INTERNATIONAL LAWYERS NETWORK

2024 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.

www.iln.com

Portugal

Introduction

Data protection is being driven by rapid technological advances and the increasing digitalization of society. Data protection legislation in Portugal is aligned with European Union law, in particular with the General Data Protection Regulation ("GDPR" – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016), whose execution in Portugal was ensured by the Personal Data Protection Law ("PDPL" – Law No. 58/2019, of 8 August 2019).

The Portuguese Constitution provides for the protection of personal data and other data whose safeguarding is justified by reasons of national interest, being the National Data Protection Commission ("CNPD") the entity responsible for monitoring and enforcing compliance with data protection legislation.

According to the GDPR, personal data is defined as any information relating to an identified or identifiable natural person ("data subject"). Considering that such personal data can be used to identify a person – either directly or indirectly –, it is therefore essential to guarantee the privacy and security of this data, to protect the rights, freedoms and guarantees of natural persons.

This paper explores the legal panorama of personal data protection in Portugal, highlighting the main differences in relation to the GDPR, as well as the rights of data subjects, the responsibilities of organizations that handle personal data and the consequences of violating data protection legislation.

GOVERNING DATA PROTECTION LEGISLATION

2.1. Overview of principal legislation

In Portugal, personal data protection is primarily provided for within the scope of fundamental rights, in Article 35 of the Portuguese Constitution, which lays the foundations for personal data and data protection. In addition, the PDPL also works as the directory for all other Portuguese data protection

Contact Us

+ 351 213 595 090

www.mgra.pt

hlr@mgra.pt

Avenida 5 de Outubro, 16, Floor 3
Lisbon, 1050-056 Portugal

legislation, ensuring the execution of the GDPR in the Portuguese legal system. The GDPR establishes the framework and rules of the European Union law on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. It should be noted that the GDPR became applicable from 25 May 2018, it is binding in its entirety and directly applicable in all Member States (including Portugal), under the terms of Article 288 of the Treaty on the Functioning of the European Union, and Article 99/2 of the GDPR. In other words, the GDPR embodies the European Union effort to strengthen and unify data protection ruling across all the EU Member States.

Other relevant laws in Portugal, besides the PDPL, are listed below:

- Law no. 59/2019, of 8 August 2019, regarding personal data for the prevention, detection, investigation or prosecution of criminal offences;
- Law no. 41/2004, of 18 August 2004 (as amended), regarding personal data protection and privacy in telecommunications;
- Law no. 43/2004, of 18 August 2004 (as amended), regarding the organization and operation of the National Data Protection Commission ("CNPD").

2..2. Additional or ancillary regulation, directives or norms

There are additional relevant regulations, directives, and standards to the GDPR and the aforementioned Portuguese legislation.

The CNPD (independent and public supervisory authority set up in Portugal under Article 51 of the GDPR) is responsible for monitoring the application of the GDPR to defend the fundamental rights and freedoms of natural persons regarding the processing and the free movement of such data within the European Union. As part of its remit, the CNPD has drawn up regulations and directives, of which we would highlight:

- Regulation no. 798/2018, of 14 November 2018 (Regulation no. 1/2018 CNPD), approved under Articles 35(4) and 57(1)(k) of the GDPR, on the list of processing operations of personal data subject to a Data Protection Impact Assessment (DPIA);
- Regulation no. 834/2021, of 14 April 2021, approved under Articles 43(1)(b), 43(3) and 57(1)(p) of the GDPR, on additional accreditation requirements for certification bodies in relation to ISO/IEC 17065/2012;
- Directive no. 2022/1, of 25 January 2022, on electronic direct marketing communications;
- Directive no. 2023/1, of 10 January 2023, on organisational and security measures applicable to the processing of personal data.

Furthermore, organizations can adopt internationally recognized technical standards and best practices to ensure the security and privacy of data. For example, the ISO/IEC 27001 standard serves as an international benchmark specifying the requirements for an Information Security Management System (ISMS).

ISO/IEC 27001 aims to encompass measures for the implementation, operation, monitoring, review, and continuous improvement of the ISMS. This includes identifying information security risks, implementing appropriate security measures, establishing security policies and procedures, and conducting regular audits and assessments to ensure compliance with the standard's requirements.
Certification in compliance with ISO/IEC 27001 is internationally recognized and demonstrates an organization's commitment and concern regarding information security. It enhances trust among customers, partners, and stakeholders, while also ensuring compliance with legal and regulatory requirements related to the protection of personal data and privacy.

SCOPE OF APPLICATION

3.1 Legislative Scope

3.1.1 Definition of personal data

The GDPR definition of personal data stands as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" – cf. Article 4(1) of the GDPR. Therefore, the concept of personal data encompasses information such as a person's name, home address, email address, identity card number, biometric data (fingerprints or facial features), location data, genetic data and online identifiers (IP address or cookies).

In other words: any information that can be used, either alone or in combination with other information, to identify a natural person is considered personal data and is subject to data protection legislation in Portugal (in particular, and from the outset, to the PDPL).

3.1.2 Definition of different categories of personal data

In Portugal, as well as in the GDPR, personal data is categorized into different types depending on its sensitivity and nature.

Article 9(1) of the GDPR establishes a general prohibition on the processing of special categories of sensitive personal data, namely those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of

uniquely identifying a natural person, data concerning health and data concerning a natural person's sex life or sexual orientation. Without prejudice to the above, this prohibition does not apply if one of the exceptions provided for in the GDPR is met (cf. Article 9(2)(a)-(j) GDPR). As a rule, the processing of this kind of personal data, where permitted, is generally subject to stricter criteria of protection and/or consent.

Special cases of data processing also include personal data relating to (i) children (Article 8 GDPR and Article 16 PDPL), (ii) criminal convictions and offences (Article 10 GDPR) and (iii) deceased persons (Article 17 PDPL).

The PDPL also contains special provisions for specific situations, for example:

- Video surveillance, imposing limits on the incidence of cameras and sound recording (Article 19 PDPL);
- Impossibility of exercising the rights to information and access to personal data (Articles 13-15 GDPR) when the law imposes a duty of secrecy on the controller or processor that is enforceable against the data subject (Article 20 PDPL);
- Articulation of the protection of personal data with the exercise of freedom of expression, information and the press, including the processing of data for journalistic purposes and for the purposes of academic, artistic or literary expression (Article 24 PDPL);
- Publication of personal data in official journals (Article 25 PDPL);
- Access to administrative documents and publication of data in the context of public procurement (Articles 26 and 27 PDPL);
- Processing of workers' personal data in the context of labour relations (Article 28 PDPL);
- Processing of health and genetic data (Article 29 PDPL);
- Processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 31 PDPL)

Additionally, and as a general rule, personal data can also be categorized according to its nature, for example: (i) identification data (i.e., name, identification number, passport number and tax identification number); (ii) contact information (i.e., email address, telephone number and home address); (iii) location data (i.e., GPS data and mobile device location data); (iv) financial data (i.e., credit card information, bank account information and financial transactions history); (v) health data (i.e., medical records, diagnoses and treatments).

3.1.3 Treatment of data and its different categories

Ø Regulation of personal and non-personal data

As referred, personal data is defined in Article 4(1) of the GDPR and consists of any information relating to an identified or identifiable person

On the other hand, non-personal data refers to data that does not relate to an identified or identifiable natural person: in other words, anonymous data or data that has been subsequently anonymized and cannot be attributed or used to identify in any way a specific individual/natural person.

It should be noted, however, that mixed records often contain both personal and non-personal data (i.e., company tax records that include the name and telephone number of the company's director). In most cases, the personal and non-personal data in mixed data sets are inseparable, and if it is a mixed data set, it must therefore comply with the rules of the GDPR and the PDPL.

Ø Regulation of electronic and non-electronic data

In Portugal, electronic and non-electronic data are primarily regulated by the GDPR and the PDPL, which establish rules for the processing of personal data, regardless of the format in which it is stored.

In the field of health and genetic data processing, Article 29(2) PDPL establishes that in the cases provided for in Article 9(2)(h) and (i) of the GDPR, the processing of the data provided for in Article 9(1) of the GDPR must be carried out by a professional bound by secrecy or by

another person subject to a duty of confidentiality, and appropriate information security measures must be guaranteed. Furthermore, access to such data shall be exclusively electronic, unless technically impossible or expressly stated otherwise by the data subject, and its subsequent disclosure or transmission shall be prohibited.

3.1.4 Other key definitions pertaining to data and its processing

Under the GDPR (Article 4) there are several basic definitions relating to data and its processing, of which we would highlight:

- Data subject: the natural person to whom the personal data relates;

- Data controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

- Data processor: the natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

- Data processing: any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction;

- Consent: Statement or clear affirmative action freely expressed by the data subject, agreeing to the processing of their own personal data;

- Personal data breach: breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

These definitions are essential for understanding obligations and responsibilities in this field and, in turn, ensuring that the processing of personal data is carried out ethically and compliantly.

3.2 Statutory exemptions

Data protection laws often provide for exemptions or exceptions to the application of protective measures when processing personal data, in certain circumstances.

For example, certain legal obligations may require the processing of personal data disregarding the consent of the data subject (i.e., to meet tax obligations, conduct criminal investigations or comply with court orders).

In addition, data protection legislation may provide exemptions for the processing of personal data for journalistic, artistic, scientific or cultural purposes, provided that it is carried out in accordance with ethical principles and fundamental rights.

There may also be exemptions for the processing of personal data for reasons of public interest in areas such as public health, public security, crime prevention or protection against threats to public security. However, the data controller, within the scope of these exemptions, is still required to ensure that the processing of personal data is fair, transparent and proportionate to the specific purposes (in other words, subject to appropriate and specific measures to protect the rights and freedoms of natural persons).

3.3 Territorial and extra-territorial application

As a general rule, the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the EU or not (Article 3(1) GDPR).

The GDPR may also be applicable to the processing of personal data of data subjects who are in the EU by a controller or processor not established in this territory (Article 3(2) GDPR) and/or to the processing of personal data by a controller not established in the EU but in a place where the Member State law applies by virtue of public international law (Article 3(3) GDPR).

The PDPL applies to the processing of personal data conducted within Portugal, regardless of the public or private nature of the controller or the processor, even if the processing of personal data is carried out in fulfilment of legal obligations or in the pursuit of public interest missions, with all the exclusions provided for in Article 2 of the GDPR applying.

Regarding the extra-territorial application, the PDPL also applies to the processing of personal data carried out outside Portugal when:

- It is carried out within the scope of the activity of an establishment located in Portugal; or
- It affects data subjects who are in Portugal, when the processing activities are subject to Article 3(2) of the GDPR; or
- It affects data registered in consular offices of Portuguese nationals residing abroad.

Legislative Framework

4.1 Key stakeholders

The data controller plays a central role in the context of personal data protection. The definition of data controller is given by the GDPR (Article 4(7) GDPR) and adopted by the PDPL: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

In addition to the data controller, we find:

- The data subject (Article 4(1) GDPR): the natural person to whom the personal data relates and belongs; both the GDPR (Article 12 and following GDPR) and the PDPL guarantee several rights to the data subjects, aiming to ensure that the data subjects have control over their personal data, and that such data is lawfully processed;

- The data processor (Articles 4(8) and 28 GDPR): the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; it should be noted that the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject;

- The Data Protection Officer / "Encarregado de Proteção de Dados" ("DPO" / "EPD"): designated by the controller and/or processor in certain cases (Article 37(1) GDPR), it shall be involved, properly and in a timely manner, in all issues which relate to the protection of personal data (Article 38(1) GDPR).

4.2 Role and responsibilities of key stakeholders

The data subject shall decide how its personal data is processed and handled and has several rights, such as the right to confirm whether the data is being processed and, if so, to have access to that data and information. Where applicable, the data subject may also: (i) request that inaccurate or incomplete personal data be corrected; (ii) request the deletion of personal data, unless there are legal grounds for its processing; (iii) object to the processing of personal data in certain circumstances, such as in direct marketing situations; (iv) request the restriction of the processing of personal data in certain specific situations.

In its turn, the **data controller** must (i) ensure that the processing of personal data is carried out in accordance with the provisions of the GDPR and national data protection legislation; (ii) define the specific purposes for which personal data are processed and (iii) ensure that the rights of data subjects are respected, including the rights of access, rectification, erasure and portability. The controller should also implement appropriate technical and organizational measures to ensure the security and privacy of personal data.

The **data processor** shall implement technical and organizational measures to ensure compliance with data protection laws (i.e., GDPR and national laws), and shall also manage the storage of personal data on servers or cloud platforms and process personal data on behalf of the data controller (i.e., payment processing and marketing services). Therefore, it is crucial for the controller to select processors who

provide sufficient guarantees regarding the implementation of appropriate security measures and compliance with data protection laws. A formal contract should be established between the two parties, clearly defining the obligations, responsibilities, and security measures that the processor must adopt to protect personal data. The parties shall work together to ensure that personal data is processed in accordance with data protection laws and regulations (Article 28 GDPR).

Finally, the **DPO** (when designated, as per Article 37(1) GDPR) has specific tasks laid down in Article 39 GDPR, such as: (i) inform and advise the controller or the processor; (ii) monitor compliance with data protection legislation; (iii) provide advice where requested as regards the data protection impact assessment and monitor its performance; (iv) cooperate with the supervisory authority; (v) act as the contact point for the supervisory authority on issues relating to processing.

In this regard, the PDPL specifies the criteria laid down in the GDPR and assigns specific duties to the DPO (Articles 9-15 PDPL).

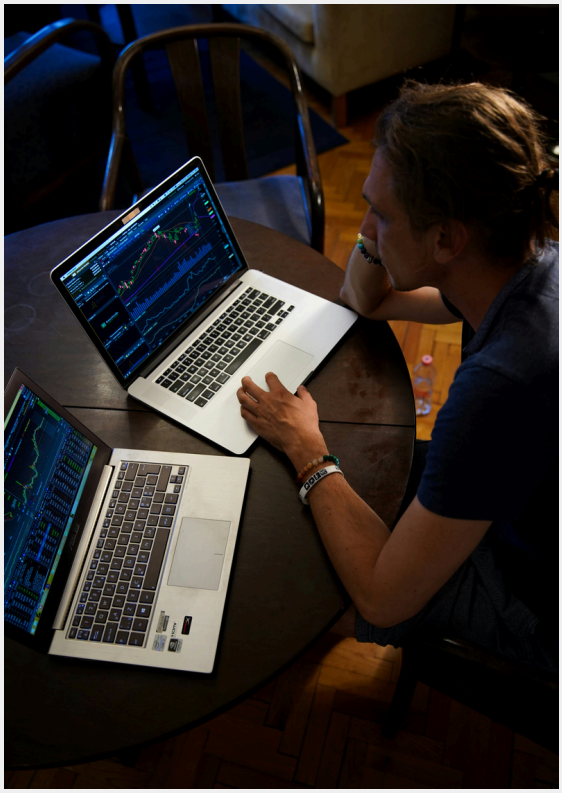
REQUIREMENTS FOR DATA PROCESSING

5.1. Grounds for collection and processing

The processing of personal data is delimited by principles such as (i) lawfulness, fairness and transparency, (ii) purpose limitation, (iii) data minimization, (iv) accuracy, (v) storage limitation and (vi) integrity and confidentiality. The controller is subject to accountability and shall be responsible for, and be able to demonstrate compliance with such principles.

Processing of personal data shall be lawful only if and to the extent that at least one of the following apply (Article 6(1) GDPR):

- the data subject has given consent to the processing of his/her personal data for one or more specific purposes;



- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

- processing is necessary for compliance with a legal obligation to which the controller is subject;

- processing is necessary in order to protect the vital interests of the data subject or of another natural person;

- 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;

- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (except if processing is carried out by public authorities in the performance of their tasks).

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has given informed consent to the processing of his/her personal data. The data subject has the right to withdraw the consent at any time, and such withdrawal shall not affect the lawfulness of processing based on consent previous to withdrawal. If consent is withdrawn, the controller must stop processing the data subject's personal data for the specific purposes for which consent was withdrawn.

5.2. Data storage and retention timelines

One of the main principles of personal data processing is "storage limitation", foreseen under Article 5(1)(e) GDPR, which provides general guidelines for limiting the storage of personal data.

The storage limits and retention periods for personal data are determined by several factors, including the purpose of the data processing, legal requirements, industry-specific regulations and the organization's internal policies.

In Portugal, the PDPL provides specific guidelines on the storage of personal data. As a general rule, the retention period for personal data is set by law or regulation or, in the absence thereof, the period necessary for the fulfilment of the purpose (Article 21(1) PDPL). Furthermore, when personal data is necessary for the controller or processor to prove the fulfilment of contractual or other obligations, it may be kept for as long as the corresponding rights are not time-barred (Article 21(3) PDPL). It should also be emphasized that when the purpose for which personal data was initially or subsequently processed ceases, the controller must destroy or anonymize such data (Article 21(4) PDPL).

5.3. Data correction, completion, updating or erasure of data

According to the GDPR (Articles 12-23 GDPR), data subjects have several rights related to their personal data, framed in (i) information and access to personal data, (ii) rectification and erasure, (iii) right to object and to not be subject to automated individual decision-making. Such rights, however, can be restricted (Article 23 GDPR).

In other words, data subjects have the right to correct, complete, update or even delete their personal data.

A data subject may request the rectification or update of inaccurate or incomplete personal data (i.e., inaccurate or out of date personal data) to ensure that it is accurate and reflects reality.

With respect to deletion, data subjects have the right to request the deletion of their personal data in certain circumstances (i.e., personal data is no longer necessary for the purposes for which it was collected, data subjects withdraw consent, or personal data is processed unlawfully).

The rights of the data subject may be restricted, when such restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure to safeguard, for example, national security, defense or public security.

In particular, the right to erasure ("right to be forgotten") is restricted to the extent that processing is necessary for the exercise of the right of freedom of expression and information, for compliance with a legal obligation, for reasons of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defense of legal claims.

Organizations are required to provide mechanisms for data subjects to exercise their rights, usually through a process for requesting the correction, completion, updating, or deletion of personal data. This process should be easily accessible and data subjects should not be subject to unjustified obstacles in exercising these rights.

5.4 Data protection and security practices and procedures

The security of processing of personal data is essential to ensure the privacy and integrity of the information of data subjects. Article 32(1) GDPR establishes that the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymization and encryption of personal data;
- 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 personal data in a timely manner in the event of a physical or technical incident;

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Access to personal data should be limited to authorized individuals who need the information to perform their duties. Access controls such as multi-factor authentication and monitoring of access activities ought to be implemented. In addition, security measures should be implemented on devices used to process or store personal data, including firewalls, anti-virus software, regular software updates, and restrictions on the installation of unauthorized applications.

Monitoring and auditing systems must be put in place to detect and respond to suspicious or unauthorized activities related to the processing of personal data. In the event of an incident, it is important to develop response plans to effectively manage data security breaches in accordance with legal requirements.

In Portugal, the competent authority for accrediting data protection certification bodies is the IPAC, I. P. (Article 14(1) PDPL) and the competent authority for drafting codes of conduct governing specific activities is the CNPD (Article 15(1) PDPL).

5.5 Disclosure, sharing and transfer of data

Disclosure, sharing and transfer of personal data involves the communication or sharing of personal data between different parties, whether within the same organization or between different organizations.

In many cases, the disclosure, sharing or transfer of personal data requires the explicit consent of the data subject. In some situations, the disclosure or transfer of personal data may be necessary for the performance of a contract, to comply with a legal obligation, to protect the vital interests of the data subject, or for the performance of tasks carried out in the public interest or in the exercise of official authority.

Organizations must therefore implement appropriate security measures to protect personal data during disclosure, sharing or transfer. This includes access controls, activity monitoring and protection against unauthorized access. Tests to identify potential vulnerabilities or threats to data security during disclosure, sharing or transfer also have to be conducted.

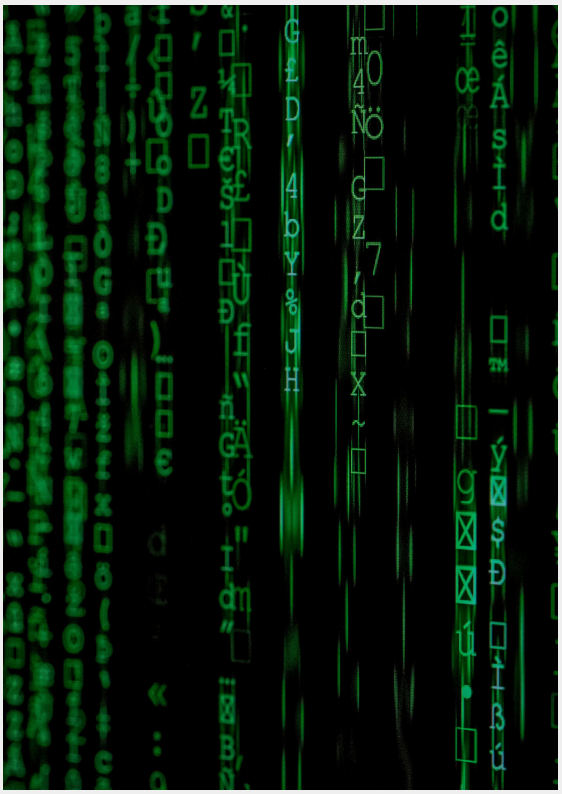
In addition, where personal data is shared with third parties, organizations shall enter into confidentiality agreements to ensure that personal data is treated in accordance with data protection laws.

5.6 Cross border transfer of data

For the purposes of the GDPR, cross-border processing means either:

- processing of personal data in the context of the activities of establishments in more than one Member State of a controller or processor in the EU, where the controller or processor is established in more than one Member State; or

- processing of personal data in the context of the activities of a single establishment of a controller or processor in the EU which substantially affects or is likely to substantially affect data subjects in more than one Member State



Cross-border transfer of personal data involves the transmission of personal information from one country to another. This type of transfer is common in a globalized world, where companies often operate in multiple countries and may need to access personal data of individuals located in different legal jurisdictions.

Transfers of personal data to third countries or to international organizations are regulated in Articles 44 to 50 GDPR. As a general rule (Article 44 GDPR) sets that any transfer of personal data which is undergoing processing or is intended for processing after transfer to a third country or to an international organization, may only occur if the conditions laid down in the GDPR are complied by the controller and processor (including for onward transfers of personal data from the third country or an international organization to another third country or another international organization).

Article 49 GDPR also establishes derogations for specific situations: in the absence of an adequate decision or of appropriate safeguards (including binding corporate rules), a transfer or a set of transfers of personal data to a third country or an international organization can only take place on one of the following conditions:

- the data subject has explicitly consented the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller 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 defense of legal claims;

- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

- the transfer is made from a register which according to the EU or Member State 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 (only to the extent that the conditions laid down by the EU or Member State law for consultation are fulfilled in the particular case).

5.7 *Grievance redressal*

In Portugal, without prejudice to the right to lodge a complaint with the CNPD, any person may resort to means of administrative protection, namely of a petitionary or impugnatory nature, to ensure compliance with the legal provisions, under the terms of the Code of Administrative Procedure (Article 32 PDPL). Furthermore, any person who has suffered damage as a result of the unlawful processing of data or any other act that violates the provisions of the GDPR or the national law on the protection of personal data has the right to obtain compensation from the controller or processor for the damage suffered (Article 33 PDPL).

Complaints relating to personal data can be addressed to the CNPD (national authority responsible for monitoring and enforcing compliance with data protection legislation) which has, amongst other competences, the power to investigate complaints, carry out audits and impose sanctions in the event of infringements.

Complaints and claims shall be submitted in writing via the official website of the CNPD by completing the form with all relevant information.

Upon receipt of a complaint, the

CNPD starts investigation, takes necessary measures to resolve the issue and ensures compliance with data protection laws (i.e., imposing sanctions on the organization that failed to comply with data protection laws).

RIGHTS OF DATA SUBJECTS AND DUTIES OF DATA PROVIDERS

6.1 Rights and remedies

The rights of data subjects are provided for in Articles 12 and following of the GDPR and have no major changes in the PDPL. Data subjects have the rights of information and access to personal data, rectification and erasure of personal data, and to object and to not be subject to automated individual decision-making.

Data subjects also have the right to withdraw their consent to the processing of their personal data at any time. This means that they can revoke a previously given consent to the processing of their personal data. In addition, data subjects have the right to lodge a complaint with the CNPD if they believe that the processing of their personal data was made or is being made in breach of data protection legislation. Data subjects have the right to obtain information about how their personal data is processed, the purposes of the processing, how the data is used and who has access to it.

In addition, data subjects can appoint a representative to act on their behalf and exercise their data protection rights. This can be particularly useful in situations where data subjects are unavailable or unable to act on their own behalf.

6.2 Duties

The duties fall on data controllers and processors, which have several obligations as set out in the data protection legislation (notably, the GDPR and the PDPL).
Data processing must comply with the principles set out in Article 5 GDPR (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality). The controller is responsible for, and shall be able to, demonstrate compliance with such principles (accountability).

Purpose limitation and data minimization imply that data should be collected for specific, explicit and legitimate purposes and should not be processed in a way that is incompatible with those purposes. In addition, data controllers must ensure that the data collected is necessary to achieve the specific purposes of the processing. When the purpose for which personal data was initially or subsequently processed ceases to exist, the controller must destroy or anonymize them.

They shall also provide data subjects with clear, concise and easily accessible information about how their data is processed (i.e., through

privacy policies, privacy notices or consent forms) and ensure data security by implementing appropriate technical and organizational measures to protect against unauthorized access, disclosure, alteration, accidental or unlawful destruction (in other words, personal data breaches).

Public or private organizations must also cooperate with the CNPD, providing it with all the information it requests in the exercise of its powers and competences.
On the other hand, the DPO is also subject to duties of secrecy and confidentiality.
Finally, the rights to information and access to personal data provided for in Articles 13 to 15 GDPR cannot be exercised when the law imposes a duty of secrecy on the controller or processor that is enforceable against the data subject; nevertheless, the data subject may request the CNPD to issue an opinion on the enforceability of the duty of secrecy (Article 20 PDPL).

PROCESSING OF CHILDREN OR MINORS' DATA

The processing of personal data of children or minors in Portugal is subject to specific provisions to ensure adequate protection, considering the vulnerability of these individuals.

The GDPR is directly applicable in Portugal and establishes that consent for the processing of personal data of children is only valid if the child is at least 16 years old (or, if the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child).

Children personal data can only be processed based on the consent provided for in Article 6(1)(a) GDPR and relating to the direct offer of information society services when they have reached the age of 13 (Articles 8 GDPR and 16 PDPL). If a child is under 13, consent for the processing of his or her personal data must be given or authorized by his or her parents or legal guardians, preferably by means of secure authentication.

Therefore, children, as well as their parents or legal guardians, must be provided with clear and transparent information about how personal data will be processed. This includes the purposes of the processing, the categories of personal data involved, who has access to the data and how long the data will be kept.

These data must be treated with special care and protection, considering the vulnerability of a child. This includes implementing appropriate security measures to protect personal data from unauthorized access, disclosure or alteration, and ensuring that processing is transparent.

REGULATORY AUTHORITIES

8.1 Overview of relevant statutory authorities

The CNPD is the national supervisory authority in Portugal for the purposes of the GDPR and the PDPL compliance.

In addition to the provisions of Article 57 GDPR, the CNPD carries out other tasks, specifically foreseen in Article 6 PDPL. Additionally, the CNPD also exercises the powers provided for in Article 58 GDPR.

As already mentioned, the competent authority for accrediting data protection certification bodies is the IPAC, I. P. as set out in Article 43(1)(b) GDPR.

It should also be noted that any person, in accordance with the general rules, may bring actions to the administrative courts against the decisions, namely of an administrative offence nature, and omissions of the CNPD, as well as civil liability actions for the damage that such acts or omissions may have caused.

Other relevant authorities are the National Communications Authority (ANACOM), the Public Prosecutor's Office (MP) and the National Council for Ethics in the Life Sciences.

8.2 Role, functions and powers of authorities

The CNPD is responsible for supervising and enforcing compliance with data protection legislation. Its main functions include promoting the application of data protection laws, issuing guidelines and opinions, investigating complaints and data breaches, imposing corrective measures and applying sanctions in the event of breaches. The CNPD also has investigative and supervisory powers, including the right to access information, request documents, conduct audits, and impose administrative sanctions such as warnings, fines and data processing bans.

In addition to the provisions of Article 57 GDPR, the CNPD has the following duties:

- Issue non-binding opinion on legislative and regulatory measures relating to the protection of personal data, as well as on legal instruments

under preparation in European or international;

- Monitoring compliance with the provisions of the GDPR and other legal and regulatory provisions related to the protection of personal data and the rights, freedoms and guarantees of data subjects, and to correct and penalize non-compliance;

- Keep available an updated list of processing operations subject to data protection impact assessment, pursuant to Article 35(4) GDPR, also defining criteria enabling to specify the notion of high risk provided for in this article;

- Prepare and submit to the European Data Protection Board draft criteria for the accreditation of code of conduct monitoring bodies and certification bodies, under the terms of articles 41 and 43 GDPR, and ensure the subsequent publication of the criteria, if approved;

- Co-operate with the Portuguese Accreditation Institute, I.P. (IPAC, I.P.). in relation to the application of the provisions of Article 14 PDPL, as well as in the definition of additional accreditation requirements, with a view to safeguarding consistency in the application of the GDPR.

Furthermore, the CNPD exercises the powers laid down in Article 58 GDPR.
In addition to general data protection laws, there are specific laws that may affect data protection in certain sectors (notably, the personal data and privacy protection in the electronic communications sector – Law no. 41/2004, of 18 August 2004, as amended).

In this regard, ANACOM is responsible for the regulation and supervision of the electronic communications sector in Portugal, including data protection in certain contexts such as telecommunications and Internet services (i.e., ensuring the security of networks, electronic communications services, privacy in electronic communications and data protection in telecommunications services).

In addition to these authorities, other bodies may have a relevant role in data protection in Portugal, such as the Public Prosecutor's Office that investigates cases of serious breaches of data protection, and the National Council for Ethics in the Life Sciences which can issue opinions on ethical issues related to the processing of personal data in the context of health and biomedical research.

8.3 Role, functions and powers of civil/criminal courts in the field of data regulation

In Portugal, without prejudice to the right to lodge a complaint with the CNPD, any person may seek administrative protection, specifically of a petitionary or impugnatory nature, to ensure compliance with the legal provisions on the protection of personal data, under the terms of the Code of Administrative Procedure.

As for civil liability, any person who has suffered damage as a result of the unlawful processing of data or any other act that violates the provisions of the GDPR or national law on the protection of personal data has the right to obtain compensation from the controller or processor for the damage suffered.

Thus, in general, any person can bring actions against the CNPD's decisions, namely of an administrative offence nature, and omissions, as well as civil liability actions for the damage that such acts or omissions may have caused. Such actions fall within the jurisdiction of the administrative courts.

On the other hand, the data subject may bring actions against the controller or processor, including civil liability actions.

Serious breaches are prosecuted and judged. This includes the person(s) and or/organization(s) responsible for illegal access to information systems, unauthorized disclosure of personal data and other forms of cybercrime related to privacy and data protection.

Overall, civil and criminal courts play a crucial role in enforcing data protection laws in Portugal, ensuring that data subjects have effective remedies in case of violations of their rights and that those responsible for such violations are held accountable in accordance with the applicable law.

CONSEQUENCES OF NON-COMPLIANCE

10.1 Consequences and penalties for data breach

According to Article 4(12) GDPR, personal data violation means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The most serious violations of personal data are classified in the PDPL as criminal offences, e.g., improper access, misappropriation, corruption or destruction of data – Articles 47 to 49 PDPL. Less serious violations of personal data are classified as very serious or serious administrative offences.

On the other hand, organizations that do not comply with the GDPR and or the PDPL may be required to take corrective action to remedy the breach and mitigate any harm caused to data subjects. This may include implementing measures to protect the affected data, notifying data subjects of the breach and, where appropriate, providing compensation for any material or non-material damage. Additionally, they may be subject to the mentioned criminal and administrative offences typified by law.

The CNPD has the power to issue warnings and impose administrative fines on organizations that violate

data protection laws. The CNPD may also intervene in legal proceedings in the event of a breach of the provisions of the GDPR and the PDPL, and must report to the Public Prosecutor's Office any criminal offences of which it becomes aware, in the performance of its duties or on account thereof, as well as carry out any necessary and urgent precautionary acts to secure evidence.

10.2 Consequences and penalties for other violations and non-compliance

On top of administrative sanctions, the person(s) and or organization(s) that violate(s) data protection legislation may face civil actions brought by affected data subjects seeking compensation for damages caused by the breach and or non-compliance with the GDPR and or the PDPL. Additionally, the data subject has always the right to lodge a complaint with the CNPD.

Depending on the nature and severity of the breach and or the non-compliance, regulatory authorities may end up revoking or suspending an organization's license and or authorization to operate in certain sectors, such as telecommunications, financial services or healthcare.

It should be noted that the PDPL does not make a profound distinction between data breaches (in the strict sense) and other breaches of the GDPR or the PDPL, treating data breaches (in the broad sense) as a unitary issue.

In summary, data breaches in Portugal can lead to various consequences and sanctions, including criminal investigations and judgements, administrative and or civil legal actions, administrative fines, reputational damages, loss or suspension of licenses, and complaints to the CNPD as well.

Conclusion

Personal data protection is governed by specific EU and internal legislation such as the GDPR and the PDPL, amongst others. The CNPD is the national independent and public supervisory authority set up in Portugal under Article 51 of the GDPR, primarily responsible for monitoring and enforcing compliance with such legislation.

Personal data is protected on first hand by being framed within the scope of fundamental rights. Data subjects have several rights, including the right of access, rectification, erasure, restriction of processing, data portability and the right to object to the processing of their personal data. If an unforeseen event occurs, data subjects should file a complaint with the CNPD or resort to courts to ensure that their rights are respected and or repair the damage caused.

Data controllers and processors handling personal data in Portugal have clear obligations to comply with data protection legislation, including by implementing appropriate technical and organizational measures to ensure

the security and privacy of the data, under penalty of severe sanctions in case of violation.

The information contained in this "Guide" is provided for informational purposes only and should not, under any circumstances, be understood as legal advice on any subject matter. Recipients of this document, clients or otherwise, should not act or refrain from acting on the basis of any content included in the document without seeking the appropriate legal advice from an attorney on their particular facts and circumstances. Mouteira Guerreiro, Rosa Amaral & Associados, Sociedade de Advogados SP R.L. expressly disclaims all liability for any possible damages caused by actions taken or not taken based on any or all the contents of this document.

This "Guide " and its contents are provided "AS IS" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

Contact Us

+ 351 213 595 090

www.mgra.pt

hlr@mgra.pt

Avenida 5 de Outubro, 16, Floor 3
Lisbon, 1050-056 Portugal