The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Portugal: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection and cyber security laws and regulations that may occur in Portugal.

This Q&A is part of the global guide to Data Protection & Cyber Security. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/practice-areas/data-protection-cyber-security/

Country Author: Coelho Ribeiro & Associados

The Legal 500

Mónica Oliveira Costa, Partner - CIPP/E

monica.costa@cralaw.com

Carolina Ribeiro Santos, Associate

carolina.santos@cralaw.com

1. **Please provide an overview of the legal framework governing privacy 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 laws enforced)?**

   The key laws governing privacy in Portugal are the following:

   a) **Portuguese Constitution** (article 35.º) – on the use of computerised data.

   b) **Regulation (EU) 2016/679 of the European Parliament and the Council, of April 27th** – the General Data Protection

Regulation applicable since 25 May of 2018 (hereinafter, the "**GDPR**").

c) **Law 67/98, of 26 October** – the Data Protection Law that implemented Directive 95/46/EC that remains in force in everything that does not contradict the GDPR and until it is revoked by the new Law (currently under discussion in Parliament) that will approve any derogations to the GDPR.

d) **Law 46/2012, of 29 August** - on the processing of personal data and protection of privacy in electronic communications that implemented the ePrivacy Directive.

e) **Law 32/2008, of 17 July** - concerning the data retention obligations applicable to publicly available electronic communications services providers (that implemented Directive 2006/24/EC which was invalidated by the CJEU in its decision of April 2014).
f) **Law 34/2013, of 16 May** - on the use of video surveillance by private security companies.

Furthermore, there are other data protection provisions in several other sectors, such as scientific research, employment, genetic information, anti-money laundering, call centers, national citizen card, and cybercrime.

Comissão Nacional de Proteção de Dados (CNPD) is the Portuguese Data Protection Authority/Regulator who enforces the Data Protection Laws.

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

   Since 25 May 2018 entities covered (natural or legal person, public authority, agency or other body that acts as a data controller or a data processor, without prejudice of a few exceptions, such as those foreseen in article 2.2 of the GDPR) by Data Protection Laws are no longer required to neither register their data processing nor apply for any authorisation to the CNPD.

3. **How do these laws define personally identifiable information (PII) versus sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?**

   Since 25 May 2018 the definition of PII is the one resulting from the GDPR, i.e., any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a

name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and the same applies to sensitive PII, known as special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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) and to the data relating to criminal convictions and offences or related security measures.

Both Portuguese Constitution and the Data Protection Law also consider as sensitive data information related to the private life of the data subject (data of a highly personal nature, such as, data linked to household and private activities). We shall wait to see how the new Data Protection Law will and on what terms address this information.

4. **Are there any restrictions on, or principles related to, the general processing of PII – for example, must a covered entity establish a legal basis for processing PII in your jurisdiction or must PII only be kept for a certain period? Please outline any such restrictions or "fair information practice principles" in**

detail?

Any processing of PII must obey to the following principles laid down mainly in articles 5 and 6 of the GDPR:

a) Lawfulness (which requires that a legal basis is established to process PII, such as, consent, performance of a contract, compliance with a legal obligation, protection of vital interests, public interest, legitimate interests, without prejudice of the Portuguese Data Protection Act introducing more specific requirements for the processing and other measures to ensure lawful and fair processing), fairness and transparency;

b) Purpose limitation, under which PII shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those principles;

c) Data minimization that demands PII to be adequate, relevant and limited to what is necessary in relation to the purposes for which such PII is processed;

d) Accuracy in order to ensure that PII is accurate and kept up to date;

e) Storage limitation, pursuant to which PII shall be kept for no longer than is necessary for the purposes for which they are processed;

f) Integrity and confidentiality to ensure PII is protected against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures;

g) Accountability in the sense that the controller is not only responsible for but also must be able to demonstrate that the processing of PII is compliant with the above principles.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of PII and, if so, are there rules relating to the form, content and administration of such consent?

It is up to the controller to decide in advance what will be the legal basis upon which the processing relies on. However, when making this decision, controllers should bear in mind Article 29 Working Party Guidelines on Consent (WP259rev.01) according to which "*if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws*

consent" as "the controller cannot swap from consent to other lawful bases". Thus, consent should be the legal basis to rely on when no other lawful bases apply.

Consent is required for direct marketing purposes, including profiling to the extent that it is related to such direct marketing. In many occasions, consent is also the lawful basis required for processing o special categories of personal data (ex.: interventional studies or clinical trials in humans, call recording, location data and biometric data outside an employment relationship).

The GDPR does not require any specific form and content nor establishes rules for consent's administration but the Portuguese Data Protection Law may introduce restrictions or special provisions in this regard particularly for processing of special categories of personal data.

Despite the above, consent must be free, specific, informed and unambiguous by means of a statement or a clear affirmative action being incumbent upon the controller to prove that the data subject has validly consented to the processing of his/her PII.
The GDPR also foresees in its article 7.2 that if consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a

manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

Furthermore, controller must ensure that data subjects can easily withdraw consent at any time.

Finally, WP259rev.01 above referred provides guidance relating to the form, content and administration of consent that controllers, in the absence of specific laws, regulations and guidelines in their jurisdiction, should have into consideration as these guidelines reflect the position of the European Data Protection Authorities and their interpretation of the GDPR provisions.

5. **Are there any circumstances where consent is required or typically used in connection with the general processing of PII and, if so, are there are rules relating to the form, content and administration of such consent?**

   Processing of sensitive PII, as defined above, is prohibited except in the cases foreseen in article 9.2 and 9.3 of the GDPR:

   a) The data subject has given explicit consent for that specific purpose;

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;

c) 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;

d) 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;

e) Processing relates to personal data which are manifestly made public by the data subject;

f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) Processing is necessary for reasons of substantial public interest;

h) 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 or pursuant to contract with a health professional;

i) 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;

j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical.The Portuguese Data Protection Law may introduce further conditions or restrictions regarding the processing of genetic data, biometric data or data concerning health.

In what concerns PII relating to criminal convictions and offences or related security measures the lawful basis for their processing shall be the law of the Members States (ex.: criminal

record, disciplinary sanctions).

In both cases, considering the nature of the PII and the risks for the data subjects, increasing attention should be paid, for example, by ensuring appropriate safeguards for the rights and freedoms of the data subjects and implementing security measures adequate to protect such PII against unauthorised or unlawful processing, accidental loss, destruction or damage.

6. **What special requirements, if any, are required for processing sensitive PII? Are there any categories of PII that are prohibited from collection?**

As foreseen in article 8 of the GDPR, where the child is below the age of 16 years and the processing of PII is related to the offer of information society services directly to him/her (except preventing or counselling services pursuant Recital 38) and is based on consent, the controller must seek consent from the holder of parental responsibility over the child.

The Portuguese Data Protection Law may establish a lower age (up to 13 years).

Furthermore, increased attention should be paid for the information to be provided to children in order to ensure it is

intelligible and clear for them.

7. **How do the laws in your jurisdiction address children's PII?**

   As foreseen in article 8 of the GDPR, where the child is below the age of 16 years and the processing of PII is related to the offer of information society services directly to him/her (except preventing or counselling services pursuant Recital 38) and is based on consent, the controller must seek consent from the holder of parental responsibility over the child.

   The Portuguese Data Protection Law may establish a lower age (up to 13 years).

   Furthermore, increased attention should be paid for the information to be provided to children in order to ensure it is intelligible and clear for them.

8. **Are owners or processors of 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.**

   In accordance with article 30 of the GDPR, Internal records of

data processing activities are mandatory – for controllers and processors – if the enterprise or organization employs at least 250 employees or, regardless the number of employees, the data processing activities are likely to result in a risk to the rights and freedoms of data subjects and is not occasional or includes special categories of data (sensitive PII) or PII relating to criminal convictions and offences.

That record shall be in writing (including electronic form) and its content varies on whether the covered entity acts as a controller or a processor.

When acting as a controller, the record shall include:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

b) the purposes of processing;

c) a description of the categories of data subjects and of the categories of personal data;

d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries

or international organizations;

e) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization;

f) where possible, the envisaged time limits for erasure of the different categories of data;

g) where possible, a general description of the technical and organizational security measures.
When acting as a processor, the record shall include:

a) the name and contact details of the processor or processors and each controller on behalf of which the processor is acting and, where applicable, the controller's and processor’s representative and the data protection officer;

b) the categories of processing carried out on behalf of each controller;

c) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization;

d) where possible, a general description of the technical and organizational security measures.

The CNPD has made available on its website forms of records of processing activities for both controllers and processors (only available in Portuguese at https://www.cnpd.pt/bin/rgpd/rgpd.htm).

Considering the accountability principal, controllers should establish internal processes and written documentation to be able to demonstrate compliance with GDPR, which may include, inter alia and as applicable:

a) Privacy policy at organizational level;
b) Privacy notices
c) Regulations to ensure accuracy of the data;
d) Data Retention Policy;
e) Regulations to ensure valid consent is obtained (including minors) and how do deal with consent withdrawal;
f) Consent forms;
g) Record of consents;
h) Documents' classification;
i) Data Subject Access Requests Protocol;
j) Data Processing Agreements;
k) Data Sharing Agreements;
l) Arrangement between joint controllers;

m) Non-disclosure agreements;
n) Data protection clauses for the several contracts in place;
o) Training on Privacy and Data Protection;
p) Internal and periodic audits;
q) Data Security Policy;
r) Security Measures Record;
s) Business Continuity Plan;
t) Data Breach Policy;
u) DPIAs Policy.

9. **Are consultations with regulators recommended or required in your jurisdiction and in what circumstances?**

   Consultations with the CNPD are required prior to processing only where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk (article 36 of the GDPR).

10. **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?**

    Under article 35 of the GDPR, carrying out a Data Protection

Impact Assessment (DPIA) is mandatory in the case of:

a) A systematic and extensive evaluation of personal aspects relating to natural persons which is 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;

b) Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences;
c) A systematic monitoring of a publicly accessible area on a large scale.

On 30 November 2018 the CNPD published its Regulation 798/2018 with the (non-exhaustive) list of the processing operations subject to the requirement for a DPIA, which includes the following:

(i) Processing resulting from the use of electronic devices that transmit, via communication networks, data concerning health;

(ii) Combination of PII or processing that combines sensitive PII or data relating to criminal convictions and offences or data of a highly personal nature;

(iii) Processing of sensitive PII or data relating to criminal convictions and offences or data of a highly personal nature where they were not obtained from the data subject, in case it is not possible or feasible to ensure the right to information;

(iv) Profiling on a large scale;

(v) Processing that allows location or behaviour tracking (employees, customers or passers-by) in order to evaluate or classify data subjects, unless the data processing is necessary for the provision of services specifically required by the data subjects;

(vi) Processing of sensitive PII or data relating to criminal convictions and offences or data of a highly personal nature for archiving purposes in the public interest, scientific research purposes or statistical purposes), unless such processing is authorized by law that foresees adequate safeguards to the data subject rights;

(vii) Processing of biometric data for unambiguous identification of the data subjects, when the later are vulnerable persons, unless such processing is authorized by law and the latter is preceded by a DPIA;

(viii) Processing of genetic data of vulnerable persons unless such processing is authorized by law and the latter is preceded by a DPIA;

(ix) Processing of sensitive PII or data relating to criminal convictions and offences or data of a highly personal nature using new technologies or new use of existing technologies.

A DPIA, pursuant article 35.7 of the GDPR, must contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects; and

d) 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 law, taking into account the rights and legitimate interests

of data subjects and other persons concerned.

Where appropriate, controllers must seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by processing operations.

Finally, Article 29 Working Party Guidelines on DPIA (WP248rev.01) provides guidance on how to carry out a DPIA that controllers, in the absence of specific laws, regulations and guidelines in their jurisdiction, should have into consideration as these guidelines reflect the position of the European Data Protection Authorities and their interpretation of the GDPR provisions.

11. **Do the laws in your jurisdiction require appointment of a data protection officer, or other person to be in charge of privacy or data protection at the organization? What are the data protection officer's legal responsibilities?**

As prescribed in article 37 of the GDPR, the controller and the processor are required to appoint a data protection officer (DPO) in any case where:

a) The processing is carried out by a public authority or body, except for courts acting in their judicial capacity

b) The core activities of the controller or the processor consist of processing operations which, by their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c) 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.

A group of undertakings may appoint a single data protection officer provided that a DPO is easily accessible from each establishment.

The DPO may be a staff member of the controller or processor or fulfil the tasks on the basis of a service contract, as long as he/she is designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks legally established.

The controller or the processor shall publish the contact details of the DPO and communicate them to the CNPD through an on-line notification form at https://www.cnpd.pt/DPO/?AspxAutoDetectCookieSupport=1. The CNPD also published FAQs regarding DPOs at https://www.cnpd.pt/bin/faqs/faqs.htm.

In case the controller or the processor are not required to appoint a DPO it is highly recommended to have other person to be in charge of data protection at the organization.

The DPO shall have at least the following tasks, as outlined in article 39 of the GDPR:

a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations;

b) to monitor compliance with GDPR, with other Union or Member State data protection provisions 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; (iii) to provide advice where requested as regards the data protection impact assessment and monitor its performance;

c) to cooperate with the supervisory authority;

d) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation and to consult, where appropriate, with regard to any other matter.

Finally, Article 29 Working Party Guidelines on DPO (WP243rev.01) provides guidance on the designation, positions and tasks of the DPO that controllers and processors, in the absence of specific laws, regulations and guidelines in their jurisdiction, should have into consideration as these guidelines reflect the position of the European Data Protection Authorities and their interpretation of the GDPR provisions.

12. **Do the laws in your jurisdiction require providing notice to individuals of the business' processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).**

Yes, under the terms and conditions foreseen in articles 12, 13 and 14 of the GDPR. Controllers are required to provide at least the following information:

a) identity and contact details of the controller and, where

applicable, its representative;

b) contact details of the DPO;

c) purpose and legal basis for the processing;

d) legitimate interests pursued by the controller or a third party when that constitutes the legal basis for the processing;

e) categories of personal data concerned (only required where the data are not obtained from the data subject)

f) recipients or categories of recipients of the personal data;

g) details of transfers to third countries and reference to the safeguards and the means to obtain a copy of them or where they have been made available;

h) period for which the personal data will be stored;

i) rights of the data subject (access, rectification, erasure, restriction on processing, objection and portability);

j) right to withdraw the consent at any time where processing is based on consent;

k) right to lodge complaint with a supervisory authority;

l) whether there is an obligation (legal or contractual) to provide the personal data and the possible consequences of failure to provide such data;

m) from which source the personal date originate, and if applicable, whether it came from publicly accessible sources (only required where the data are not obtained from the data subject);

n) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The information above shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It can be provided in writing, including electronically (on-line) or orally.

Article 29 Working Party in its Guidelines on transparency

(WP260rev.01) "*recommends that the entirety of the information addressed to data subjects should be available to them in one single place or one complete document (e.g. whether in a digital form on a website or in paper format)*" regardless the privacy layered approach to avoid information fatigue and other methods such as "push" and "pull" notices.

Finally, the Guidelines on transparency (WP260rev.01) above referred provide further guidance on what, when, where and how to provide the required information that controllers, in the absence of specific laws, regulations and guidelines in their jurisdiction, should have into consideration as these guidelines reflect the position of the European Data Protection Authorities and their interpretation of the GDPR provisions.

13. **Do the laws in your jurisdiction apply directly to service providers that process PII, or do they typically only apply through flow-down contractual requirements from the owners?**

Yes. GDPR provisions apply directly to data processors. Notwithstanding, processors shall also comply with any additional contractual provisions they have committed themselves vis-à-vis the controller, including any lawful instructions of the controller regarding the data processing.

14. **Do the laws in your jurisdiction require minimum contract terms with service providers or are there any other restrictions relating to the appointment of service providers (e.g. due diligence or privacy and security assessments)?**

GDPR in its article 28 requires the controller to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Although not mandatory, due diligence or privacy and security assessments are a good mean of ensuring the above goal.

Nevertheless, while the data processor agreement concluded between the controller and the processor, the controller should audit and inspect the processor in order to ensure the later complies with the legal and contractual obligations undertaken.

The GDPR also requires that the processing by a processor shall be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

Furthermore, it requires the following minimum contract terms

under which the service provider:

a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law to which the processor is subject (in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest)

b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) takes all measures required by the GDPR to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage;

d) shall not engage another processor without prior specific or general written authorisation of the controller (and in the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes);

e) where engages another processor for carrying out specific processing activities on behalf of the controller (i) the same data protection obligations as set out in the contract between the controller and the processor shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR and (ii) shall remain fully liable to the controller for the performance of the other processor's obligations, if the later fails to fulfil them;

f) assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;

g) assists the controller in ensuring compliance with the obligations concerning security, notification of a data breach to the supervisory authority and to the data subject, DPIAs and prior consultations to the supervisory authority, taking into account the nature of processing and the information available to the processor;

h) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies

unless Union or Member State law requires storage of the personal data;

i) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller;

j) inform the controller if, in its opinion, an instruction infringes the GDPR or other data protection Laws.

15. **Is the transfer of PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (for example, does cross-border transfer of PII require notification to or authorization form a regulator?)**

Under article 13 of the GDPR, the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

However, transfer of PII to a third country (outside the EEA) or to an international organization shall only take place if the same level of protection of the data subjects guaranteed by the GDPR

is ensured by an adequacy decision of the European Commission or the adoption of appropriate safeguards.

Up to date the European Commission has issued several adequacy decisions attesting that the following third countries ensure an adequate level of protection: Switzerland, Canada, Argentina, Guernsey, Jersey, Man Island, Faroe Island, Andorra, Israel, Uruguay, New Zeeland, United States for organizations that are certified under the Privacy Shield Framework and Japan. Transfers made under these adequacy decisions do not require any specific authorization.

In the absence of an adequacy decision, transferring personal data to a third country or an international organization shall only take place if the controller or the processor relies on one of the following safeguards:

a) Legally binding and enforceable instrument between public authorities or bodies;

b) Binding corporate rules approved by the competent Supervisory Authority;

c) Standard data protection clauses (Controller-to-Controller or Controller-to-Processor) adopted by the European Commission;

d) Standard data protection clauses adopted by the CNPD and approved by the European Commission;

e) An approved code of conduct;

f) An approved certification mechanism.

Furthermore, article 49 of the GDPR also foresees derogations for specific situations, in the absence of an adequacy decision or of the above appropriate safeguards, allowing transfers to a third country or an international organisation in the following cases:

a) 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;

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

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between

the controller and another natural or legal person;

d) the transfer is necessary for important reasons of public interest;

e) the transfer is necessary for the establishment, exercise or defence of legal claims;

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

g) the transfer is made from a register which according to the applicable law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by law for consultation are fulfilled in the particular case.

Finally, if none of the above can apply, a transfer to a third country or an international organisation may take place only if the transfer (i) is not repetitive (ii) concerns only a limited number of data subjects (iii) is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of

the data subject, and (iv) the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. However, the controller is required to inform the supervisory authority of the transfer.

16. **What security obligations are imposed on PII owners and on service providers, if any, in your jurisdiction?**

According to article 32 of the GDPR, the controller and the processor shall (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and protect the personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, including inter alia as appropriate:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity,

availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

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

In this respect and although it only applies to the public sector it is worth to mention the Resolution of the Council of Ministers no. 41/2018, March 22nd that established the minimum technical requirements applicable to networks and information systems of the Public Administration that need to be implemented until the end of September 2019.

17. **Does your jurisdiction impose requirements of data protection by design or default?**

Yes, article 25 of the GDPR imposes both requirements:

a) data protection by design by prescribing that the controller shall (taking into account the state of the art, the cost of

implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing), 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 to be compliant with the data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing; and

b) data protection by default by establishing that the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing are processed (which is applicable to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility) and that by default personal data is not made accessible without the individual's intervention to an indefinite number of natural persons.

18. **Do the laws in your jurisdiction address security breaches and, if so, how does the law define “security breach”?**

Yes, and a personal data breach is defined, pursuant article 3(12) of the GDPR, as 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.

19. **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?**

Breach notification to the Regulator (CNPD) is required by law and must be made 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 natural persons. The notification should be made through an on-line form available at https://www.cnpd.pt/DataBreach/ where controllers must provide all the information required under the GDPR.

Breach notification to individuals is required by law only where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject and should be made without undue delay, unless any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data

breach and render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize;

c) it would involve disproportionate effort, in which case, a public communication or similar measure whereby the data subjects are informed in an equally effective manner will be adequate.

Finally, Article 29 Working Party Guidelines on personal data breach notification (WP250rev.01) provides guidance on inter alia assessing the risk and high risk and cross-border breaches that controllers, in the absence of specific laws, regulations and guidelines in their jurisdiction, should have into consideration as these guidelines reflect the position of the European Data Protection Authorities and their interpretation of the GDPR provisions.

20. **Do the laws in your jurisdiction provide individual rights, such as the right to access and the right to deletion? If so, please provide a general description on what are the rights, how are**

they communicated, what exceptions exist and any other relevant details.

Data subjects are provided with the following data protection rights prescribed in articles 12 to 22 of the GDPR (regardless any restrictions that the Portuguese Data Protection Law may foresees when it is approved):

a) Information: the data subject is entitled to be provided by the controller with all the information regarding the processing of his/her data;

b) Access: the data subject is entitled to have access of the data held by the controller about him/her, receive a copy free of charge and get additional information. Notwithstanding, the use of this right shall not affect the rights and freedoms of others (including trade secrets or intellectual property);

c) Rectification: the data subject is entitled to request the controller to correct and/or complete any inaccurate data concerning him/her;

d) Erasure: the data subject is entitled to request the controller to delete personal data concerning him/her in case (i) personal data are no longer needed (ii) consent is withdrawn and there is no other legal ground for the processing (iii) the data subject

has objected to the processing (iv) the data has been unlawfully processed (v) personal data have to be erased for compliance with a legal obligation to which the controller is subject to (vi) personal data were collected in relation to the to the offer of information society services directly to a child. Notwithstanding, this right is not absolute and shall not apply if the processing is necessary for certain purposes (exercising the right of freedom of expression and information, compliance with a legal obligation to which the controller is subject, public interest in the area of public health, archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or the establishment, exercise or defence of legal claims);

e) Restriction of processing: the data subject is entitled to obtain from the controller restriction of processing if (i) the accuracy of the data is contested (ii) the processing is unlawful but the data subject does not want the data to be erased (iii) the data is no longer needed but data subject requires them for the establishment, exercise or defence of legal claims (iv) the data subject has objected and the decision is pending; with the exception of storage, the data can only be processed with consent of the data subject or for the establishment, exercise or defence of legal claims, the protection of the rights of another natural or legal person or reasons of public interest.

f) Portability: the data subject is entitled to receive the personal data provided to the controller in a structured, commonly used and machine-readable format and also to be transferred to another controller (where technically feasible) if the processing is based on consent or on a contract and is carried out by automated means.

g) Objection: the data subject is entitled to object to processing his/her data for (i) direct marketing (ii) when the processing is based on the legitimate interests of the controller and (iii) for scientific or historical research purposes or statistical purposes. However, in (ii) controller may continue the processing by demonstrating having compelling legitimate grounds that override the data subject’s interests, rights and freedoms or for the establishment, exercise or defence of legal claims. In (iii) controller may continue the processing if is necessary for the performance of a task carried out for reasons of public interest.

h) Not to be subject to automated individual decision-making, including profiling: data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, unless the decision is (i) necessary to enter or perform a contract (ii) authorised by the law to which the controller is subject (iii) based on data subject’s explicit consent.

In addition, the data subject is also entitled to lodge a complaint with the supervisory authority as well as to withdraw his/her consent at any time where processing is based on consent not to mentioned to claim compensation before the courts, in case the controller or the processor has infringed the data protection laws, for material and non-material damages suffered.

Finally, Article 29 Working Party Guidelines on data portability and on automated individual decision-making and profiling (WP242rev.01 and WP251rev.01) provides guidance on the terms and conditions under which these rights can be exercised and how controllers should conduct should requests that controllers, in the absence of specific laws, regulations and guidelines in their jurisdiction, should have into consideration as these guidelines reflect the position of the European Data Protection Authorities and their interpretation of the GDPR provisions.

21. **Are individual rights exercisable through the judicial system or enforced by a regulator or both? When exercisable through the judicial system, does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances? Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury of feelings sufficient?**

Both: individual rights are exercisable through the judicial system and enforced by the Regulator (CNPD), according to articles 77, 78 and 79 of the GDPR.

Any person who has suffered material or non-material damage as a result of an infringement of data protection legislation has the right to an effective judicial remedy against a controller or a processor (expressed private right of action) and receive compensation from the controller or processor for the damage suffered (actual damage and injury of feelings) pursuant article 82.1 of the GDPR.

In turn, the controller involved in processing is liable for the damage caused by processing which infringes data protection legislation and the processor is liable for the damage caused by processing only where it has not complied with obligations of data protection legislation, specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller, as prescribed in article 82.2 of the GDPR.

22. **How are the laws governing privacy and data protection enforced? What is the range of fines and penalties for violation of these laws? Can PII owners appeal to the courts against orders of the regulators?**

Laws governing privacy and data protection are enforced by the CNPD.

The GDPR in its article 83 sets out two tiers of maximum thresholds for fines depending on the obligations breached:

a) Up to € 10.000.000 or, in case of an undertaking, up to 2% of the total annual worldwide turnover of the preceding financial year, whichever is higher;

b) Up to € 20.000.000 or, in case of an undertaking, up to 4% of the total annual worldwide turnover of the preceding financial year, whichever is higher.

In accordance with the Data Protection Law that implemented Directive 95/46/EC and is still in force in everything that does not contradict the GDPR and until the new Data Protection Law is approved, criminal offences are punished with imprisonment up to 1 year or a penalty of up to 240 days depending on the offence (and in certain circumstances these thresholds can increase up to 100%).

In addition to the above fines and penalties, other sanctions can be ordered, such as the temporary or definitive prohibition of the processing, blocking, erasure and total or partial destruction

of the personal data as well as the advertisement of the conviction.

Both controllers and processors can appeal to the courts against orders and decisions of the Regulator (CNPD) and the same applies to data subjects when the CNPD does not handle a complaint or does not inform the data subject within 3 months on the progress or outcome of the complaint lodged.

Finally, Article 29 Working Party Guidelines on the application and setting of administrative fines (WP253), in the absence of specific laws, regulations and guidelines in their jurisdiction, could be useful to controllers and processors to better understand the criteria and assessments that the supervisory authority will follow when enforcing the law as these guidelines reflect the position of the European Data Protection Authorities and their interpretation of the GDPR provisions.

23. **Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.**

The Portuguese Data Protection Law that will accommodate the GDPR in Portugal may include derogations, exclusions and limitations other than those provided in the GDPR but up to

date its content is not known as the first version of the draft Law was not approved and since almost a year ago it is under discussion in the Parliament

24. **Please describe any restrictions on monitoring 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?**

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 (article 4 (4) of the GDPR). Please refer to answers 5 and 20 above regarding restrictions applicable to it.

In what concerns to cookies, Law 46/2012, on the processing of personal data and protection of privacy in electronic communications, establishes that storing of information, or gaining of access to information already stored, in the terminal equipment of a subscriber or user shall only be allowed with prior consent and as long as clear and comprehensive information (in accordance with the Data Protection Laws has been provided) including inter alia, about the purposes of the

processing, unless such storage or access is required for:

a) the sole purpose of carrying out the transmission of a communication over an electronic communications network;

b) the provision of a service explicitly requested by the subscriber or user.

In the absence of guidelines from the CNPD regarding cookies, controllers should take in consideration the Working Document 2/2013 Article 29 Working Party which provides guidance on obtaining consent for cookies as these guidelines reflect the position of the European Data Protection Authorities and their interpretation of the GDPR provisions at least until the new ePrivacy Regulation is approved and enters in force.

25. **Please describe any laws addressing email communication or direct marketing?**

Law 46/2012 on the processing of personal data and protection of privacy in electronic communications that implemented the ePrivacy Directive rules the sending of unsolicited communications for direct marketing purposes, through the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile

machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) as well as through other kinds of similar applications.

Pursuant this Law, sending email for marketing purposes is subject to the prior and explicit consent of the recipient (whenever the recipient is a natural person) except for those recipients with whom the sender has, in the past, sold goods or provided services similar to the ones intended to be promoted and provided that:

a) By the time of the sale or the provision of services the recipients' contacts were collected, and they were informed, in accordance with the Data Protection Laws, that their contacts would be used for marketing purposes; and

b) At that time as well as in each subsequent communication, they were given the opportunity to opt-out, free of charge and in an easy manner.

Regardless the above, Companies that intend to send e-mail marketing to natural persons are required to keep, on their own or through representative bodies, an up-to-date list of the natural persons that consented to receive this type of

communications, as well as of those who did not opt-out afterwards.

Sending e-mail for marketing purposes to legal persons is allowed until they opt-out or they register themselves in a National Opt-Out List for Legal entities. Companies that intend to send e-mail marketing to legal persons are required to consult this List on a monthly basis at https://www.consumidor.gov.pt/ficheiros-audio/lista-de-pessoas-coletivas-para-nao-rececao-de-comunicacao-nao-solicitadas-marketing-direto.aspx.

Moreover, it is not allowed sending electronic mail for marketing purposes which, disguise or conceal the identity of the sender on whose behalf the communication is made, without providing a valid address to which the recipient may opt-out or encourage recipients to visit websites which do not comply with these rules.