing for unique identification of a natural person or processing of genetic PII, involving individuals such as children and employees (vulnerable individuals). except for processing covered by legal provision which impact has been assessed;
- sensitive PII processing or processing or PII relating to criminal convictions and offences;
- PII of a highly personal nature together with:
  - the use of new or innovative technology;
  - for scientific or historical purpose, public interest archiving purposes or statistical purposes except when authorised by legal provision providing for appropriate safeguards for the fundamental rights and the interests of the individual;
  - based on PII that has not been obtained from the individual and no information may be provided or would involve disproportionate effort to the PII owner; or
  - PII processing that involves PII matching or combining;
  - processing of location PII or behaviour monitoring PII for evaluation or scoring except if strictly required provide services requested by the individual.

The DPA includes a provision whereby this assessment is not required in the case of PII processing that had been previously authorised by the CNPD, under the previous authorisation (and prior notification) regime.

REGISTRATION AND NOTIFICATION

Registration

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

The personally identifiable information (PII) owner is not required to notify the supervisory authority or obtain prior processing authorisation before any PII processing activities are initiated (with the exception of the prior consultation with the supervisory authority before processing that is required from the PII owner under the terms of article 36 of the General Data Protection Regulation (GDPR), where a data protection impact assessment under article 35 of the GDPR indicates that the processing would result in a high risk in the absence of measures taken by the owner to mitigate the risk).

Law 58/2019 of 8 August (the DPA) contains a provision that subjects the use of CCTV systems to prior authorisation from the supervisory authority to be used in surveillance of areas during opening periods, in cases where the system simultaneously captures sound.

Formalities

26 | What are the formalities for registration?

No specific regulation may be found on applicable formalities.

Penalties

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

Not applicable.

Refusal of registration

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

Not applicable.

Public access

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

The National Commission for the Protection of Data register (mainly authorisation decisions) that refers to registrations and authorisations issued prior to 25 May 2018 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.

Effect of registration

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

Not applicable.

Other transparency duties

31 | Are there any other public transparency duties?

There are no general transparency duties in addition to the GDPR requirements.

The DPA includes a general provision requiring that the individual is notified of any access that takes place relating his or her health data. It is for the PII owner to guarantee that a traceability and notification system is in place.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

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

Entities providing outsourced processing services qualify as processors. The processor must only act on instructions from the personally identifiable information (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 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.

All requirements contained in article 28 of the General Data Protection Regulation (GDPR) on the contents of the data processing agreement apply.

Restrictions on disclosure

33 | 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 GDPR and in Law 58/2019 of 8 August (the DPA). 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.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

The transfer of PII to another European Union member state or European Economic Area (EEA) member country 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.

PII may flow from Portugal to non-EU or non-EEA member states that have been covered 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.

Prior to the GDPR, the Portuguese authority did not accept binding corporate rules for the transfer of PII. This is now admitted under the terms of article 47 of the GDPR.

Following the European Court of Justice's landmark judgment in Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* released on 16 July 2020, in which the Court declared the US-EU Privacy Shield invalid, the EU-US Privacy Shield framework is currently not a valid option for exporting data from the EU to the US. The Portuguese National Commission for the Protection of Data (CNPD) has not provided guidance on the impact of the decision. Currently, the standard contractual clauses approved by the Commission will probably prove to be the most feasible alternative for EU-based entities to continue with the transfer of personally identifiable information (PII) required in the context of their activities, subject, therefore, to appropriate data-transfer agreements to be executed. In any case, entities must keep in mind that these agreements will probably need to be modified so as to reflect updates promised by the Commission to same standard clauses, so as to take full account of General Data Protection Regulation (GDPR) provisions, particularly those set forth in article 28 of the GDPR on data-processing agreements between data controllers and data processors.In the absence of an adequacy decision pursuant to article 45(3) of the GDPR or of appropriate safeguards pursuant to article 46 of the GDPR, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the conditions indicated in article 49(a) to (g), being:

- the individual has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for him or her due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the individual and the controller or the implementation of pre-contractual measures taken at the individual's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the PII owner and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the individual or of other persons, where the individual is physically or legally incapable of giving consent; or
- the transfer is made from a register which according to EU or Portuguese law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Portuguese law for consultation are fulfilled in the particular case.

Notification of cross-border transfer

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

No prior notification or authorisation from a supervisory authority is required for the cross-border transfer of PII.

Further transfer

36 | 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).

RIGHTS OF INDIVIDUALS

Access

37 | 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 personally identifiable information (PII) owners. The General Data Protection Regulation (GDPR) provides for the right of access, fully applicable in Portugal. Under the right of access, an individual is entitled to obtain confirmation from the owner whether or not PII concerning him or her is being processed, and, where that is the case, access to the PII and to relevant information on the processing of it. The right of access also entitles the individual to obtain a copy of the PII undergoing processing from the owner.

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.

Other rights

38 | Do individuals have other substantive rights?

Individuals are entitled to require the rectification 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 the same individual.

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

All other substantive rights granted to individuals by the GDPR fully apply: the erasure of PII or restriction of processing concerning the individual, the right to object to processing, and the right to PII portability.

Compensation

39 | 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 PII protection legislation, the same individual is entitled to compensation for damage claimable through the courts. Compensation for serious injury to feelings may be also claimed.

Enforcement

40 | 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

Further exemptions and restrictions

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

Employee biometric personally identifiable information (PII) may only be used for access control (to premises) and worktime control and recording.

When public contracting formalities require that PII are publicised (eg, official gazette publications or equivalent) no PII other than the name of the individual should be published whenever that is sufficient to guarantee the identification of the public contractor and counterparty.

There are specific rule restricting the use of CCTV on certain areas in premises or outdoors.

Law 58/2019 of 8 August does not include derogations, exclusions or limitations other than those already described.

SUPERVISION

Judicial review

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

Personally identifiable information (PII) owners can appeal against orders issued by the National Commission for the Protection of Data to the courts. In the case of decisions issued by the authority applying penalties for administrative misdemeanours, PII owners may appeal to the criminal courts. To appeal against decisions on authorisation or registration proceedings, competence lies with the administrative courts.

SPECIFIC DATA PROCESSING

Internet use

43 | 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 (ePrivacy Directive). The implementation came into effect on 30 August 2012.

Except for essential cookies such as those that enable core website functionality, the use of cookies requires the individuals' consent (ie, they must 'opt-in' to their use) after having been provided with clear and comprehensive information on the use of cookies, as well as on the categories of personally identifiable information (PII) processed and the purposes thereof.

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

Electronic communications marketing

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

The use of automated calling and communication systems without human intervention (automatic calling machines), fax machines or email for the purposes of direct marketing is allowed only 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.

Cloud services

45 | 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 PII owners will fully apply in the case of cloud computing services contracted by the owner.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In the past year, key developments in data protection are still very much around the application of the General Data Protection Regulation and Law 58/2019 of 8 August, which entered into force in August 2019.

Trends and changes on the horizon expected legislation to complement the 2018 law which transposed Directive (EU) 2016/1148, of the European Parliament and of the Council, concerning measures for a high common level of security of network and information systems across the Union and the European Parliament and Council Regulation concerning the respect for private life and the protection of personal data in electronic communications to replace the 2002 ePrivacy Directive.

Covid-19 prevention and mitigation measures have put pressure on personally identifiable information (PII) processing when looking into digital technologies and advanced analytics to provide swift and extensive collection, tracking, combining and sharing of personally identifiable information (PII) for effective responses. In addition, options such as the taking of body temperature to allow access to premises (eg, for employees to access their workplaces and students to their schools) and the use of thermal screening cameras and the use of location-tracking PII and contact monitoring to prevent and fight infection, are some of the approaches that raise discussions and, in some cases, have been controversial in view of the risk they represent to the protection of fundamental rights, particularly when their effectiveness to mitigate the spread of the coronavirus is also questioned.

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

Helena Tapp Barroso
htb@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

Other titles available in this series

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

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-322-7