Portugal

*Tomás Vaz Pinto, João Alfredo Afonso, and Vasco Stilwell d'Andrade**

---

*Tomás Vaz Pinto joined the firm of Morais Leitão, Galvão Teles, Soares da Silva & Associados, Sociedade de Advogados, R.L (www.mlgts.pt), in 1994. He became a Partner in 2006. He is currently working with the corporate and commercial team. He is highly experienced in the areas of M&A and has been involved in several high level transactions, both at a domestic and international level. Tomás Vaz Pinto is also an expert on private equity and assists various clients in this sector. He is currently the one responsible in the firm for the non-litigation practice of all intellectual property matters, dealing notably with copyrights, trademarks, licensing, software, data protection and related issues.

João Alfredo Afonso joined the firm in 1998. He is currently working with the corporate and commercial team. João has handled mergers, acquisitions and sales of companies of varying sorts on behalf of domestic and foreign clients, as well as assisting several clients in setting up their telecommunications activities in Portugal and running business activities through the Internet. He was involved in the corporate restructuring of a major consulting company on TMT matters, in the context of its worldwide restructuring, and in the structuring and execution of a major write-off operation of a wireless communications company in Portugal. João also participated in one of the first IPOs of a Portuguese company (in the media area). He advises several Internet companies, namely on gambling activities and financial services areas. Concerning data protection issues, João assists clients in getting the required registrations and/authorizations from the Portuguese Data Protection Commission for the processing and transferring of personal data. He focuses in particular in the transfer of data from Portugal to other countries. He also assists companies whose core business involves the provision of software related services, notably in the preparation and negotiation of license agreements.

Vasco Stilwell d'Andrade joined the firm in September 2008. He is currently working with the corporate and commercial team. Prior to joining the firm Vasco worked as an IP consultant for several law and patent attorney firms. He has also interned at the Portuguese Patent and Trademark Office (PTO) and has obtained certification from the World Intellectual Property Organization (WIPO) and Federation International des Conseils en Propriété Industrielle (FICPI). He currently works mainly in the Intellectual Property field, namely in protection strategy and implementation, licensing, assignments, valuation and litigation, occasionally assisting in litigation matters involving trademarks, patents and copyright.

1. Introduction

As a Member State of the European Union, Portugal has implemented the EU Data Protection Directive,[1] which it effectively did on the 27th of October of 1998 with the entry into force of Lei da Protecão de Dados Pessoais (Personal Data Protection Law, hereinafter PDPL).[2] The enactment of the PDPL was preceded by the 4th Amendment to the Constitution of the Portuguese Republic which had, as one of its main purposes, the introduction of a new drafting for Article 35 which specifically addresses Portuguese citizens' rights regarding the processing and access of personal data.

With the amendment of Article 35 of the Constitution, the existence of an independent administrative authority to oversee the protection of personal data was also set forth in the constitutional law for the first time in Portuguese history. One of the main objectives of the PDPL was to implement that constitutional entity known as the Commissão Nacional de Protecão de Dados (National Commission for the Protection of Data, hereinafter CNPD). The purpose of CNPD, which follows a previous similar institution,[3] is twofold: to monitor the application of the law related to personal data protection by issuing recommendations and to provide authorizations for particular requests and, secondly, to regulate and enforce the law on data protection.[4] Despite the PDPL having come into effect in 1998, it was not only until 2004 with the approval of Law No. 43/2004 of August 24th that CNPD came fully into operation in its current form.

In substantive terms, the PDPL is applicable to the processing of personal data by wholly or partially automated means, and to the processing of personal data contained in or for manual files in a manner other than by automatic means. With regards to geographic scope, the PDPL regulates the processing of personal data performed by a data

---

[1]Directive 95/46/EC of the European Parliament and of the Council of the 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data.

[2]The PDPL repealed Laws No. 10/91 of April 29th and No. 28/94 of August 29th which had, up to that point, regulated these matters.

[3]The predecessor of CNPD was named CNPDI (Comissão Nacional de Protecão de Dados Informatizados) which had a more limited scope of operation.

[4]Under the PDPL (see Article 22, paragraph 2), CNPD should also be consulted in relation to any national or international legal diplomas that address data processing matters.

controller[5] established in Portuguese territory or in locations in which Portuguese law is applied due to international law. The PDPL is also applicable when the data controller is not established in the European Union but resorts to automated (or other) means located in Portuguese territory, except if these means are used exclusively for transferring data through the EU zone.

The present chapter will seek to provide a brief outline of Portuguese law surrounding the international transfer of personal data and other practical notes that have resulted from the CNPD's resolutions, recommendations and clarifications.

2. Personal Data under Portuguese Law

The definition of the term "personal data" given by the PDPL goes slightly beyond that provided in the EU Data Protection Directive. Under Portuguese law, personal data is considered any information, whatever its nature and irrespective of its format, including sound and image, related to an identified or identifiable natural[6] person (hereinafter data subject).

The term "identifiable" is, without a doubt, of the utmost importance for the definition of personal data. Following the lead of the EU Data Protection Directive, the PDPL also states that an identifiable person is one that can be directly or indirectly identified, namely by referring to an identification number or one or more specific elements of his/her physical, physiological, mental, economical, cultural or social identity.[7] In addition to this it is necessary to factor in case law[8] and scholarly work surrounding this theme so as to have a clearer idea of how the term personal data would be

---

[5]The PDPL defines a data controller as a natural or legal person, a public authority, the branch or any other entity that, individually or jointly, determines the purposes and the means of processing personal data; whenever these purposes and processing means are determined by legal norms or regulations, the ability to process personal data must be mentioned in the organizational and operational law or the legal statutes setting up the controller.

[6]The CNPD has clarified that despite self-employed professionals being considered equivalent to corporate entities for many legal purposes, their personal data is protected by the PDPL since under this diploma they are considered natural persons.

[7]Article 3, paragraph a of the PDPL.

[8]In Decision C-101-01 of November 6th, 2003, the ECJ had the opportunity of addressing the definition of "personal data" considering that it encompasses, without a doubt, the name of a person, in addition to his/

understood by a Portuguese court of law. In Portugal, some discussion has centered on the necessity of applying the principle of reasonableness so as to better qualify the term "identifiable". Legal commentators have looked, in particular, to Consideration No. 26 of the EU Data Protection Directive which states that "to determine whether a person is identifiable, account should be taken of all the means likely reasonable to be used either by the data controller or by any other person to identify the said person."

Pursuant to the above definition, personal data may constitute a great myriad of things under Portuguese law. An exact list of what is considered personal data does not exist and there is not a relevant amount of case law or CNPD decisions that can help in narrowing down the scope of the definition. As to specific issues such as whether a computer IP address or a car license plate would constitute personal data, it is our belief that under Portuguese law the answer would depend heavily on the reasonability factor. In other words, it would all depend on whether such information could lead, under normal circumstances and a reasonable level of effort, to the identification of the data subject linked to that information. There have been, nevertheless, situations where the CNPD have already considered IP addresses as constituting personal data.

3. Personal Data Processing Rules

According to the PDPL, the general rule is that personal data may only be processed if the data subject has unambiguously given his/her consent and the CNPD has been previously notified. In other words, by default, the data subject must expressly give his/her consent in a positive manner (e.g., by ticking the appropriate box agreeing to the processing) and not in the negative, whereby if nothing is said to the contrary, one presumes consent. Furthermore, it should be noted that consent can be withdrawn at any time and, in addition, the data collected and processed can be consulted, amended and deleted at the data subject's discretion.

Five exceptions to the above rule are nevertheless established in the PDPL, said exceptions following very closely the equivalent provisions contained in the EU Data Protection Directive.[9]

The exceptions are:

---

her telephone contact or information related to his/her work conditions and hobbies.

[9]See Article 7 of the EU Data Protection Directive.

(a) Processing is necessary for the performance of a contract or contracts to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into contract or issuing a declaration;
(b) Processing is necessary for compliance with a legal obligation to which the data controller is subject; or
(c) Processing is necessary in order to protect the vital interests of the data subject, if he/her is physically or legally incapable of providing consent;
(d) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the data controller or in a third party to whom the data are disclosed;
(e) Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.[10]

The PDPL also provides for the possibility of certain personal data processing activities being exempt from prior notification to the CNPD, namely when such exemption is aimed at improving speed, efficiency and resources and does not put into question the data subject's rights and freedoms.[11] The CNPD has decided to exempt from notification the following specific data processing: (i) the processing of wages, income and benefits of employees and staff; (ii) the management of library and archive users; (iii) invoicing and management of contacts with clients, suppliers and service providers; (iv) administrative management of staff, employees and service providers; (v) entry and exit of persons in buildings; and (vi) collection of contributions to associations and the contacts of the associates.[12]

Notwithstanding these exemptions, data controllers maintain certain obligations, namely to process the personal data within the limits established by the CNPD in each specific case of exemption, supply the data subject with the information foreseen in the PDPL whenever it is requested,

---

[10]See Article 20, paragraph 1 of the PDPL.

[11]See Article 27, paragraph 2 of the PDPL.

[12]Published in the Diário da República (official state bulletin) no. 22, II series of December 27, 2000 in Resolution 60/2000.

and provide the data subject with the right to access, amend, oppose and delete the data. Furthermore, the data controller has the duty to comply with the principles of loyalty, legality, legitimacy and proportionality in the processing of the data.

Processing sensitive personal data, such as philosophical or political convictions, party or union membership, religious faith, private life, racial or ethnic origin and data regarding health, sexual life and genetic information, is strictly forbidden bar a few narrow exceptions duly regulated in the PDPL.[13] Likewise, creating or storing files on criminal suspects or other criminal activities must be limited to the minimum that is necessary to prevent further crime and can only be stored and processed by specific public entities legally sanctioned to do so. Regardless of the specific grounds that may justify the application of an exception, the processing of sensitive personal data is always subject to a prior case-by-case assessment and authorization from the CNPD, which will ultimately evaluate whether the grounds invoked are admissible. For example, data subjects' consent may not always be admitted as a sufficient ground notably when such consent is obtained in circumstances where the data subject is deemed as not having enough freedom to decide (e.g., an employee within the context of an employment relationship).

4. Cross-Border Flows of Personal Data

4.1. General Considerations

4.1.1. What constitutes a "transfer" under the PDPL?

No specific definition of cross-border transfer, access or disclosure of personal data is provided by the PDPL, leading one to believe that the Portuguese legislator considered these terms sufficiently self-explanatory—in other words, that an international transfer encompasses the providing of personal data to another entity that is not generally subject to the Portuguese State's jurisdiction. The CNPD has, likewise, not yet felt the need to come forward and provide an official interpretation or clarification of the matter.

Despite there being no case law or official position, the CNPD has informally stated that permitting the access and disclosure of personal data to others in another country via the intranet of a company falls within the understanding of a cross-border "transfer" and therefore the rules discussed below will apply.

---

[13] Exceptions foreseen in Article 7 of the PDPL.

4.1.2. Data Subject's Rights

A key characteristic of personal data processing in Portugal is that, in principle, prior consent must be obtained from the data subject. The same principle applies to international personal data transfers. Although, under the PDPL, the data subject is not required to authorize every individual international transfer, consent must have been granted at some point in the past and concrete information must have been given as to the eventual recipients of the personal data. Alongside this obligation, it is also mandatory that the data subject be informed of his/her other rights such as the ability to access and amend the data abroad. This mandatory information may only be withheld in exceptional cases sanctioned by law or the CNPD.

4.1.3. The CNPD's Supervisory Powers

Under the PDPL, it is up to the CNPD to control cross-border flows of personal data out of Portugal. As we will discuss below, cross-border flows are free (in the sense that they have no different treatment from the ones applying to the internal flows of personal data) within EU member states but restricted out of the EU area, in particular to countries deemed not to provide adequate protection. In order to proceed with the transfers in the latter situation, the general rule is that authorization must be obtained from the CNPD.

The CNPD does not have a pre-established list of these states that do not provide adequate protection since it acts on a case-by-case basis upon consultation. However, for this purpose, the CNPD coordinates with the European Commission, which also issues decisions regarding the recognition of extra-EU States as providing adequate or inadequate protection.[14] In order to avoid the duplication of work, in November 2004, the CNPD acknowledged that, in addition to sending national decisions on this matter to the European Commission, something already set forth in the PDPL, it would also automatically accept the European Commission's decisions involving this matter.[15] In other words, there is today a bilateral and permanent exchange of information in

[14]According to the latest information, the following territories have been found to provide adequate protection for personal data by the European Commission: Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Jersey, and Switzerland.

[15]Interpretive Resolution regarding Articles 19 and 20 of Law No. 67/98, approved by the CNPD in plenary session of 29th of November, 2004.

place between Portugal and the European Commission involving the adequacy of third party countries.

It is also worth mentioning that, in parallel to this, there are some international treaties that have come to set certain standards in relation to data protection. For example, the signatories of the Council of Europe's Convention for the Protection of Persons Relatively to the Automatic Processing of Personal Nature Data (the so-called "Convention 108") and the co-related Protocol (CETS No. 181) are considered to provide an adequate protection by the CNPD. Additionally, as will be discussed below, the EU also has a treaty with the US aimed at regulating this matter.

Given that the PDPL distinguishes between personal data transfers between EU member-States[16] and non-EU member states,[17] the following section will discuss the differences between the two systems.

4.2. Transfers from Portugal to other EU Member States

Under the terms of the PDPL, "the flow of personal data is free amongst European Union member States, notwithstanding that laid down in fiscal and customs community acts."[18]

The manner in which this legal norm has been drafted may lead one to assume that there are no restrictions involved in the transfer of personal data in between Portugal and other EU member states. The truth, however, is that although these transfers do not require CNPD authorization, this administrative authority must nevertheless be notified.

In addition to the mandatory notification, the CNPD may also request from the recipient proof that the latter is entitled to receive the personal data.

The information that is necessary for said notification will be dealt with further in Part 5.1.

4.3. Transfers from Portugal to Third Countries

Contrary to the situation described in Part 4.2, the general rule for the transfer of personal data from Portugal to a non-EU state is that it is restricted. However, not all third countries are the same and the PDPL takes this into consideration by dividing the latter into those that have been considered to provide an adequate level of protection

[16]See Article 18 of the PDPL.

[17]See Article 19 of the PDPL.

[18]Article 18 of the PDPL.

and those that do not. Whereas for the latter group, personal data can only be transferred under some strict conditions (as we will discuss further below), the restrictions for transfers to the former are as lax as for other EU members.

Under the PDPL, the adequacy of the level of protection afforded by a State that does not belong to the EU is assessed in light of all the circumstances that surround the transfer operation, notably the nature of the data, the purpose and duration of the processing, the countries of origin and final destination, general or sect oral legal rules in force in the State in question, as well as the professional rules and the privacy measures that are respected in that State.[19] As seen in Part 4.1.3, international agreements can also be entered into for this purpose.

4.3.1. Transfers from Portugal to Third Countries with Inadequate Protection

When a State does not provide adequate protection, the rule is that personal data may not be transferred to entities established in that State. However, even in this situation, exceptions can be made and the transfer of personal data can be authorized by the CNPD under certain circumstances.

Firstly, the transfer of personal data may be authorized by the CNPD when the data subject has *unambiguously* consented to that cross-border transfer. The unambiguous nature of the consent is the cornerstone to this point. There must be an explicit sign on the part of the data subject that he/she agrees to allow his/her personal data to be sent to a jurisdiction, which does not foresee the level of data protection rights that exist in the EU. It is for this reason that under Portuguese law, consent must be "opt-in" and not "opt-out". It is also for this reason that the consent should be in writing and preferably signed.

Although the unambiguous consent is vital, there are five situations that, in accordance with the CNPD's interpretive resolution, do not require any prior control by the latter. The exceptions are:

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

[19] See Article 19 No. 2 of the PDPL.

performance of a contract concluded in the interest of the data subject between the data controller and a third party; or

c) When the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or

d) When the transfer is necessary in order to protect the vital interests of the data subject; or

e) When the transfer is made from a register which according to laws and regulations 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 legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Notwithstanding the above, the CNPD may also authorize the transfer or a set of transfers of personal data to a State that provides inadequate protection if the data controller assures that sufficient guarantees to protect the privacy and the respect and exercising of the data subject's fundamental rights and liberties through the placement of adequate contractual clauses.[20] These authorizations must follow a specific procedure before the CNPD or be in conformity with European Commission decisions.[21]

4.3.2. Transfers from Portugal to the United States of America

Decision No. 2000/520/EC issued by the European Commission on July 26th of 2000, approved the agreement signed on March 14th, 2000 between the European Union and the United States of America (USA) relative to the protection of personal data, also otherwise known as the Safe Harbor system. Pursuant to the terms of this Decision, it is recognized that the international principles of the Safe Harbor system issued by the US Department of Commerce provide an adequate level of protection for personal data transferred from the European Union.

In essence, Safe-Harbor is a self-certification system whereby companies can register themselves and declare to be compliant with a set of "Principles" and "FAQs". Naturally, given the approval of this system at the EU level, the Portuguese CNPD will also accept the transfer of personal data from Portugal to the USA if made under this framework.

---

[20] See Article 20, No. 2 of the PDPL.

[21] See Article 20, No. 3 of the PDPL.

4.4. Model Clauses

The PDPL also expressly provides for a fast-track procedure for extra-EU zone personal data flows when sample contractual clauses approved by the European Commission have been established.[22] In these cases, the CNPD has declared that its interpretation of the PDPL is such that it does not need to authorize the data flow but simply needs to verify that the model clauses have been respected. The significance of this is that even when EU Commission approved model clauses are adopted, the CNPD still has to be notified.[23]

To this date, the EU Commission has approved three decisions[24] regarding standard contractual clauses for the transfer of personal data to third countries, and is currently revising the set of model clauses involving controller-to-processor relations.

4.5. The Transfer of Personal Data Across Borders for State Security Reasons

Yet another exception to the ban on transferring personal data to third countries with inadequate protection levels exists in matters of State security. The PDPL provides for the possibility of public authorities transferring or exchanging personal information about persons should it be necessary for State security, defense, public safety and for preventing, investigating and combating criminal activities. In addition to the PDPL, other specific legal norms and international treaties to which Portugal is a signatory regulate this matter.[25] In other words, Portuguese data protection law is sufficiently flexible so as to permit the transfer of personal data that is necessary for border control (e.g., for the implementation of the Schengen Agreement and so forth).

---

[22]See Article 20, No. 5 of the PDPL.

[23]Interpretive Resolution regarding Articles 19 and 20 of Law No. 67/98, approved by the CNPD in plenary session of 29th of November, 2004.

[24]Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (2001/497/EC); Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (2002/16/EC); Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/915/EC).

[25]See Article 20, No. 6 of the PDPL.

4.6. The Transfer of Sensitive Personal Data Abroad

The international transfer of sensitive personal data is not dealt with specifically in the PDPL. Nevertheless, given the restrictions in place and prior authorization for processing these types of data, it is implicit that an international transfer of sensitive personal information may only take place if all the checks and balances are foreseen. In other words, only with prior CNPD approval may personal data of this nature be transferred abroad.

5. Legal and Technical Formalities for International Transfers

5.1. Notification of the CNPD

The CNPD must be notified of *every* crossborder personal data flow out of Portugal by an entity with an establishment in Portugal, even when the processing in itself does not require a notification procedure. Only some transfers require both a prior notification and authorization. These notifications and authorizations must be made by the data controller or its representative prior to the processing or transfer and must include the following information:[26]

a) Name and address of the data controller or its representative;
b) The purpose of the processing;
c) Description of the data subjects or their categorization and the personal data or categories to which they are related;
d) The recipients or categories of recipients to whom the data may be conveyed;
e) The entity in charge of the processing of the information, if it is not the data controller;
f) Any eventual interconnection of the personal data;
g) The duration of the storing of the personal data;
h) The manner and conditions in which the data subjects can access and correct their personal data;
i) Data transfers that are foreseen to third countries;
j) General description that enables a brief evaluation of the measures taken to guarantee the safety of the data processing.

As mentioned above, the PDPL does not apply to data

[26]Form available at the following URL: http://www.cnpd.pt/bin/legal/Formulario-geral.pdf.

controllers established in other EU member states that have no establishment in Portuguese territory and have collected personal data to process abroad. In this situation, the CNPD does not need to be notified, although the data subjects must be informed of their access and amendment rights.

In short, with regards to transfers to third countries, it will suffice to notify the CNPD when said transfers are made: (i) under a European Commission Decision on the adequacy of the data protection; (ii) standard contractual clauses approved by the EC; and (iii) when the transfers are made under one of the conditions of number 1 of article 20 of the PDPL. In all other cases, it is necessary to obtain the prior authorization of the CNPD.

5.2. Data Security in International Data Transfers

The PDPL does not specify any particular security measures that should be adopted in international data transfers. Instead, it establishes certain technical and organizational actions that data controllers must undertake to protect the collected personal data from accidental or unlawful destruction, accidental loss, modification, dissemination or unauthorized access, especially when the processing implies the transmission over a network. In general, the data controller must provide its best efforts to prevent unlawful processing of the personal data. The measures adopted must take into consideration the available technical know-how and the costs resulting in their application so as to obtain a security level that is adequate for the risks that the processing entails and the nature of the personal data to protect.

In accordance with the PDPL, in the cases where the data controller subcontracts the processing to another entity, a set of conditions must be respected such as a written contract binding both parties and the obligation of the subcontractor to comply with all the data protection terms that apply to the data controller. The contracts entered into and other binding declarations must be kept in a form that is legally valid as proof (e.g. the originals of signed documents must stored).

6. Consequences of Non-Compliance

Aside from civil liability for damages caused to those harmed by the inappropriate and illegal processing of personal data, the infringement of the legal rules contained in the PDPL can lead to either misdemeanor or criminal punishment depending on the seriousness of the offense.

Sections II and III of Chapter VI of the PDPL clearly define which actions will lead to either a misdemeanor, punishable by a fine[27] applied by the CNPD, and those that are classified as crimes and therefore merit a more severe consequence.[28]

In addition to the above consequences, in which the maximum penalty obtainable is a two years prison sentence, a court can also decide to apply a supplementary penalty which can be, for example, a temporary or permanent ban on processing personal data and the destruction of the data already processed or even the public disclosure of the illegal activities that have been perpetrated by the infringer.

7. Final Considerations

Given that its genesis can be found in the EU Data Protection Directive, it is no surprise that the PDPL is generally the same as the laws found elsewhere in the other EU states. Since 1998, a plethora of other statutes have also been enacted so as to regulate other more particular aspects of privacy protection, for example, video surveillance, electronic communication privacy and so forth. No further legislation is currently being discussed and the legal framework can be said to be consolidated in Portugal.

In Portugal, the CNPD's main activities have been in supervising and enforcing the domestic processing of personal data and little attention has been given to cross-border transfer questions, hence the lack of case law and CNPD resolutions on this matter. Particular attention has

---

[27]For misdemeanors, the PDPL establishes two separate levels of fines for different types of infringements. For less serious misdemeanors, the fine can range from €500 to €5,000 and these values may be doubled when other factors are also applicable. Graver misdemeanor penalties range from € 250 to € 2,500 for natural persons and €1,500 to € 15,000 for legal persons. These amounts can be doubled when the illegal action or inaction was subject to prior CNPD authorization (please note that the above values in Euros are approximates since the PDPL still has these values in "escudos", Portugal's pre-Euro currency.

[28]Similarly to the situation with misdemeanors, personal data related crimes under the PDPL also carry different punishments depending on the seriousness of the infringement concerned. For less serious crimes, the penalty can reach one year's imprisonment or a fine of up to 120 days. More serious crimes carry a maximum sentence of two years imprisonment or a fine of up to 240 days. Negligent breach of confidentiality is punished with a maximum sentence of six months imprisonment or a fine of up to 120 days. For the purpose of fines under criminal procedural laws, each day can vary between €1 and €498.80. It is up to the judge to weigh the financial resources of the defendant and the fairness of the penalty.

been recently given to the question of whether the consent given by an employee or service provider can be deemed to be free, given the possible consequences that may derive from an eventual refusal.

Without a doubt, the main difficulty felt in Portugal in terms of personal data protection is the delay in obtaining approval from the CNPD, when such authorizations are required (e.g., video surveillance, sensitive data, cross border transfers). The main reason behind the time that the CNPD takes to issue decisions can be found in the large scope of its mandate and the lack of human and financial resources at its disposal. The result of this combination is an inevitable backlog in pending files, which then results in uncertainty and postponed actions on the part of users.

An additional difficulty relates to the uncertainty of the applicable proceeding, i.e., whether it implies a notification or authorization notably when addressing data, which can arguably be considered as sensitive (e.g. as past billing records, information of debts log, utilities consumption information when processed by the utilities companies). When submitting an application to the CNPD, the form's field on the applicable proceeding is to be filled by the CNPD itself which sometimes results in leaving the interested party in doubt on whether it may start to process personal data immediately after presenting the application (mere notification proceeding) or if it must wait for an authorization.