COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Portugal

DATA PROTECTION & CYBERSECURITY

Contributor

Sérvulo & Associados

José Lobo Moutinho

Equity Partner | jlm@servulo.com

João Carmona Dias

Partner | jcd@servulo.com

Inês de Sá

Senior Associate | is@servulo.com

Ana Margarida Cerqueira

Trainee | amc@servulo.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Portugal.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

PORTUGAL
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The key laws which govern the protection of personal data in Portugal are the following:

- Constitution: sets out fundamental rights specifically related to the protection of personal data.
- 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 or «GDPR»): general and detailed regime governing the processing of personal data, which applies directly in Portugal as a member state of the European Union.
- Law no. 58/2019, of 8 August 2019: supplements the GDPR.
- Law no. 59/2019, of 8 August 2019: sets out the rules on the processing of personal data by competent authorities for the purpose of prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (transposes into the Portuguese law the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016).
- Law no. 41/2004, of 18 August 2004, as last amended by Law no. 46/2012 of 28 August 2012: sets out the rules concerning the processing of personal data and the protection of privacy in the electronic communications sector (transposes into the Portuguese law the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002).

Other important acts which apply in Portugal are the European Convention on Human Rights, as regards right to respect for private and family life, the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data («Convention 108») and the Charter of Fundamental Rights of the European Union, regarding specifically rights to personal data protection.

The GDPR and Law no. 58/2019 govern any processing of personal data, by any natural person or legal entity, wholly or partly by automated means and the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, excluding the processing of personal data by a natural person in the course of a purely personal or household activity and the processing in the course of certain activities, such as activities concerning national security, by the state in activities concerning foreign and security policy and by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

The monitoring and enforcement of GDPR, Law no. 58/2019 and other data protection legal and regulatory provisions in Portugal are entrusted to one specific authority: Comissão Nacional de Protecção de Dados.

The key laws which govern the cybersecurity in Portugal are the following:

- Law no. 46/2018, of 13 August 2018: establishes the legal framework for cyberspace security applicable to public administration entities, critical infrastructure operators, operators of essential services, digital service providers and other entities using networks and information systems

(transposes into the Portuguese law the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of network and information security across the European Union).
- Decree-Law no. 65/2021, of 30 July 2021: regulates the above mentioned legal framework for cyberspace security and defines cybersecurity certification obligations.

The monitoring and enforcement of these laws are entrusted to one specific authority: Centro Nacional de Cibersegurança.

2. Are there any expected changes in the data protection, privacy and cybersecurity landscape in 2023-2024 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

It may be expected a new regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications. If this regulation is approved, it will apply directly in Portugal and will change or replace the current Portuguese law on processing of personal data and protection of privacy in the electronic communications sector.

There are other proposals adopted by the European Commission and under legislative process for new regulations of the European Parliament and of the Council which are also supposed to apply directly in the member states of the European Union, as Portugal, and might supplement data protection laws in Portugal. They are: the proposal for a regulation on harmonised rules on artificial intelligence («Artificial Intelligence Act»), published on 21 April 2021; the proposal for a regulation on fair access to and use of data («Data Act»), published on 23 February 2022; and the proposal for a regulation on the European Health Data Space, published on 3 May 2022.

Regarding cybersecurity, Portugal must transpose into the national law up to 17 October 2024 a new directive on measures for a high common level of cybersecurity across the European Union (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022), which will imply changes into the current Portuguese laws on cybersecurity.

Also, on 15 September 2022 the European Commission published a proposal for a new regulation on horizontal cybersecurity requirements for products with digital elements («Cyber Resilience Act»), also to apply directly in Portugal, which is under legislative process.

3. Are there any registration or licensing requirements for entities covered by these laws, and, if so, what are the requirements? Are there any exemptions?

There are no registration or licensing requirements for entities covered by the above-mentioned laws, meaning no registration or license is required so that such entities may process personal data.

However, there may be cases where specific operations of processing of personal data depend on a prior decision of the supervisory authority (for example where prior consultation with the supervisory authority is required) or where such entities are required to provide information to the supervisory authority (for example as regards the appointment of data protection officers, where applicable).

4. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The data protection laws applicable in Portugal use the terms «personal data» and «special categories of personal data».

«Personal data» means any information relating to an identified or identifiable natural person, being an identifiable natural person the 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.

«Special categories of personal data» are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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.

Other key definitions used in the laws are the following:

- «Processing», any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- «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; where the purposes and means of such processing are determined by law, the controller or the specific criteria for its nomination may be provided for by law;
- «Processor», a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- «Data subject», the natural person whom the personal data relates to.

5. What are the principles related to the general processing of personal data or PII. For example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction, or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

There are principles which summarize the basic rules on processing of personal data in general. Under such principles, personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject («lawfulness, fairness and transparency»);
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes («purpose limitation»);
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed («data minimisation»);
- Accurate and, where necessary, kept up to date, wherefore every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay («accuracy»);
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed («storage limitation»);
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures («integrity and confidentiality»).

Moreover, the controller shall be responsible for and be able to demonstrate compliance with the above-mentioned principles («accountability»).

Regarding the lawfulness of processing in particular, any processing of personal data must comply with at least one of the legal bases specified by the GDPR. In general, the processing of personal data shall be lawful only if and to the extent that at least one of the following cases applies:

- The data subject has given consent to the processing of his or 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.

6. Are there any circumstances where consent is required or typically used in connection with the general processing of

personal data or PII?

In general, the consent of the data subject is one of the legal bases on which depends the lawfulness of processing of personal data and it is as valid as other bases laid down by law.

Nevertheless, under the Portuguese law there are few cases where the data subject's consent is specifically required. For example, the law on processing of personal data and protection of privacy in the electronic communications sector requires the data subject's prior consent for the following purposes:

- To record communications and the related traffic data when carried out in the course of a lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication with the data subject;
- To store information or to gain access to information stored in the terminal equipment of a subscriber or user, unless for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service; and
- To send unsolicited electronic communications for direct marketing purposes, in particular through the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail, including SMS, EMS and MMS messages and other similar, although the requirement of consent is softened in the context of existing customer relationship if the supplier intends to use the electronic contact details which it has collected from its customers for the offering of its own similar products or services.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

The consent of the data subject must be a free, specific, informed and unambiguous indication of wishes by which the data subject, by a statement or by a clear affirmative action, agrees to the processing of personal data relating to him or her. In the absence of any such requirements, consent is not valid.

In some cases, the data subject's consent must be explicit (more than unambiguous), for example for the processing of special categories of personal data and for sending unsolicited electronic communications for direct marketing purposes.

If the consent is to be given in the context of a written declaration which also concerns other matters (for example terms of service), the request for consent shall be presented to data subject in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain declaration. Otherwise it shall not be binding.

For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.

Consent should cover all processing activities carried out for the same purpose or purposes and, when the processing has multiple purposes, consent should be given for all of them.

The data subject is entitled to withdraw the consent at any time and in a way as easy as to give it, although without affecting the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw the consent.

In accordance with the accountability principle, the controller shall be able to demonstrate the data subject's consent.

8. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection or disclosure?

The processing of special categories of personal data is prohibited unless one of the following additional requirements is fulfilled:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- Processing is necessary for carrying out the obligations and exercising specific rights of

the controller or of the data subject in the field of employment, social security and social protection law;
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- Processing is related to personal data which are manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest, on the basis of the 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;
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis the law or pursuant to contract with a health professional;
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of the law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes 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.

The processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of an official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects.

9. How do the laws in your jurisdiction address children's personal data?

The processing of children's personal data is subject to the same provisions of processing of personal data in general, but with additional specific protection, considering that children may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

As regards the processing of personal data related to the offer of information society services directly to children, the processing based on children' consent is lawful provided that they are at least 13 years old. For children of age below 13 years, the consent must be given by the holders of parental responsibility.

When controllers provide information or communication related to the processing, they must take extra care if they are addressing to children and use such clear and plain language that the child can easily understand.

Also, if for a given processing of personal data related to a child the controllers wish to rely on the necessity of such processing for the purposes of legitimate interests as legal basis for the processing (which requires that such legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject), controllers must take into special consideration the fact that the data subject is a child when assessing the impact on the child's interests or fundamental rights and freedoms.

10. How do the laws in your jurisdiction address health data?

Personal data concerning health are defined under the law as personal data relating to the physical or mental health of a natural person, including the provision of health services, which reveal information about the state of health of that person.

Personal data concerning health are addressed as a special category of personal data and their processing is subject to additional restrictions and requirements of security and confidentiality. For example, any access to personal data concerning health is subject to a need-to-know principle and must be notified to the data subject. Even processing for the purposes of preventive or occupational medicine, assessment of working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services can only be processed by or under the responsibility of a professional subject to the obligation of professional secrecy or by another person also subject to an obligation of secrecy.

Apart from the general laws on data protection, there are other laws which include specific provisions on processing of personal data concerning health, for example the law concerning personal genetic information and health information (Law no. 12/2005, of 26 January 2005); the law concerning clinical investigation (Law no. 21/2014, of 16 April 2014); and the law which establishes a public health surveillance system that identifies risk situations, collects, updates, analyses and disseminates data on communicable diseases and other public health risks, and prepares contingency plans for emergency situations or situations as serious as public calamity (Law no. 81/2009, of 21 August 2021).

11. Do the laws include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

Apart from the fields of processing of personal data which are excluded from the scope of the general data protection laws, namely the GDPR and Law no. 58/2019, the national law also includes some derogations from the general rules as regards, for example, the processing of personal data for journalistic purposes or the purpose of academic, artistic or literary expression, to reconcile the right to the protection of personal data with the freedom of expression and information; and also the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, where the data subjects' individual rights to access, to rectification, to restriction of processing and to object to processing are restricted, although subject to certain conditions and safeguards.

Furthermore, the scope of specific controllers' obligations and of data subjects' rights may be restricted by legislative act under certain conditions, when such restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard, *inter alia*, important objectives of public interest. An example of such restriction can be found in the law on prevention and combating of money laundering and terrorist financing (Law no. 83/2017 of 18 August 2017, as last amended by Law no. 99-A/2021 of 31 December 2021), which sets out limitations to the data subjects' individual rights to information and of access to personal data.

12. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

In Portugal, controllers must comply with requirements of «data protection by design» and of «data protection by default» regarding any processing of personal data.

Data protection by design requires that the controllers, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures which are designed to the data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

To comply with this requirement, controllers must take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

Data protection by default requires that the controllers implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Furthermore, the measures to be implemented must ensure that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

13. Are owners/controllers or processors of

personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Each controller or processor which employs 250 or more persons is required to maintain a record of data processing activities, as well as each controller or processor which employs fewer than 250 employees but carries out a processing which is likely to result in a risk to the rights and freedoms of data subjects, a processing not occasional or a processing which includes special categories of data or personal data relating to criminal convictions and offences.

The information to be included in such record varies according to the capacity in which an entity carries out the processing – controller or processor – and the record itself needs to be in writing, including in electronic form.

There are different ways to set this record, depending on the resources of the organizations. The supervisory authority also makes available templates for the purpose.

Regardless of the record of data processing activities, any controller has a duty to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing is performed in accordance with the GDPR, in line with the principle of accountability. This implies that any controller must establish documented processes and records to comply with the data protection laws' requirements.

Moreover, there are also requirements of records and documents which controllers must comply with in specific situations, for example a record of personal data breaches.

14. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

The law requires that personal data should only be kept in a form that permits identification of the individual for no longer than is necessary for the purposes for which the personal data are processed, in line with the principle of storage limitation. After that, the controllers must delete or irreversibly anonymize the data.

Furthermore, as general rule, the controller must define a period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period. This requirement arises out of different provisions of the GDPR, such as those concerning the controller's obligations of transparency and information to be provided to data subjects concerning the processing of their personal data, as well as rules concerning the record of data processing activities, where applicable.

15. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

The controllers are required to consult with the supervisory authority prior to the processing if, after having performed an assessment of the impact of certain processing operations on the protection of personal data, the outcome of such assessment indicates that the processing will result in a high risk to the rights and freedoms of natural persons, despite the measures considered by the controller to mitigate the risks.

16. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

The law requires that the controllers, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where the processing is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the processing, in particular if new technologies are to be used.

The GDPR lists three examples of data processing activities which require a data protection impact assessment:

- Systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- Processing on a large scale of special categories of data or of personal data relating

to criminal convictions and offences; or
- Systematic monitoring of a publicly accessible area on a large scale.

In addition to those cases, in November 2018 the Portuguese supervisory authority has issued a regulation establishing a list of kinds of processing operations subject to the requirement for a data protection impact assessment.

The data protection assessment must contain at least:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to the rights and freedoms of data subjects; and
- The measures envisaged to address the risks., including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

17. Do the laws in your jurisdiction require appointment of a data protection officer or a chief information security officer (or other person to be in charge of privacy or data protection at the organization), and what are their legal responsibilities?

Any controller or processor must appoint a data protection officer where:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- The core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

The data protection officer has at least the following tasks:

- To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to data protection laws;
- To monitor compliance with the data protection laws and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to the relevant provisions;
- To cooperate with the supervisory authority;
- To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation with such authority, where required, and to consult, where appropriate, with regard to any other matter.

In connection with such tasks, the law also specifies the following responsibilities:

- To ensure the performance of periodic and non-programmed audits;
- To create awareness of the users for the importance of timely detecting security incidents and for the need of immediately reporting to the security officer any such event; and
- To ensure the interactions with data subjects in any matters covered by the GDPR and by national laws concerning data protection.

18. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

The Portuguese laws do not explicitly require nor recommend employee training in data protection matters. Nevertheless, depending on the organisation of a controller or processor, as well as on the kinds of processing operations which they carry out, the employee training may be necessary so that such controller or processor can comply with the data protection requirements. For example, employee training and awareness may be required to enable the fulfilment of requirements of security of processing, given that any controller or processor must implement appropriate

technical and organisational measures to ensure a level of security appropriate to the risk for the rights and freedoms of natural persons presented by the processing.

19. Do the laws in your jurisdiction require businesses to provide notice to data subjects of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

Whenever controllers collect personal data, they must provide data subjects with several information relating to the intended processing, except in very few cases. Such information must include, for example: the identity and the contact details of the controller; the contact details of the data protection officer, where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the recipients or categories of recipients of the personal data, if any; the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; the existence of certain individual rights; the right to lodge a complaint with the supervisory authority.

The information to be provided and the moment when it must be provided vary according to whether the personal data are collected from the data subject or from a third party. If the personal data are collected from the data subject, the controller must provide information at the time when personal data are obtained; if the personal data are not collected from the data subject, but from a third party, the controller must provide the information in a short term, as defined by GDPR, but at the latest within one month after the controller has obtained the data.

If later on the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller must also provide the data subject with information on that new purpose and other relevant information prior to that processing.

The law does not specify formats or modalities for the provision of information. However, the controllers must take appropriate measures to provide it in a concise, transparent, intelligible and easily accessible form and using clear and plain language, especially where children are the intended recipients of the notice.

Moreover, the information must be provided in writing or by other means, including, where appropriate, by electronic means. It may only be provided orally if the data subject so requests, provided that the identity of the data subject is proven by other means.

20. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data, and, if so, what are they? (For example, are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

The law makes a distinction between controllers and processors.

The «controller» is defined by law as a 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. The «processor» is defined by law as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The controllers and the processors have direct obligations under the law. Controllers must comply with and demonstrate compliance with all the data protection principles, as well as with other requirements and are also responsible for the compliance of their processors. Processors have also specific obligations of their own under the law and may be held liable for damages caused to any person for the breach of such obligations. However, the obligations of the processors are more limited than those of the controllers.

21. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII, or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

The appointment of processors for the processing of personal data on behalf of controllers and the contracts which govern such processing are subject to specific requirements.

Before hiring a processor, the controller must ensure that the processor provides 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 subjects.

The contract between the controller and processor must be in writing, binding on the processor with regard to the controller and set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data to be processed, the categories of data subjects and the obligations and rights of the controller.

The contract must also stipulate various obligations on the processor, for example that the processor: may only process personal data on documented instructions from the controller; shall not engage another processor without authorization of the controller and respects specific conditions for that purpose; shall assist the controller in ensuring compliance with several obligations imposed on the controller; takes measures adequate to ensure the requirements of security of processing; and, at the choice of the controller, deletes or returns all personal data to the controller after the end of the provision of services.

22. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including the use of tracking technologies such as cookies. How are these terms defined, and what restrictions are imposed, if any?

«Monitoring» itself is not defined in Portuguese data protection laws, although it is referred in connection with operations of processing of personal data for different purposes.

«Profiling» is defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

«Automated individual decision-making» is referred as a form of making a decision based solely on automated processing, without human involvement, which produces legal effects concerning the data subject or similarly significantly affects the data subject (also under the GDPR).The data subject has the right not to be subject to such decision based solely on automated processing, including profiling, unless the data subject has given explicit consent for that purpose, or the decision is necessary to enter into or to perform a contract between the data subject and a controller or is authorized by law.

Even though the decision is necessary for the entering into or the performance of a contract between the data subject and the controller or is authorized by law, the controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to challenge the decision.

Decisions as such cannot be based on special categories of personal data, unless the individual has given explicit consent for that purpose or the processing is necessary for reasons of substantial public interest, on the basis of a law which respects some requirements stated by the GDPR, and the controller applies suitable measures to safeguard the data subject's rights and legitimate interests.

Furthermore, in the event a given processing implies automated decision-making, including profiling, the controller must provide the data subject with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The term «cookies» is not used in the Portuguese law. Nevertheless, under the law on processing of personal data and protection of privacy in the electronic communications sector (Law no. 41/2004), the storing of information or the access to information stored in the terminal equipment of a subscriber or user is only allowed if the subscriber or user concerned has given consent, save the technical storage or access which is necessary for the sole purpose of carrying out the transmission of a communication over an electronic communications network or is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

23. Please describe any restrictions on targeted advertising and cross-contextual behavioral advertising. How are these terms or related terms defined?

The Portuguese law does not specifically address the target advertising or the cross-contextual behavioural advertising. Nevertheless, the activities of processing of personal data which it may imply are subject to data protection laws, for instance profiling and sending of unsolicited communications for purposes of direct marketing.

24. Please describe any laws in your jurisdiction addressing the sale of personal data. How is "sale" or related terms defined, and what restrictions are imposed, if any?

The Portuguese law does not specifically address the sale of personal data. However, to the extent such sale may consist of or implies disclosure or making available personal data, it must comply with all the data protection principles, as well as with other requirements of GDPR and remaining data protection laws, for example the requirement of a legal ground (data subject's consent or other ground that may be adequate).

25. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

In Portugal, there are two laws addressing telephone calls, text messaging and email communication for the purposes of direct marketing:

- Law no. 41/2004, of 18 August 2004, as last amended by Law no. 16/2022, of 16 August 2022, concerning the processing of personal data and the protection of privacy in the electronic communications sector (transposes into the Portuguese law the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002), which includes specific provisions on unsolicited communications for the purposes of direct marketing;
- Law no. 6/99, of 27 January 1999, which governs advertising by post, direct distribution, telephone and fax.

In the framework of the law concerning the processing of personal data and the protection of privacy in the electronic communications sector, «communication» means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. «Electronic mail» means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient.

Under such law, the sending of unsolicited electronic communications for direct marketing purposes, in particular through the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail, including SMS, EMS and MMS messages and other similar, is subject to the prior and explicit consent of the subscriber to the electronic communications services who is a natural person or of the user. Nevertheless, the aforementioned requirement is softened in the context of an existing customer relationship: if a supplier obtains from its customers their electronic contact details, in the context of the sale of a product or a service, the supplier may use these electronic contact details for direct marketing of its own similar products or services, provided that customers are given the opportunity to object to such use at the time of the collection of their contact details and after that on the occasion of each message, in case the customer has not initially refused such use.

However, to the extent that the telephone calls, text messaging and email communications for the purposes of direct marketing are addressed to natural persons or imply any other processing of personal data, they are also subject to the requirements established by the general data protection laws, namely by GDPR and Law no. 58/2019.

The entities that promote the sending of electronic communications for direct marketing purposes must keep an up-to-date list of individuals who have consented to receive said communications, as well as a list of clients who have not objected to it (in the cases where the requirement of consent softened).

The regime may be different if the unsolicited electronic communications for direct marketing purposes are addressed to subscribers who are legal entities (in particular if it does not imply processing of personal data).

In any case, the law prohibits the sending of electronic mail for direct marketing purposes which disguise or conceal the identity of the person on whose behalf the communication is made and without providing a valid means of contact to which the recipient may send a request to cease such communications.

26. Please describe any laws in your jurisdiction addressing biometrics such as facial recognition. How are these terms defined, and what restrictions are imposed, if any?

«Biometric data» is defined under the GDPR as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.

The processing of biometric data for the purpose of uniquely identifying a natural person is subject to the regime of processing of special categories of personal data, which prohibits such processing unless in exceptional cases more restrictive than those which may constitute legal grounds for the processing of personal data in general.

The processing of employees' biometric data is permitted for the purposes of control of attendance and access to employer's premises, under certain conditions.

27. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

A transfer of personal data to countries outside the European Union or the European Economic Area, or to an international organization, is subject to specific conditions, in addition to other data protection requirements which may apply to such transfer as processing of personal data.

Such transfer is permitted if the European Commission has decided that the country, territory or one or more specified sectors within that country, or the international organization in question, ensures an adequate level of protection. In the absence of such decision, a controller or processor may transfer personal data to the country or an international organization if they have provided appropriate safeguards. These safeguards may for example consist of standard contractual clauses adopted by the European Commission for the purpose, binding corporate rules within a group of enterprises or undertakings that are part of a joint economic activity, codes of conduct or certification mechanisms together with binding and enforceable commitments of the controller or processor in the country of destination.

In the absence of an adequacy decision or of appropriate safeguards, a transfer can still take place in few specific situations, for example:

- The data subject has explicitly consented to 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 to perform a contract between the data subject and the controller or to implement pre-contractual measures taken at the data subject's request;
- The transfer is necessary to conclude or perform 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 to establish, exercise or defend legal claims;
- The transfer is necessary 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.

28. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

The controllers and processors must comply with a general obligation to implement appropriate technical and organizational measures to ensure a level of security of the processing appropriate to the risks inherent in such processing and, for that purpose, they must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The GDPR provides examples of measures which may be applied *inter alia* as appropriate, such as:

- 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, accessing and evaluating the effectiveness of technical and organizational measures for ensuring the

security of processing.

In assessing the appropriate level of security, controllers and processors must take into account, in particular, risks from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The controller and processor must also take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller unless such person is required to do so by law.

29. Do the data protection, privacy and cybersecurity laws in your jurisdiction address security breaches, and, if so, how does the law define “security breach”?

The data protection laws, in particular the GDPR and the law concerning the processing of personal data and the protection of privacy in the electronic communications sector (Law no. 41/2004), use the term «personal data breach», which 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 law which sets out the regime of security in the cyberspace (Law no. 46/2018, of 13 August 2018) uses the term «incident», as an event having a real adverse effect on the security of networks and information systems.

30. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

The Portuguese laws impose specific security requirements on certain sectors and entities.

For example, the legal framework of cyberspace security imposes security requirements on certain public bodies and entities, operators of critical infrastructures, operators of essential services, digital service providers and entities which use networks and information systems.

The laws on electronic communications and on the processing of personal data and protection of privacy in the electronic communications sector set out security requirements for providers of publicly available electronic communications networks and of publicly available electronic communications services.

Providers of electronic trust services are also subject to specific security requirements.

31. Under what circumstances must a business report security breaches to regulators, to individuals or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator, and what is the typical custom or practice in your jurisdiction?

In the case of any personal data breach, the controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, in the terms specified by GDPR. If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall also communicate the personal data breach to the data subjects without undue delay.

In the context of electronic communications, the providers of publicly available electronic communications services must notify any personal data breaches to the supervisory authority and, depending on the seriousness of the risks presented, to the subscribers or users of the services.

The entities subject to the legal regime of cyberspace security must also notify, in certain terms, incidents with serious impact on the safety of their networks and information systems or on the continuity or provision of their services, depending on the kind of entity, to a specific authority: Centro Nacional de Cibersegurança.

The providers of publicly available electronic communications networks and of publicly available electronic communications services must also notify, in certain terms, breaches of security or losses of integrity with significant impact on the functioning of networks and services to the respective national regulatory authority: Autoridade Nacional de Comunicações («ANACOM»).

32. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cybercrime, such as the

payment of ransoms in ransomware attacks?

The law does not set out a specific requirement regarding dealing with the criminal offences of the cybercrime kind, such as the payment of ransoms in ransomware attacks. There are however legal requirements regarding dealing with cybersecurity incidents, which may relate to such offenses.

There is also guidance in Portugal about dealing with cybersecurity threats and attacks, including ransomware attacks and payment of ransoms in ransomware attacks (which is not recommended). Such guidance is published by the national authority in matters of cybersecurity Centro Nacional de Cibersegurança and also by the European Union Agency for Cybersecurity («ENISA»).

33. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

In Portugal there is an authority with the specific competence of cybersecurity regulator: Centro Nacional de Cibersegurança.

Centro Nacional de Cibersegurança is a governmental body which tasks include, among others, to be the single point of contact for international cooperation, without prejudice to the competence of the criminal police related to international cooperation in criminal matters, and to cooperate with other national bodies responsible for cyberespionage, cyber-defence, cybercrime and cyberterrorism and also with the data protection authority in the event of incidents which have caused personal data breaches. It has also the power to issue instructions on cybersecurity.

Centro Nacional de Cibersegurança is also competent to monitor compliance with and to apply sanctions for infractions to the law on cyberspace security.

34. Do the laws in your jurisdiction provide individual data privacy rights such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

The laws in Portugal provide individual data protection rights. The data subjects are granted the following specific rights related to their personal data:

- Right to be informed;
- Right of access;
- Right of rectification;
- Right to erasure;
- Right to restriction of processing;
- Right to data portability;
- Right to object to processing;
- Right not to be subject to automated individual decisions.

Right to be informed. Whenever controllers collect personal data for any purpose or intend later on to process such data for another purpose, they must provide data subjects with several details of the intended processing, except in very few cases.

Right of access. The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and to be informed of several details, for example the purposes of the processing, the categories of personal data concerned, the recipients or categories to whom the personal data have been or will be disclosed.

Right to rectification. Enables data subject to obtain from the controller the rectification of inaccurate personal data and also, depending on the case, the completion of incomplete personal data.

Right to erasure («right to be forgotten»). The data subject may obtain from the controller the erasure of personal data in some cases, for example where the personal data are no longer necessary in relation to the purposes for which they were processed, the data subject withdraws his or her consent and there is no other legal ground for the processing, or the personal data have been unlawfully processed. Nevertheless, there are a number of exceptions to this right, e.g. where the processing is necessary for reasons of freedom of expression and information or to establish, exercise or defend legal claims.

Right to restriction of processing. In some cases, the data subject may demand the processing of personal data to be restricted, for example where the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data, or the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead. When the processing has been restricted, the personal data retained may only be processed with the data subject's consent or for very few purposes.

Right to data portability. The data subject has a right to receive the personal data which the data subject has

provided to a controller, in a structured, commonly used and machine-readable format and also the right to transmit those data to another controller. This right may only apply when the processing of personal data is based on the data subject's consent or on the necessity for the performance of a contract with the data subject and the processing is carried out by automated means.

Right to object to processing. When the processing is for purposes of performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for purposes of the legitimate interests pursued by the controller or by a third party, the data subject may object to processing on grounds relating to the data subject's particular situation. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or the processing is necessary for the establishment, exercise or defence of legal claims. Still, where personal data are processed for direct marketing purposes, the data subject may unconditionally object to processing, including profiling related to such direct marketing, and the personal data shall no longer be processed for such purposes.

Right not to be subject to automated individual decisions. The data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject, unless the data subject has given explicit consent for that purpose, or the decision is necessary to enter into or to perform a contract between the data subject and a data controller or is authorized by law.

The data subjects may exercise their individual rights by contacting the controller and must reply to the data subjects' requests without undue delay and in any event within one month of receipt of request, save the above referred right to be informed, which must be satisfied by the controller in certain occasions without need of request. In such reply, the controller must provide information on action taken or the reasons for the delay, if there are grounds for such delay, or the reasons for not taking action and the remedies available to the data subject in that case.

The controller must provide the information and communications relating to the above-mentioned rights in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Any action of the controller to comply with the data subjects' rights is free of charge, except in the event of requests manifestly unfounded or excessive.

35. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

The data subjects may exercise their individual data protection rights through the judicial system and may also lodge a complaint with the supervisory authority, whenever they consider that such rights have been infringed.

The submission of complaints to the supervisory authority may lead this to order controllers or processors to comply with the data subjects' requests or with other measures, depending on the circumstances, and to start proceedings for infringement and consequently to impose sanctions on them.

36. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

Under express provision of the law, the data subjects may bring actions in the judicial courts against controllers or processors in the event they consider that their rights have been infringed as a result of the processing of personal data in non-compliance with the laws, or against the supervisory authority, for example for not handling complaints, as well as actions for damages suffered as result of unlawful processing personal data or other infringement to data protection laws or of acts and omissions of the supervisory authority.

37. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection, privacy and/or cybersecurity laws? Is actual damage required, or is injury of feelings sufficient?

Any person who has suffered material or non-material damage as result of an infringement of the data protection or cybersecurity laws has the right to receive compensation for the damage suffered.

38. How are data protection, privacy and cybersecurity laws enforced?

In Portugal, the enforcement of the laws governing data protection is entrusted to one public and independent

supervisory authority: Comissão Nacional de Protecção de Dados. This authority enforces the laws in particular through the exercise of its investigative and corrective powers. Such corrective powers include, *inter alia*, the power to order controllers and processors to comply with data subjects' requests to exercise their rights, to bring processing operations into compliance with the provisions of the data protection laws, to impose a temporary or definite limitation or even a ban on processing and to impose administrative fines in addition to or instead of other corrective measures.

Noncompliance with the decisions taken by the supervisory authority under its corrective powers is itself an infringement set out by law (Law no. 58/2019) and punishable with an administrative fine.

Under the law on processing of personal data and protection of privacy in the electronic communications sector (Law no. 41/2004), the supervisory authority has also a power to impose compulsory payments for delay in compliance with its decisions.

The supervisory authority has the competence to start legal proceedings for infringements to data protection laws and to impose administrative fines for such infringement. It also has a duty to report to the public prosecutor the criminal offences of which it becomes aware of by virtue of its functions, as well as to perform necessary and urgent precautionary acts to secure the means of proof.

As for the enforcement of cybersecurity laws, Centro Nacional de Cibersegurança has the power to issue cybersecurity instructions and the competence to start legal proceedings for infringements to such laws and to impose administrative fines for such infringement

However, any person may appeal to judicial courts from the decisions of the aforementioned authorities which impose administrative fines and other sanctions for infringements.

39. What is the range of sanctions (including fines and penalties) for violation of data protection, privacy and cybersecurity laws?

The range of sanctions for violation of data protection laws varies according to the kind of violation set out by such laws, which can be criminal offences or other infringements.

Criminal offences are punished with imprisonment up to four years or fines up to 480 days.

Other infringements are punished with administrative fines up to EUR 20.000.000,00 or, in case of an undertaking, 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Accessory sanctions can also be imposed together with the above referred penalties, such as temporary or definitive prohibition of processing, blocking, erasure or total or partial destruction of data. In the case of crimes or fines exceeding EUR 100.000,00, the conviction may be published.

Infringements to cybersecurity laws are punished with administrative fines up to EUR 25.000,00, if committed by a natural person, or up to EUR 50.000,00, if committed by a legal entity.

40. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

The laws specify minimum and maximum amounts of administrative fines according to the degree of seriousness of the infringements, the kind of infringer (natural person or legal entity) and, in the case of infringements to data protection laws, the size of enterprise.

Regarding the setting of the amount of the fine to be imposed in each individual case, data protection laws state several factors which the supervisory authority must take into account, such as:

- The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- The intentional or negligent character of the infringement;
- Any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- The degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them;
- Any relevant previous infringements;
- The degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects;
- The categories of the personal data affected;

- The manner in which the infringement became known to the supervisory authority, in particular whether the controller or processor notified the infringement;
- The adherence to approved codes of conduct or approved certification mechanisms;
- Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided from the infringement;
- The economic situation of the agent, in the case of a natural person, or the turnover and annual balance sheet, in the case of a legal entity;
- The continuity of the infringement;
- The size of the entity, taking into account the number of employees; and
- The nature of the services provided.

There are also guidelines on the application, setting and calculation of administrative fines under the GDPR, which were issued by the Article 29 Data Protection Working Party (independent European advisory body on data protection set up under article 29 of Directive 95/46/EC) and by the European Data Protection Board (which replaced the Article 29 Working Party) in October 2017 and May 2022 respectively.

41. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Any natural or legal person may appeal to judicial courts against legally binding decisions of the supervisory authority concerning them, for example from decisions which impose administrative fines for infringement.

42. Are there any identifiable trends in enforcement activity in your jurisdiction?

There are not particular identifiable trends in enforcement activity in Portugal. However, it is usual that whenever an individual makes a complaint to the data protection authority for infringement of individual rights such authority starts investigations which may lead to the imposition of corrective measures or legal proceedings for the imposition of fines or other sanctions.

43. Are there any proposals for reforming data protection, privacy and/or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

There is a proposal of an awaited new regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications. This proposal is since years depending on the progress of the legislative procedure of the European Union. If it is approved, it will apply directly in the member states of the European Union, as Portugal, and will change the Portuguese law concerning the processing of personal data and the protection of privacy in the electronic communications sector.

There are other proposals adopted by the European Commission for new regulations of the European Parliament and of the Council under legislative process which are also supposed to apply directly in the member states of the European Union, as Portugal, and might supplement data protection laws in Portugal. They are: the proposal for a regulation on harmonised rules on artificial intelligence («Artificial Intelligence Act») published on 21 April 2021; the proposal for a regulation on fair access to and use of data («Data Act») published on 23 February 2022; and the proposal for a regulation on the European Health Data Space published on 3 May 2022.

Regarding cybersecurity, on 15 September 2022 the European Commission published a proposal for a new regulation on horizontal cybersecurity requirements for products with digital elements, also to apply directly in Portugal, which is under legislative process.

Contributors

José Lobo Moutinho
Equity Partner
jlm@servulo.com

João Carmona Dias
Partner
jcd@servulo.com

Inês de Sá
Senior Associate
is@servulo.com

Ana Margarida Cerqueira
Trainee
amc@servulo.com