Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

Portugal: Law & Practice

Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.

chambers.com

2019

Law and Practice

Contributed by Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.

Contents

Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL. has a cross-practice, dedicated and business-oriented team comprising specialised lawyers in the field of data protection. The firm's primary office is based in Lisbon, with four other offices located in Porto, Funchal, Angola, Mozambique and Macau. The firm's practice covers different areas of specialism such as Corporate and M&A, Gaming, Litigation and Arbitration, and TMT. It is the firm's belief that compliance with data protection standards should not be an obstacle to the development of clients' businesses and, therefore, we seek to present solutions that are a true compromise between the respect of standards and the interests of our clients.

Authors

Helena Tapp Barroso is a partner, a member of the employment and pensions team and one of the partners in the data protection team. She joined the firm in 2006 and became a non-equity partner in 2010. Helena has wide experience in the areas of labour and employment (including dispute regulation and litigation activity) and she has developed extensive activity throughout her practice on data protection and privacy issues, providing legal assistance in drawing up personal data privacy and protection policies, data protection compliance, assessment and auditing programmes, data processing and data transfer agreements, including specific sector issues for business areas such as insurance and insurance distribution, the media, technology, banking and financial, retail and health) particularly in the GDPR context. Helena is a member of the Portuguese Bar Association (member of the Lisbon District Council from 1999 to 2001) teaching regularly in the postgraduate studies in labour law and data protection studies at several law faculties, as well as regularly contributing to publications on these subjects. Helena is a Certified Information Privacy Professional/Europe (CIPP/E) (International Association of Privacy Professionals – IAPP, 2017).

Tiago Félix da Costa is a partner and head of one of the litigation and arbitration teams - the criminal litigation, administrative sanctions/misdemeanour and compliance team and co-ordinator of the data protection team. He joined the firm in 2007 and became a partner in 2015. Having been a practitioner of law since 2004, Tiago has wide experience in the areas of criminal and misdemeanour litigation and civil, corporate and commercial litigation. Recently, Tiago has acted increasingly in the personal data protection sector, providing legal assistance on criminal and misdemeanour processes in this area and assisting several companies on the creation of policies and programmes of "compliance" in the personal data protection sector. Tiago is a member of the Portuguese Bar Association (admitted in 2004) teaching regularly in the postgraduate studies in different law faculties and has contributed to several publications relating to data protection law. Tiago holds certification from the Advanced Training Course on Data Protection Compliance in the EU (European Institute of Public Administration – EIPA, 2017).

1. Basic National Legal Regime

1.1 Laws

Portugal has had national constitutional privacy provisions for over four decades, and Article 35 of the Portuguese Constitution continues to set forth the main relevant principles and guarantees that rule personal data protection.

The Constitution guarantees all citizens rights of access to, and correction and update of, any computerised data relating to them, as well as full information rights on the purposes and use intended for such data. The Constitution also contains reinforced provisions regarding sensitive data and establishes a general restriction towards third-party access to personal data. A general constitutional provision prohibiting the allocation of a single national number to any citizen is also upheld in Portugal.

Although Article 35 is focused on the use of information technology towards data processing, the same Article contains a rule that states that personal data kept in manual files must receive equivalent protection and guarantees.

Currently – and as of 25 May 2018 – the legal framework for personal data protection in Portugal is 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 ('General Data Protection Regulation') (GDPR).

Although a proposal for specific national legislation providing for specific rules in the context of the GPDR (the 'New DPA') has been under discussion in Parliament since March

2018, final law approval and publication is only expected in 2019.

Before the GDPR, the Portuguese legal framework mainly comprised of a 1998 Data Protection Act (Law No 67/98) (the DPA), which implemented EU Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The DPA is only expected to be formally revoked once the New DPA is finally approved and passed; nevertheless, a number of the DPA's provisions are not totally aligned with the GDPR and, to such extent, should be deemed to have been superseded (derogated) as of May 2018.

1.2 Regulators

The supervisory authority responsible for monitoring the application of the data protection rules and principles in Portugal is the 'Comissão Nacional de Proteção de Dados', better known as the CNPD. The CNPD holds broad powers of investigation, specifically, the power to request information, the power to perform data protection audits and the power to obtain access to the data controller's or data processor's facilities, including equipment and data processing means.

CNPD's powers and responsibilities, as granted by currently applicable law, include:

- compliance supervision and monitoring powers regarding privacy and personal data processing;
- investigation powers related to any personal data processing activities;
- powers of authority, to order personal data blocking, erasure or destruction, and to impose temporary or permanent mandatory orders banning unlawful personal data processing;
- powers to issue public warnings towards data controllers (and processors) failing to comply with privacy and data protection legal provisions; and
- powers to impose fines and to report criminal offences to the public prosecution office.

Once approved, the New DPA will also contain specific measures on the CNPD's role, responsibilities and powers in accordance with Articles 51, 57 and 58 of the GDPR.

1.3 Administration and Enforcement Process

Regulatory offence procedure is split into two phases, which are:

- an administrative phase, where the supervisory authority investigates the relevant facts and ultimately decides whether or not to impose a penalty; and
- a judicial phase, where the respondent may challenge the supervisory authority's decision in court.

The Portuguese Regulatory Offence Act establishes that no penalty may be imposed without the defendant first having been heard regarding all the facts under investigation.

After hearing the defendant, if the supervisory authority decides to impose a penalty, this decision may be challenged in court.

Defendants in a regulatory offence procedure enjoy most due process rights granted in criminal procedure law, namely the presumption of innocence, the right to produce and present evidence and the right to appeal against unfavourable decisions. However, in these procedures, the privilege against self-incrimination is mitigated, since controllers and processors are obliged to co-operate with the CNPD, namely by supplying investigators with documents required and information requests.

1.4 Multilateral and Subnational Issues

As Portugal is an EU Member State, all privacy regulation is either European legislation or local legislation based on European instruments.

The first specific Data Protection Act in Portugal was issued in 1991 (Law No 10/91), at which time constitutional guarantees and protection principles contained in Article 35 had already been in place for 15 years (although the wording of this Portuguese Constitution provision was the object of a few subsequent revisions that added further guarantees). The provisions of the 1991 Act were essentially based on the principles and provisions contained in the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), adopted by the Council of Europe.

Amongst the relevant international instruments adopted in Portugal, Convention 108 (Council of Europe), the European Convention on Human Rights (Article 8) and the Charter of Fundamental Rights of the European Union (Articles 7 and 8) deserve mention.

1.5 Major NGOs and Self-Regulatory Organisations

Currently there are no relevant active privacy and data protection NGOs in Portugal, although there are a few associations that are growing increasingly active on the data protection officer and privacy professional side.

1.6 System Characteristics

The first specifically dedicated data protection law was created in 1991, containing principles inspired by Convention 108, adopted by the Council of Europe. The 1998 DPA that followed implemented EU Directive 95/46. The GDPR provisions now directly apply in Portugal.

E-Privacy rules in Portugal are also EU Directive implemented local laws (EU Directives 2002/58 and 2009/136) and once the new e-Privacy Regulation is finalised and approved this will also apply in Portugal.

1.7 Key Developments

In the past 12 months, the most important developments in data protection and cybersecurity have been the GDPR's entry into force and application, and the transposition through Portuguese Law no 46/2018 of 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.

1.8 Significant Pending Changes, Hot Topics and Issues

The proposal for the New DPA is still pending discussion in Parliament. Final law approval and publication is expected in 2019.

Other significant changes on the horizon over the next 12 months include the approval of legislation that complements Law No 46/2018 and the Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Before the GDPR there were no specific local law requirements for the appointment of privacy or data protection officers. The New DPA proposal under discussion contains specific rules for the designation of the DPO, both for the public and private sectors. As far as the public sector is concerned, the provisions define the entities that qualify as public authorities and bodies for the purposes of the requirement to appoint a data protection officer, and provide for a few rules on the appointment's requirements and role.

As far as private entities are concerned, appointment is required in accordance with the GDPR (ie, in the case of controllers or processors whose core activities consist of processing operations which, by virtue of their nature, their scope and/or their purpose, require regular and systematic monitoring of data subjects on a large scale; or consist of processing on a large scale of special categories of data and/or data relating to criminal convictions and offences). According to the current wording of the New DPA, the proposal does not provide for other cases where the appointment of a privacy or data protection officer would be required.

Even when not legally required, other private sector controllers or processors may choose to appoint a data protection officer as encouraged by EU regulators.

Under the GDPR principles relating to processing of personal data, data controllers are under an obligation to process personal data lawfully, fairly and in a transparent manner in relation to the data subject. Processing is limited to purpose, as personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Lawful bases of processing, in line with the provisions of the GDPR fully applicable in Portugal, include:

- the data subject's specific, free (and therefore able to be withdrawn by the subject, at any time), unambiguous and informed consent (explicit consent for one or more specified purposes is additionally required for processing of sensitive data, when such processing is based on data subject consent);
- processing required 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;
- the legitimate interest of the data controller or a third party – typically, in the case of data processing performed by a private sector controller – except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data;
- processing required by the public interest or – in the case of public authorities or bodies in the performance of their tasks – in the exercise of official authority vested in the controller;
- processing needed to comply with legal obligations imposed on the controller; and/or
- processing that is necessary to protect the vital interests of the data subject or another natural person.

When it comes to the processing of special categories of data – such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation – processing is only admitted under the processing prohibition exceptions in Article 9(2) of the GDPR.

In line with the principles reinforced by the GDPR it is understood that the protection of the rights and freedoms of the data subjects, as regards the processing of their personal data, requires appropriate technical and organisational measures to be taken by controllers and processors to ensure that the requirements of the GDPR are met.

When developing and designing products and services that involve the processing of personal data and when selecting and using solutions to support, develop and offer such products or services, controllers must take into account the right to data protection of potential clients, customers, employees and other affected data subjects in accordance with the principle of data protection by design.

Similarly, the concept and principle of data protection by default, as established in Article 25 of the GDPR, is also fully applicable in Portugal requiring that controllers implement appropriate technical and organisational measures for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed. This applies, among others, to the amount of personal data collected, the extent of their processing and the period of their storage and their accessibility.

Processing operations that are likely to result in a high risk to the rights and freedoms of the data subjects must be subject to prior assessment to be performed by the controller. Such assessment is carried out pursuant to the rules foreseen in Article 35 of the aims of evaluating the origin, nature, particularity and severity of the risk to such rights and freedoms that the intended processing activity will represent. It also allows the controller to determine which measures should be adopted to conform the processing to all principles relating to the processing including, among others, those of lawfulness, fairness, transparency, purpose limitation and minimisation and also to guarantee data accuracy, integrity and confidentiality.

With reference to Article 35(4) and (6) of the GDPR, the CNPD has established a list of processing operations that are subject to the requirement for a data protection impact assessment (DPIA). As was the case with a vast number of other EU supervisory authorities, the draft list prepared by the Portuguese supervisory authority (CNPD) was subject to the consistency mechanism, and the European Data Protection Board (EDPB) assessed such draft and issued an opinion prior to the list being finally approved and issued.

The list was published in the last quarter of 2018 as CNPD Regulation No 1/2018, and aims to identify processing operations likely to result in a high risk and that therefore require a DPIA.

In the case of Portugal, the list includes:

- processing of health data with the aid of an implant;
- processing that involves or results in large-scale profiling;
- processing of biometric data for the purpose of uniquely identifying a natural person when the data subjects qualify as vulnerable subjects (which will include children and employees) with the exception, in both cases, of processing supported by legal provision that has been subject to previous impact assessment;
- processing of genetic data when the data subjects qualify as vulnerable subjects subject to the same exception;
- processing of sensitive data or personal data relating to criminal convictions and offences or data of a highly personal nature:
- with the use of new or innovative technology;
- for scientific or historical purposes, public interest archiving purposes or statistical purposes except when authorised by law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- based on data that has not been obtained from the data subject and the provision of information to the data subject proves impossible or would involve a disproportionate effort; or
- matching or combining datasets; and
- the processing of location data or behaviour monitoring data that may result in evaluation or scoring, except when processing is essential to render services specifically requested by the data subject.

Although there is no strict provision determining that the controller must adopt internal or external privacy policies, based on best practices there are relevant measures to be able to demonstrate compliance with the GDPR, specifically policies (and measures) that meet the principles of data protection by design and data protection by default.

Data subjects are granted the right to access their personal data as provided for in the GDPR. The DPA does not provide for any specific formalities for data subjects to exercise this right and the New DPA is also not expected to do so.

The right of access comprises the subject's entitlement to obtain confirmation from the data controller as to whether or not personal data concerning the subject are being processed and, that being the case, an entitlement to have access to the personal data, to all the information provided for in Article 15(1) (a) to (h) and (2) of the GDPR and to obtain a copy of the personal data undergoing processing.

Data subjects are also entitled to request corrections or updates of inaccurate or outdated data from the controller.

Subjects are entitled 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, subjects are entitled to the right not to be subject to a decision that produces legal effects concerning them

or significantly affecting them, based solely on automated processing of information intended to evaluate certain personal aspects relating to the subject.

Data subjects are also granted erasure rights and the right to restriction of processing, particularly when the data held by the controller does not comply with the provisions and principles set out for processing under the GDPR.

All other substantive rights granted to individuals by the GDPR fully apply, including the right to data portability within the limits provided in Article 20 of the GDPR.

Naturally, none of the above rights are unrestricted and are therefore exercisable under the conditions foreseen in Articles 15 to 22 of the GDPR.

Damages suffered by data subjects as a result of an act or omission purported by the controller in breach of the GDPR provisions or other legal provisions for the protection of personal data will trigger an entitlement to compensation for damage claimable through the courts. Compensation for serious injury to feelings may also be claimed.

2.2 Sectoral Issues

In Portugal, special categories of data (sensitive data) are those set forth in Article 9(1) of the GDPR (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation).

The previous DPA also qualified private life data as sensitive data in line with the special protection granted by the Portuguese Constitution to data concerning the subject's private life. Under the GDPR, nevertheless, this does not qualify as special categories of data.

As referred to above, the GDPR states the general rule that processing of such special categories of data is prohibited with the exception, only, of processing of such data on the grounds or required in the cases provided in Article 9(2) of the GDPR.

Exceptions include, among others:

- explicit consent given by the data subject to the processing of those personal data for one or more specified purposes, except where the law provides that the processing prohibition may not be lifted by the data subject;
- processing necessary for compliance with obligations or exercising rights under employment and social security and social protection laws, as set out in the law or a collective agreement pursuant to the law providing for appropriate safeguards for the rights and freedoms of data subjects;
- protection of the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent;
- processing required for the establishment, exercise or defence of a legal claim or whenever courts are acting in their judicial capacity;
- processing necessary for reasons of substantial public interest on the basis of legal provisions law, which are proportionate, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the rights and interests of the data subjects;
- processing required for preventive or occupational medicine, medical diagnosis, provision of health or social care or treatment or management of health or social care systems and services on the basis of the law or pursuant to a contract with a health professional; and
- requirements resulting from archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of legal provisions.

Under the legislation formerly applicable in Portugal (DPA), financial data was subject to special categorisation (and, as was formerly the case for sensitive data, its processing required prior authorisation from the CNPD). Authorisation and prior notification formalities that applied in Portugal prior to the GDPR are no longer applicable.

The MiFID II Directive (Directive 2014/65/EU on markets in financial instruments) has been implemented in Portugal and involves an increase in record-keeping regarding financial transactions, including requirements on financial intermediaries to keep a record of market orders and information exchanged with investors, which involves relevant financial personal data processing and abiding with high levels of security requirements regarding the electronic processing of data, as well as reinforced requirements regarding the integrity and confidentiality of the data recorded.

The initial proposal for the New DPA that was made public did not include further conditions with regard to the processing of genetic data, biometric data or data concerning health under the provision contained in Article 9(4) with the exception of employee biometric data, the processing for which is required for access control and working hours control.

Nevertheless, relevant discussion has occurred over the need for the New DPA to address the possibility of insurance companies to process health data in the context of all coverages that require health data processing, particularly health insurance, life insurance and personal accident insurance.

Under the GDPR, the processing of data concerning health (as is the case for other special categories of data) is only

admitted under the specific exception grounds foreseen in Article 9(2).

A number of EU Member States have included insurance-specific provisions in national laws passed before 25 May 2018, providing for sector-specific grounds for the processing, in particular, of health data in the insurance industry. These provisions have been provided, in some cases, in the context of the grounds for processing granted by Article 9(2)(g) of the GDPR, which refers to processing that:

"is necessary for reasons of substantial public interest, on the basis of (…) Member States law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

In Portugal, as mentioned above, neither the former DPA nor the initial proposal for the New DPA in the context of the GPDR contained any insurance-specific provisions for processing health data. It is, nevertheless, possible that the final version of the New DPA will address the issue, potentially through a legal provision that acknowledges 'substantial public interest' pursuant to Article 9(2)(g).

The processing of data in the context of electronic communication service providers and services (telecom sector) is subject to specific legislation. Currently, the Regulation is contained in Law No 46/2012 (amending the 2004 legislation), transposing part of Directive 2009/136/EC, amending Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Additionally, Law No 32/2008 of 17 June 2008, on the retention and transfer of personal data for the purposes of the investigation, detection and prosecution of serious crime by competent authorities, implemented Directive 2006/24/EC, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks.

The former DPA did not include a general obligation to notify the supervisory authority or individuals of data breaches, but this requirement has been in force since 2012 in the electronic communications sector, where data breaches have been subject to notification by the controller to the CNPD, without undue delay and if the data breach was likely to adversely affect individuals (typically telecom service subscribers or users). Subjects must also be notified in cases where the data breach may cause identity fraud or theft, physical or reputational damage, or relevant humiliation (thus being deemed to adversely affect the subjects).

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

The use of third-party or marketing cookies requires the subject's consent, upon having been provided with clear and comprehensive information on the use of cookies as well as on the categories of data processed and purposes thereof.

No consent is required where the information is only used for transmission of communications over electronic communications networks, or strictly necessary for the provision of a service requested by the user.

The GDPR provides subjects with the right to data portability, under the conditions and terms provided in Article 20, fully applicable to Portugal. Under this new data subject right, data subjects are entitled to receive, from the data controller, the personal data they previously provided to the same controller in a structured, commonly used and machine-readable format, limited to data that is processed by automatic means and on the basis of the data subject's consent or pursuant to contract. Under the right to data portability, the subject may request that the data is transmitted to another controller without hindrance.

The New DPA proposal contains a provision on portability that underlines that the data subject's right to data portability only includes data that has been provided by the data subject to the controller in wording that may be interpreted in accordance with the understanding contained in Article 29 of the Working Party Guidelines on Portability to include data indirectly 'provided' by the data subject through use of a service or device.

The New DPA proposal also states that, whenever possible, portability should be operated in an open format. In the case of public service bodies it provides that whenever data interoperability is not technically possible the data should be provided to the subject in an open digital format in accordance with the National Regulation on Digital Interoperability (approved and published by the Government in January 2018).

Children receive some specific protection as far as their personal data processing is concerned. Notably, specific requirements apply to language used to provide any information and communication on data processing addressed to a child, which is required to be written in a clear and plain language that the child can easily understand.

Some educational initiatives have been launched to increase child awareness towards the risks connected with the use of the internet, social media and online platforms, but not as part of the official school syllabus.

Under the GDPR, when consent is the basis for child data processing in relation to the offer of information society services directly to a child, parental consent is not required where the child is at least 16-years-old. As permitted by the GDPR, the New DPA contains a proposed provision to lower the age threshold to 13 years.

In 2016, the CNPD issued guidelines on the availability of student (and other data subjects) personal data on school internet pages and in 2018 additional guidelines were issued on the same subject matter regarding university and equivalent institutions.

2.3 Online Marketing

The local Portuguese laws that transposed the e-Privacy Directives (namely Law No 41/2004 as amended by Law 46/2012 governing the processing of personal data and privacy in the electronic communications sector), contains specific provisions on unsolicited communications for marketing purposes.

Unsolicited electronic commercial communications aimed at data subjects (natural persons) are limited to cases where prior consent has been provided, except where the controller has obtained the electronic contact of its customers, in the context of the sale of products or services, in which case the same controller may address the subject of direct marketing on products or services marketed by the controller and similar to those previously provided. This possibility is, however, subject to the controller having provided the subject with the prior possibility of opting out from unsolicited communications, in an easy and free of charge manner, and of providing an easy opt-out option on the occasion of each marketing message that is sent.

Under the guarantees granted by the GDPR (particularly Articles 21(2) and (3)), where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to such processing, including to profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the controller may no longer process such data for those purposes.

Once the current proposal for an e-Privacy Regulation is finally approved, enters into force and replaces the existing e-Privacy Directive, Portugal, as an EU Member State, will be subject to its direct application.

2.4 Workplace Privacy

The Portuguese Labour Code (2009) contains certain provisions on employee privacy, including provisions on monitoring and surveillance.

As a rule, the use of surveillance equipment by the employer to control employee performance is excluded. Closed circuit TV in office premises is lawful only where it aims to protect the safety of persons and goods or when the nature of the activity so requires.

Employees are granted privacy and confidentiality guarantees regarding personal correspondence and messages even when using work email addresses.

Employers are limited in their ability to request information on a candidate's or employee's private life, except for information that is strictly necessary or relevant to assess their aptitude or abilities for the job. In such cases, the specific reasons for requiring such information must be provided in writing by the employer. The same rules apply to information on health or pregnancy and in this case the information must be provided to a doctor who will merely inform the employer on the person's aptitude for the job.

Employers may govern the terms of use of company IT means of communication, but employees are entitled to keep their private use confidential, including the content of personal emails and internet access. Admissible use of IT means of communication should form part of an internal regulation (policy).

The CNPD issued guidelines in 2013 for such purposes.

Before implementing any monitoring system, the employer shall inform the employee about the conditions under which IT and communication equipment made available at the workplace may be used for private purposes and on the monitoring schemes and personal data processing resulting from the same monitoring. Generic monitoring methodologies must be adopted, avoiding the individual consultation of personal data.

The document includes fairly detailed and specific guidelines for phone use and for the use of email and internet access.

Consultation with employee work councils is required for certain types of processing, particularly for the processing of employee biometric data and the use of closed circuit TV in office premises.

The CNPD published a resolution (in 2009) setting forth the conditions according to which whistle-blowing programmes are admissible. Under such resolution, the CNPD's understanding is that the purpose of whistle-blowing (and the purpose of the data processing resulting from whistle-blowing hotlines) must be limited to the internal control of reports of misconduct intended to prevent or repress internal irregularities in the fields of accounting, internal accounting controls, auditing matters, the fight against corruption and banking and financial crimes.

In general, the Portuguese labour law does not establish an obligation to inform works councils about the implementation of this kind of scheme in the company. However, if the company intends to provide binding rules to all employees, the whistle-blower scheme will typically be laid out in an internal company regulation. This type of instrument is subject to prior consultation with employee representative structures (works councils or union representatives).

2.5 Enforcement and Litigation

Any offence, be it regulatory or criminal, must be defined by law, and its elements – including culpability – must be proven beyond a reasonable doubt in order for any penalty to be applied.

Regulatory offences are investigated by the CNPD, which also has the power to convict, although CNPD's convictions may be subjected to judicial review.

Criminal offences are investigated by the Public Prosecutor's Office but only a court may convict a defendant.

Under the GDPR, enforcement penalties for data privacy or data protection violations may reach EUR20 million or up to 4% of a company's total worldwide annual turnover for the preceding financial year, whichever is higher.

Criminal offences related to data protection are currently punishable with fines or prison terms that range from six months to four years.

On 11 October 2018, the CNPD imposed a EUR400,000 penalty on a public hospital in the Greater Lisbon area, for irregularities in access to patients' medical records. This case is relevant for being the first penalty imposed under the GDPR framework, for having a public entity as a defendant, and for dealing with a special category of personal data, specifically medical records.

Legal standards for private litigation regarding alleged data privacy and data protection violations are currently the same as any other civil case regarding personal rights.

The proposal for the New DPA contains rules shifting the burden of proof from the plaintiff to the data controller and data processor.

Portuguese civil procedure law allows for class action lawsuits for the protection of consumer interests, which may include consumers' right to privacy and personal data protection.

In 2018, the Portuguese Association for Consumer Protection (DECO), following the Cambridge Analytica scandal, sued Facebook for unlawful processing of Facebook's Portuguese users' personal data.

This case is relevant because it is one of the first class actions in Portugal based on a data protection violation.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Law enforcement access to data for serious crimes is covered by the Criminal Procedure Code and the Portuguese Cybercrime Law. Public prosecutors may unilaterally authorise the search and seizure of stored computer data, except for data covered by professional privilege, in which case access to those systems must be ordered by an investigating judge.

Law No 32/2008 establishes the legal framework for the collection of meta data by law enforcement. The collection of meta data must be authorised by an investigating judge and must be indispensable for the investigation of crimes at hand.

3.2 Laws and Standards for Access to Data for National Security Purposes

Organic Law no 4/2017 establishes the legal framework for the collection of meta data by intelligence services. The collection of meta data must be authorised by a special section of the Supreme Court and must be proportional to the ends for which such data is collected.

3.3 Invoking a Foreign Government

Access to data by foreign governments must be carried out via the Judiciary Police and comply with the principles of international co-operation established in the Cybercrime Law, without prejudice to any applicable international conventions.

3.4 Key Privacy Issues, Conflicts and Public Debates

Access to meta data by intelligence services is an issue that has divided Parliament and raised questions of constitutionality. At first the law that allowed access to meta data by intelligence services was deemed unconstitutional by the Constitutional Court, since the Portuguese Constitution only allows for access to communications in the context of criminal investigations. The current law's constitutionality was challenged by a number of members of Parliament and is currently being evaluated by the Constitutional Court.

4. International Considerations

4.1 Restrictions on International Data Issues

The transfer of personal data to another European Union Member State and European Economic Area (EEA) member

countries is not restricted. Transfer outside these territories is restricted.

Transfers of personal data to third countries or international organisations is permitted only when it is compliant with the requirements of the GDPR and when the state to which data is transferred ensures an adequate level of protection assessed in the light of all the circumstances surrounding the data transfer, with special consideration being given to the nature of the data to be transferred, the purpose and duration of the proposed processing, the country of final destination, the rules of law in force in such country (both general and sector rules) and the professional rules and security measures applicable in such country.

Data may be transferred from Portugal to a non-EU or non-EEA country covered by an adequacy decision issued by the European Commission, which acknowledges that the country in question ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.

4.2 Mechanisms That Apply to International Data Transfers

Transfer may also be made under contracts that follow the standard form model clauses approved by the European Commission, although currently approved standard clauses have yet to be adopted and updated in line with the GDPR.

Prior to the GDPR, the CNPD was amongst the supervisory authorities that rejected the 'binding corporate rules' as a support for data transfer, but this is now allowed under Article 47 of the GDPR.

Transfer to the US is permitted under the EU–US Privacy Shield.

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 if:

- the data subject explicitly consents 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 undertaken in the interest of the 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 defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the individual is physically or legally incapable of giving consent; or
- the transfer is made from a register that, according to law, is intended to provide information to the public and that 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 law for consultation are fulfilled in the particular case.

4.3 Government Notifications and Approvals

There are no prior government notifications or approvals required to transfer data internationally in Portugal.

4.4 Data Localisation Requirements

Portuguese law does not provide for any requirement for data to be maintained in-country.

4.5 Sharing Technical Details

Article 27(1)(o) of the Electronic Communications Law requires electronic communications service providers to install and make available to the authorities communications interception systems, as well as decryption methods whenever encryption services are offered.

4.6 "Blocking" Statutes

Article 48 of the GDPR establishes that judicial and administrative decisions that require the transfer or disclosure of personal data may only be recognised or enforced if they are based on an international agreement, without prejudice to other grounds for transfer found in Chapter V of the GDPR.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

The provisions of Article 22 of the GDPR on automated individual decision-making (including profiling) fully apply in Portugal. Therefore, the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning the data subject, or similarly significantly affects the data subject, is granted to all data subjects. Such automated decision-making processing is restricted to cases where the decision:

- is necessary for entering into, or for performing a contract between, the data subject and the controller;
- is authorised by law applicable to the controller and lays down suitable measures to safeguard the data subject; or
- is based on the data subject's explicit consent.

Additionally, the data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her based on legitimate interests or in the public interest, including profiling. When the subject objects to such processing, the controller shall not continue unless it is able to demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The use of employee biometric data for access control and work time controlling was also addressed by the CNPD in specific guidelines issued in 2004, although some of these have to be read in the light of the new legal framework and interpreted accordingly, particularly because a number of principles would have been considered by the CNPD under the prior system to have required prior notification to the authority for the processing of biometric data for controlling access and monitoring hours worked.

The New DPA proposal contains a provision stating that the processing of employee biometric data is (only) admissible for the specific purposes of access control and monitoring hours worked.

Geolocation is another area in which the CNPD issued guidelines, in 2014, focused on the processing of employee personal data resulting from the use of geolocation devices. The CNPD's understanding – which has found support in some court decisions – is that the use of GPS devices and the tracking they allow is equivalent to a distance surveillance system and their use – and the processing of data that results from their use – should be limited to purposes of safety protection or when the nature of the activity so requires.

The first relevant line drawn by the authority in the guidelines issued is that the employer shall not process data collected by geolocation (typically GPS) systems that reveal employee movements outside his or her working time. Within the limits of the employee's working time, the CNPD considers that the processing of such data to pursue purposes of efficiency, service quality, optimisation of company resources or protection of property is legitimate. Geolocation data shall not be used to control employee performance.

The CNPD's understanding is restrictive on the ability of the employer to use geolocation devices – and processing information thus collected – on smartphones and laptops attributed to employees as opposed to the use of the same devices in company vehicles. In the latter case, legitimate use and purposes are specifically indicated in the guidelines regarding fleet management in the case of activities involving services rendered to clients outside company premises, for the protection of property against theft and activities involving transportation of dangerous substances or high value goods. Clear and transparent information must be provided by the employer to their data subject employees on the use of geolocation devices included in vehicles or equipment used by the employee when performing his or her role.

The Portuguese Civil Aviation Authority (ANAC) issued a Regulation in December 2016 (Regulation No 1093/2016) implementing specific provisions and rules on the use of drones in Portuguese airspace.

Drone flights require prior authorisation by the ANAC except in cases where:

- the flight occurs in daylight;
- within a maximum altitude of 120 metres above the ground; and
- visual contact with the drone is kept at all times.

Night flights or flights over groups of more than 12 people requires specific prior authorisation.

There are a number of relevant restrictions applicable to flights in the surroundings of airport infrastructures or other aircrafts, and fines of up to EUR250,000 may apply in the case of breach of regulatory provisions.

This authorisation does not apply or refer to any data processing that occurs in connection with the use of drones (namely to the collection of photos of filming) and such processing is within the scope of data processing activities subject to the provisions of the GDPR.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators

The 'Centro Nacional de Cibersegurança Portugal National Cybersecurity Centre' (CNCS) is the Portuguese national authority dedicated to cybersecurity, working with public authorities (public service) critical infrastructure and essential services operators as well as digital service providers. As the CNCS itself describes, its mission is to:

"(…) contribute to the free, reliable and secure use of cyberspace in Portugal, through the continuous improvement of national cybersecurity and international co-operation, in co-ordination with all competent authorities, and the implementation of measures and instruments required for the anticipation, detection, reaction and recovery of situations that, in the imminence of occurrence of incidents or cyberattacks, may compromise the operation of critical infrastructures and national interests."

6.2 Legal Requirements

In March 2018 the Portuguese government issued a resolution (Resolution No 41/2018) defining technical guidelines to be adopted by the public services (and recommended to

public sector companies) regarding measures for the security architecture of networks and information systems, aimed at defining a minimum baseline on adequate technical and organisational measures to be adopted by such entities, pursuant to being GDPR-compliant. An 18-month period was provided for the public services to adopt the compulsory technical measures provided in the Resolution, which additionally includes a number of merely recommended measures.

6.3 Data Breach Reporting and Notification

The previous DPA did not include any general notification requirements in the case of security incident data breach, either to the local data protection authority or to data subjects. This was, therefore, specific to the electronic communications sector, before the provisions of the GDPR became applicable.

Under the provisions of the GDPR, fully applicable in Portugal, personal data breaches must be notified by the controller to the CNPD without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

Notification to the CNPD can be made online via an appropriate form made available by the authority on its public website.

Pursuant to Article 44(1) of the GDPR, in the event that the personal data breach is likely to result in a high risk to the rights and freedoms of the affected data subjects, the controller shall also communicate the personal data breach to the data subjects without undue delay.

Law No 46/2018 (which implemented Directive (EU) 2016/1148 – NIS Directive) requires various service providers to notify the CNCS in the event of cybersecurity incidents.

The CNCS is the national competent authority in Portugal both for digital service providers and operators of essential services.

Under the implementation provisions, the public administration and critical infrastructure operators shall notify the CNCS of incidents having a relevant impact on network security and information systems, within the period provided for in specific legislation. This notification must include information that allows the CNCS to determine the transborder impact of the incident. Whenever the circumstances allow, the CNCS provides the notifier with the relevant information regarding the follow-up of the notification, namely information that may contribute to the efficient handling of the incident. After consulting with the notifier, the CNCS may disclose specific incidents with respect to public interest, safeguarding the safety and interests of critical infrastructure operators.

Operators of essential services notify the CNCS of incidents with a relevant impact on the continuity of essential services provided by them, within the period provided for in specific legislation. This notification must also include information that allows the CNCS to determine the transborder impact of the incident.

Providers of digital services must notify the CNCS of incidents with a substantial impact on the provision of digital services, within the period provided for in specific legislation. This notification must include information that allows the CNCS to determine the significance of the transborder impact. The obligation to notify an incident is only applicable if the digital service-provider has access to the necessary information to assess the transborder impact of an incident. If these incidents concern more than one Member State, the CNCS must inform the single contact point of the other Member States involved.

6.4 Ability to Monitor Networks for Cybersecurity

Article 18 of the Cybercrime Law allows for the real-time interception of content and traffic data for the investigation of cyber-crimes and crimes where wiretaps would be allowed under the Criminal Procedure Code. The real-time collection of data must be authorised by an investigating judge and must be indispensable for the investigation of the crimes at hand.

6.5 Cyberthreat Information Sharing Arrangements

The CNCS is also responsible for liaising with the private sector on cybersecurity incidents. In the context of the CNCS, the so-called national network of CSIRTs is organised, consisting of a forum that enables sharing of operational information aimed at:

- building a trust network between computer security professionals towards a co-operative and mutual assistance environment for incident treatment and sharing of best practice;
- developing indicators and national information statistics on security incidents to improve proactive and reactive counter measures;
- creating co-operation instruments for the prevention and quick answer in a large-scale incident scenario; and
- promoting a security culture in Portugal.

Notwithstanding the above-mentioned obligation to notify incidents, any entities may voluntarily notify the CNCS of incidents with a significant impact on the continuity of services provided by them, pursuant to Article 20 of Law No 46/2018.

The voluntary notification cannot give rise to the imposition of obligations to the notifying entity, to which that entity would not have been subjected, had it not made that notification.

6.6 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

There are a number of regulatory offences laid down in Law No 46/2018. These offences are divided between 'serious offences' and 'very serious offences.'

Very serious offences, which include non-compliance with the obligation to implement security requirements and non-compliance with the instructions of cybersecurity issued by the CNCS, are punishable with a fine of between EUR5,000 and EUR25,000, in the case of an offence by a natural person, and a fine of between EUR10,000 and EUR50,000, in the case of an offence by a collective entity.

Serious offences include non-compliance with the obligation to notify the CNCS of any incidents occurred, non-compliance with the obligation to notify the CNCS of activities carried out in the digital infrastructure sector, and non-compliance with the obligation to notify the CNCS of identification as a digital service-provider. These offences are punishable with a fine of between EUR1,000 and EUR3,000, in the case that the offence is committed by a natural person, and a fine of between EUR3,000 and EUR9,000, if the offence is committed by a collective entity.

Regarding private litigation, the general principles of civil law apply to data security incidents or breaches.

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Rua Castilho, 165
1070-050 Lisboa

Tel: +351 21 381 74 00
Fax: +351 21 381 74 99
Email: mlgtslisboa@mlgts.pt
Web: www.mlgts.pt