FRA

Thematic Legal Study on assessment of data protection measures and relevant institutions

February 2009

Contents

Foreword

[1]. This report was written by Alexandre Sousa Pinheiro (Senior Expert), Dinamene de Freitas (Expert) and Inês Marinho (Expert).

[2]. Based on the Guidelines drawn up by FRA, the main objective of this Thematic Study is to provide country specific information and data to permit a comparative assessment of effectiveness of data protection measures and relevant institutions. The study will highlight Portuguese good practice, such as legal provisions, measures, projects and other initiatives by public authorities, which have proven to be particularly effective and/or innovative and could serve as a model.

[3]. We gratefully acknowledge the cooperation of the Comissão Nacional de Protecção de Dados (CNPD) [*National Commission of Data Protection (NCDP)*] – in particular of Ms Clara Guerra – in providing us the necessary information.

[4]. The research was carried out through a variety of websites, in particular the webpage of CNPD, and in various publications in the field of data protection.

[5]. In this area of data protection, it was possible to find statistical data that had already been produced.

[6]. The Portuguese NCDP has an extensive mandate and powers. However, the lack of personnel is limiting their full implementation.

[7]. As regards case law, decisions from different courts were selected.

Executive Summary

[8]. The Portuguese Constitution enshrines a specific article concerning data protection since 1976.

[9]. Portugal is part of the Convention 108 of the Council of Europe[1], and has adopted his first Protocol[2].

[10]. The Portuguese law (Law 67/98[3]), fully transposed Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and added some more powers to the Data Protection Authority (DPA), related to police files.

[11]. Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector was transposed by Decree-Law 7/2004 (only the matters related to *spam*)[4] and Law 41/2001[5]. The technique used for transposing the same into a law and a decree law does not affect the quality of the transposition.

[12]. The Portuguese Commission is a body composed of 7 members elected by the Parliament, the Government or the Supreme Councils of Judges and the Supreme Council of Prosecutors.

[13]. There are guarantees for the DPA members to perform an independent work during their tenure.

[14]. The NCDP has large powers in the area of data protection, including police files, and must be consulted before the approval of any legislative instrument in the field of data protection.

[15]. A major problem of the NCDP is the lack of qualified personnel in order to carry out all the powers defined by law.

[16]. The processing of personal data should be notified or authorised by NCDP (except the ones concerning personal or domestic purposes).

---

[1] http://www.cnpd.pt/bin/legis/internacional/Convencao108.htm (18/01/09).
[2] http://www.dgpj.mj.pt/sections/relacoes-internacionais/copy_of_anexos/sections/relacoes-internacionais/copy_of_anexos/protocolo-adicional-a5325/downloadFile/file/STE%20181.pdf?nocache=1200589702.07 (18/01/09)
[3] http://www.cnpd.pt/bin/legis/nacional/lei_6798.htm (18/01/09)
[4] http://www.cnpd.pt/bin/legis/nacional/DL7.2004.pdf (18/01/09)
[5] http://www.cnpd.pt/bin/legis/juris/decisoes/Lei41-2004.pdf (18/01/09)

[17]. The NCDP often apply fines to persons or companies. The Portuguese DPA is entitled to apply fines to public entities, and uses this power.

[18]. There is a complete network of sanctions resulting from the transposition of Directives 95/46 and Directive 2002/58.

[19]. The NCDP has undertaken important efforts to make people aware of their rights in the field of data protection.

[20]. In terms of good practices, the Dadus Project should be underlined. This programme aims at "giving privacy a chance" among young people. For a complete analysis of the Dadus Project see 5 – Rights Awareness.

1. Overview

[21]. The Portuguese Constitution of 1976[6] was the first to make express reference to matters of data protection (article 35º). Despite the fact that in the original text the term data protection was not used as such, it was clearly stated that citizens had the right to know all the information concerning them that was stated on computer files and were entitled to demand any necessary rectifications and updates.

[22]. It was also explicitly stated that no information on political tendencies, religious beliefs or private life could be processed, except for statistical purposes. A single identity number was forbidden.

[23]. In another article of the Constitution (33º), respect for one's good name or reputation and for one's personal and family privacy was enshrined as a right.

[24]. The Constitution also requires the law to put in place all the mechanisms necessary for protecting a person's dignity.

[25]. The first amendment to the Constitution (1982)[7], prohibited third parties from having access to computer files with data records as well as interconnections between such records. Trans-border flows of data were also prohibited, except in those cases where the law indicated otherwise.

[26]. As far as sensitive data was concerned, this concept was extended to include philosophical beliefs, and political and trade-union affiliations. According to the Constitution, the law should define what is meant by personal data for the purpose of computer records.

[27]. The second amendment to the Constitution (1989)[8] established limitations for access to personal data in the case of State secrets. The Constitution also refers to secrecy of judicial proceedings - in Portuguese *segredo de justice* – which is a phase in a criminal procedure where neither the people who are being investigated nor other entities such as the media are allowed to have access to data of the investigation.

---

[6] http://debates.parlamento.pt/r3/dac/constituicao/c_76-3.aspx (18/01/2009).
[7] http://www.cne.pt/dl/crp_lc_1982.pdf (18/01/2009).
[8] http://www.cne.pt/dl/crp_lc_1989.pdf (18/01/2009).

[28]. The amendment of 1997[9] brought the concepts of and the wording of the Constitution more in line with Directive 95/46/CE. The principle of finality was clearly stated and article 35º was extended to encompass non-computerised (i.e manual) data.

[29]. The current version of article 35º[10] is:

- To define the right to access to all computerised data and the right to require that it be corrected and updated and the purpose for which it is intended made known (paragraph 1);

- To define the concept of personal data, together with the terms and conditions applicable to its automated treatment and its linkage, transmission and use and to guarantee its protection, particularly by means of an independent administrative body (paragraph 2);

- To define the legitimacy of personal data concerning philosophical or political convictions, party or trade union affiliations, religious beliefs and private life or ethnic origins (paragraph 3);

- To forbid third-party access, save in exceptional cases provided for by law (paragraph 4);

- To define the rules applicable to cross-border data flows and the appropriate means for protecting personal data (paragraph 6);

- To define the protection of data contained in manual files (paragraph 7).

[30]. Portugal transposed Directive 95/46 as well as Directive 2002/58, by Law 67/98, Decree-Law 7/98 and Law 41/2001.

[31]. Portugal is part of Convention 108 of the Council of Europe – Convention for the Protection of Individuals Regarding the Automated Processing of Personal Data - as well as its Additional Protocol Regarding Supervisory Authorities and Transborder Data Flows.

[32]. The most important body as far as data protection is concerned is NCDP. The powers of this entity are explained in detail in section 2 of his report. Concerning the effectiveness of the legal framework applicable to data protection, the problem is lack of staff – not lack of legal provisions. This is discussed in section 2.

[9] http://www.dre.pt/pdfgratis/1997/09/218A00.pdf (18/01/2009).

[10] http://www.parlamento.pt/RevisoesConstitucionais/Documents/Revisao2005/155a00.pdf (18/01/2009)

2. Data Protection Authority

[33]. The Portuguese Data Protection Authority (DPA) is the NCPD. According to Law 67/98, the DPA is empowered to control and supervise compliance with the legal and regulatory dispositions regarding the protection of personal data. This must be done showing due consideration for the human rights, freedoms and guarantees enshrined in the Constitution and in law (article 22.1).

[34]. Without wishing to describe all of the Commission's competences (articles 22 and 23, even though the former falls under the epigraph competences), it is important to mention that it is endowed with:

a) The power to investigate and to inquire, being able to access data subject to processing and to collect all information necessary to perform control activities (article 22.3, § a));
b) The power of authority, namely to order the blocking, erasure or destruction of data as well as to prohibit, temporarily or definitely, the processing of personal data, even those included in open flow networks through computers on national territory, (article 22.3), § b));
c) The power to implement all necessary and urgent interim actions in order to attain proof of evidence (article 22.5);
d) The competence to verify, upon request, the unlawfulness of the data processing whenever the processing is subject to restriction of access or information (article 23.1, § j));
e) The competence to judge claims, complaints or requests (article 23.1, §k));
f) The competence to deliberate on the application of fines (article 23.1, § n));

[35]. The NCDP is also competent to authorise, or exempt from the duty to notify, certain categories of data that do not put data subjects' rights and freedoms at risk (article 27.2). In the field of data protection, there is no limitation to the NCPD's authority remit.

[36]. These provisions not only cover legal competences proper to administrative bodies but also others close to the jurisdictional function, which has given rise to some doubts on the eventual judicial nature of the NCDP.

[37]. It is possible to appeal against any decision adopted by the NCPD. Such an appeal can be lodged at the Central Administrative Court (article 23.3).

[38]. Particular attention should be give to the NCDP's *powers* to advise or criticise the data processing controller publicly in the event of non-compliance with legal provisions in matters of personal data (article 22.4). As such, relevance is given to the independent nature of the body which, ultimately, may censure the bodies responsible for the appointment of its members.

[39]. Looking at all of the authority's competences, we can group them in the following way:

- *Consultative powers*; as regards the issuing of compulsory reports by virtue of legal provisions or by acts of community or international law (article 23.1, § a));
- *Decision-making powers*; which, among other things, determines the *prior authorisation* for the processing of sensitive data as specified in article 7, of personal data related to suspicious illegal activity, criminal infractions, misdemeanours, judicial sanctions, security measures, fines and accessory sanctions, of personal data obtained through the interconnection of data on credit and solvency (combining the dispositions of articles 8.2, 9, 23.1 § b), c) and d) and 28); *prior authorisation* for the pursuit of non-determinant purposes in the collection of data (article 23.1 § c)); and in the *recording* of personal data processing (article 23.1 § b));
- *Regulatory powers*; it may authorise *exemptions from the obligation to notify* and the *simplification of the notification required* through the publication in the "Official Journal" of the act containing the specified purposes, the categories of data to be processed and the categories of recipients (article 27.1 and 2); to issue *directives* on the duration of personal data registers in certain sectors of activity (article 23.1, § f)); to issue *directives* on safety measures relating to certain sectors of activity (article 23.1, § l)).

[40]. The NCDP has all the powers incorporated in the Directive as well as the power to examine police activities in the area of data protection. All public entities are obliged to cooperate with NCDP (article 46.º, Law 67/98), so NCDP officials can enter all public facilities and have access to all electronic systems and documentation regarding data protection. They can also collect whatever evidence is deemed relevant in the course of their investigations. The NCDP can also close sites in the Internet

[41]. It should be stressed that the NCDP can use their powers not only in the private, but also in the public sector.

[42]. In fact, on one occasion it was even decided to close the website of the Ministry of Justice. Such a measure was adopted because for sexual crimes, the full identities of victims were revealed on the site when judicial decisions were published, and the identities needed to be protected[11].

[43]. In order to implement these powers effectively, the Portuguese DPA is understaffed. The NCDP had 27 staff members in 2008, which is not considered sufficient to effectively carry out the tasks in its mandate. Therefore, it is considered necessary to increase the staff resources. The NCDP's annual budget for 2008 was nearly 2.4 million EUR. For more details about budget and staff, please see Annex 1.

[44]. As far as the independence of the members of the NCDP is concerned, it is important to know the nature of the body and the selection process involved.

[45]. The NCDP is composed of 7 members of impeccable standing. 3 of these are elected by the Parliament; 2 are appointed by the Government; one is appointed by the Supreme Council of Judges and 1 is appointed by the Supreme Council of Prosecutors. This balance is an attempt to ensure impartiality. Their mandate is incompatible with other public or private functions except teaching. The mandate has a duration of 5 years. Members of the Commission cannot be removed from office by the powers that chose them. The guarantees of independence mentioned above are enough to ensure effective use of powers given to the DPA.

[46]. The Portuguese DPA has the power to initiate investigations or audits on his own initiative, when deemed necessary. It means that the members of the DPA can submit to the collective body the proposal of starting an investigation. The Portuguese DPA can decide to check the application of data protection legislation even when there is no suspicion that a hypothetic violation has taken place. It means the Portuguese DPA can start an investigation when it deems necessary or adequate. These investigations can cover an entire sector or a company or administrative body.

[47]. Sometimes, items in the news or facts found during an investigation can make the DPA initiate such an operation. Because of their proactive approach, this process is followed by a full investigation – an ad hoc investigation. It means that an investigation methodology is used. A case in point was when a thorough audit was made to

[11] http://www.cnpd.pt/bin/decisoes/2000/htm/del/del042-00.htm (18/01/09).

hospitals[12]. In this case, some hospitals were chosen by the DPA, and a list of questions regarding data protection legislation was sent to them. Then a member of the DPA, joined by officials of the investigation department, visited said hospitals – verifying the veracity of the answers - and a final report was made and approved by the DPA.

[48]. The methodology used varies. A questionnaire or a check list with the legal duties of the public or private entities can be made if the DPA has decided to investigate an entire sector. When the initiative of the DPA is based on information collected in the news, a technical investigation is the most usual procedure.

[49]. An individual can complain about violation of data protection rights by contacting the NCDP. Other public bodies or the police can also report cases of data protection violations. In both cases, the Commission can investigate the circumstances or adopt the simplified procedure of contacting the alleged violator in order to persuade him/her to abide by the law. In this field, the NCDP has been very proactive in defending citizens.

[50]. Decisions are available to the public on the site of the NCDP. Some important decisions are published in Law books.

[51]. The Group of Article 29.º (constituted by members of every DPA according to the Directive 95/46) written opinions and other pronouncements made by the Group are taken very seriously by the NCDP. In fact, those decisions are often quoted by the NCDP in its findings. However they are not binding upon the Portuguese Authority.

[52]. According to the law, the Government and Parliament are obliged to ask for a written opinion of the NCDP in all matters concerning personal data, before legislation is adopted. As a result, the number of the decisions in this area is very high. Of course, the written opinions issued by the Commission are not binding upon the Government or Parliament.

[53]. The law takes into account the need to promote awareness of data protection among the public. To put this into practice, the Commission has published documents on video surveillance and privacy at the workplace. Members of the Commission have also participated in conferences and workshops on data protection. In addition, a strong link between law enforcement authorities and the

[12] http://www.cnpd.pt/bin/relatorios/outros/Relatorio_final.pdf (18/01/09).

Commission exists. For instance, members of the Commission give lectures in training courses for police forces. The Commission issues press releases about the main decisions taken.

3. Compliance

[54]. The NCDP must be notified of all data processing in both the public and private sector. Failure to rectify the information is punishable by fines. When sensitive data are involved, the NCDP must give prior authorisation. In the public sector, the entities involved in processing personal data were informed by the Portuguese DPA about the need to register or to ask for authorisation.

[55]. In the area of marketing, the NCDP took the initiative to promote codes of conduct for companies. It is possible to register or request authorisation over the Internet.

[56]. In Portuguese law, there is no reference to a data protection officer. However, major companies sometimes recruit qualified personnel to

deal with data protection issues, as these companies are aware of the legal problems that can arise in this area.

[57]. In spite of great efforts by the DPA and other public bodies, or by the press, there is a great lack of knowledge on the part of the general public of the legal obligations in this area. Small companies do not pay sufficient attention to these requirements and very often incur fines.

4.Sanctions, Compensation and Legal Consequences

[58]. The sanctioning regime in matters related to the protection of personal data classifies any violations as misdemeanours and crimes.

[59]. Especially relevant to misdemeanours are articles 37 onwards. So, within the meaning of article 37, the following behaviours are sanctioned with a fine:

- Non-compliance, through negligence, with the obligation to notify the Commission of the processing of personal data;

- Presenting false information or inadequately fulfilling the obligation to disclose the details needed for the recording or authorisation request;
- Keeping data flow networks open to persons who do not abide by Law No. 67/98, of 26 October.

[60]. Sanctions are set between 249.40 and 2,493.99 euros for natural persons and 1,496.39 and 14,963.94 euros for legal persons. These limits are doubled whenever the data refers to persons subject to prior control (paragraph 2).

[61]. Within the meaning of article 38, the following behaviours are punishable with fines of between 498.70 and 4,987.98 euros:

- Failing to inform the Commission about a representative in cases where the processing is done by a controller not established on Community territory (paragraph 1, §a)) and article 4.3, §c) and 4.5);
- Non-compliance with the rules related to data quality (paragraph 1, § b) and article 5);
- Non-compliance with the rules related to the right of information (paragraph 1, § b) and article 10);
- Non-compliance with the rules related to the right of access (paragraph 1, § b) and article 11);
- Non-compliance with the rules related to the subject's right to object (paragraph 1, § b) and article 12);
- Non-compliance with the rules related to automatic personal decisions (paragraph 1, § b) and article 12);
- Non-compliance with the rules related to special security measures (paragraph 1, § b) and article 15);
- Non-compliance with the rules related to the processing of data by a subcontractor (paragraph 1, § b) and article 16);
- Failing to provide due information (paragraph 1, § b) and article 31.3);

[62]. Fines are doubled whenever obligations are not fulfilled. Such as:

- Legitimate conditions for the processing of data (paragraph 2 and article 6);
- Processing of sensitive data (paragraph 2 and article 7);
- Processing of data related to illegal activities, criminal offences and misdemeanours (paragraph 2 and article 8);
- Processing through the interconnection of data (paragraph 2 and article 9);
- Processing related to the transfer of data outside the European Union (paragraph 2 and articles 19 and 20).

[63]. As regards the criminal issue, the epigraph in article 43 reads "*non-fulfilment of the obligation related to the protection of data"* and punishes with a prison sentence of up to one year those who, intentionally:

- Omit the notification or the authorisation request required by the personal data protection law (paragraph 1, § a));
- Give false information in the notification or in the authorisation request (paragraph 1, §b));
- Divert or use personal data contrary to the purpose for which it was collected (paragraph 1, § c));
- Promote or perform illegal interconnections (paragraph 1, § d));
- Do not abide, in due time, with the obligations imposed by the Commission in accordance with the law (paragraph 1, § e));
- Keep data flow networks open to access after the Commission's notification to the contrary (paragraph 1, §f));

[64]. The limits on the applicable fines are doubled whenever sensitive data or data referring to suspicious illegal activities, criminal offences and misdemeanours are at stake (paragraph 2).

[65]. Article 44 punishes the accessing of forbidden data with a prison sentence of up to one year.

[66]. The crime of *destroying or corrupting personal data* is punishable with a prison sentence of up to two year. These are applicable to anyone who, without authorisation, erases, destroys, damages, suppresses or modifies personal data, altering its usage (article 45.1).

[67]. The limits to the sentence are doubled if the damage is *particularly serious* (paragraph 2). In cases of violation of data protection through negligence, a prison sentence not exceeding is applicable (paragraph 3).

[68]. The law characterises and punishes the crime of *qualified disobedience* (article 46.1), the non-interruption, stoppage or blockage of data processing, after notification to that effect. Similar sentences apply to those who, after being notified:

- Refuse, without cause, to collaborate as required (paragraph 2, § a));
- Do not erase and destroy the personal data totally or partially (paragraph 2, §b));
- Do not destroy the personal data once the storage period has expired (paragraph 2, § c));

[69]. "*Breach of the duty of confidentiality*" (article 47) results from the disclosure or dissemination of information, without cause and without the subject's prior consent, by persons subject to professional confidentiality. The sanction applied is a prison sentence of up to two years. Within the meaning of paragraph 2, the sentence may be extended by half if:

- The agent is a civil servant or similar (§ a));
- The agent acts with the intention of gaining patrimonial advantage or illegal benefit (§ b));
- The agent puts the reputation, honour and consideration or intimacy of somebody else's private life at risk (§ b));

[70]. Except for the cases under paragraph 2, criminal proceedings depend on the lodging of a complaint (paragraph 4). Negligence is punished with a prison sentence of up to six months.

[71]. The attempt to commit one of these crimes is also punishable for all the crimes foreseen in the personal data protection law (article 48).

[72]. As regards the right to sanction, article 49 under the *accessory sanction* epigraph deserves special attention. It states that the following sentences may be accessorily applied:

- A temporary or permanent prohibition on processing, blocking, erasing and destroying data totally or partially (paragraph 1, § a));
- Publication of the sentence (paragraph 1, § b));
- A public warning or criticism of the person responsible for the processing (paragraph 1, § c));

[73]. There are difficulties in the way article 22.3 § a) and § b) interconnect. The main doubt concerns whether the temporary or permanent prohibition on processing, blocking, erasing and destroying data totally or partially may be ordered *except via an accessory sanction*. The doubt is even greater when one considers that article 22 refers generically to the Commission's functions. We feel that these operations should neither have the nature of a sanction or of a main sentence, nor that of an *accessory sanction* or *necessary and urgent interim act in order to assure proof of evidence* (article 22.5).

[74]. Data protection is also an important issue in the electronic communications sector. In this regard, the implementation of article 13 of European Parliament and Council Directive No. 2002/58/EC, of 12 July, by way of article 22 of Decree-Law No. 7/2004, of 7 January, deserves particular attention.

[75]. In the Decree-Law preamble, it states that "the implementation of Directive No. 2005/58/EC relating to the processing of personal data and the protection of privacy in the electronic communications sector was taken into consideration. (…) Article 13 of the directive refers to the use of unsolicited communications, which can only be established for purposes of direct marketing and may only be allowed in respect of subscribers who have given their prior consent. Our system derives from these provisions".

[76]. Article 22, entitled *unsolicited communications*, stipulates in paragraph 1 that the sending of messages for purposes of direct marketing, whose reception does not involve the recipient's intervention, namely those done through automated calling systems, facsimile machines or electronic mail, do not have the *prior consent* of the subscriber.

[77]. Paragraph 2 states that the system used to send messages to legal persons, gives the subscribers the opportunity to object. Unsolicited communications are admitted by the decree-law when *a natural or legal person obtains his customers electronic contact details, within the context of the sale of a product or service, and the same natural and legal person is allowed to send unsolicited publicity to its customers provided that the customers are clearly and distinctly given the opportunity to object, free of charge, to such use of electronic contact* (paragraph 3).

[78]. In any of the aforementioned cases, the recipient should have access to the means to refuse, at any moment, free of charge and with or without just cause, the sending of that publicity (paragraph 4).

[79]. For the purposes of creating an honest relationship between senders and receivers of unsolicited communications, the practise of sending electronic mail for purposes of direct marketing, and disguising or concealing the identity of the sender on whose behalf the communication is made, is forbidden (paragraph 5). According to this prohibition, therefore, "*each communication must have a valid address, electronic or otherwise, that is easily identified and to which the recipient may send a request that such communications cease* (paragraph 6).

[80]. The decree-law also makes reference for a list of people who do not wish to receive unsolicited advertising messages to be drawn up (paragraph 7). This list consists of names furnished by the Direct Marketing Association to advertising companies and anyone can approach this association in order to be put on the list.

[81]. The decree-law does not clearly establish which entity is empowered to adopt sanctions. Article 35.1 ascribes those functions – *central supervisory entity* – to the National Communications Authority (NCA) [*Instituto de Comunicações de Portugal (ICP-ANACOM)*]. At the same time, the special law assigns sanctioning competence to *specific entities* (paragraph 2). This issues of what entity (entities) are empowered to apply sanctions is not clear because of the wording of the law (this problem has not been resolved yet by the courts).The intervention of these specific entities leads to:

- The sanctioning regime foreseen in the decree-law only being applicable if there are no special rules (articles 41.1);
- The instruction and imposition of sanctions being the entire responsibility of the competent supervisory entity at the start of proceedings (article 41.2).

[82]. Article 37.1, § b) of the decree-law stipulates that the "*sending of unsolicited messages which do not abide by the legal requirements"* are misdemeanours sanctioned with a fine of between 2,500 to 50,000 euros,

[83]. Amongst the "common duties of the intermediary service providers" (article 13) is the fulfilment of "decisions intended to prevent or end an infraction, namely with regard to the removal or denial of access to information" (§ c)).

[84]. The sanctioning regime also comprises the following elements of the legal system:

- An accessory sanction necessarily implies the loss, to the State, of the means used in the practise of misdemeanours (article 38.1);
- Negligence is also subject to sanctions (article 37.4);
- An infraction by a legal person increases the maximum and minimum limits of a fine by a third (article 37.5);
- The publication of the sentence in cases of misdemeanours and the applicable sanctions is allowed (article 38.4);
- The definition of misdemeanours sanctioned with a fine of between 5,000 and 100,000 euros applicable to intermediary service providers that *do not abide by the court's decision or with the decision of the competent entity to prevent or to end criminal infractions* (article 37. 2, §c));
- Similar fines apply to those who repeatedly carry out the acts sanctioned by article 22 (§ f)).

[85]. The decree-law also regulates the *supervisory entities'* duty to "stimulate" the approval of codes of conduct (article 42.1). It is also

up to the entities to ensure these codes are *advertised on-line* (paragraph 3).

[86]. The remaining aspects of data protection within the field of electronic communications are governed by Law No. 41/2004, of 18 August.

[87]. Under the terms of the law, *electronic communication* means any information exchanged or delivered among a certain number of persons through the use of a publicly available electronic communications system (article 2.1, § a)).

[88]. In article 4.2, the article foresees the fundamental principle of the inviolability of communications, which comprises the prohibition on listening-in, tapping and the storage or other means of interception or surveillance of communications and respective traffic data by third parties without the explicit and prior consent of the users, except in those cases foreseen in law (such as cases of investigation during criminal proceedings). Legal recordings are also allowed when, within the context of illicit commercial practises, the evidence of proof is necessary (paragraph 3).

[89]. In general, traffic data related to subscribers or users which is processed and stored by companies on electronic communications networks should be deleted or made anonymous when no longer necessary (article 6.1).

[90]. The same principle applies to location data. Article 7.1 refers to cases where location data, other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services are processed. Such data may only be processed when it is made anonymous.

[91]. The right to the issuing of non-detailed invoicing (article 8.1) is foreseen. In this regard, paragraph 2 foresees the intervention of the NCDP, stipulating that the companies on electronic communications networks or publicly available electronic communications services should reconcile subscribers' rights to receive detailed invoicing with users' rights to privacy, namely by submitting proposals to the NCDP regarding the means by which subscribers can be given anonymous or strictly private access to publicly available electronic communications.

[92]. It is not obligatory to be included in public directories and subscribers always have the right to withdraw or to object (article 13.2).

[93]. When violations are detected by the DPA or other public bodies or through complaints received, these are investigated immediately. If the law has not been respected, sanctions are applied, which include fines. This is a frequent occurrence, In cases where no violation has taken place, the investigation is discontinued.

[94]. According to the law, compensation can be requested only in court. Since the NCDP does not intervene in these cases, it does not provide legal assistance. The NCDP is not aware of any requests of this nature presented in courts to date. There are no NGO's or other similar organisations that help the public in these matters.

[95]. The trade-unions ask the NCDP a great number of questions relating to data protection in the workplace. They also make complaints and draw the attention of the NCDP in particular to video surveillance and biometrics. The labour code demands that workers be heard through representatives in cases where video surveillance and biometrics are to be implemented. The authorisation and monitoring of such procedures are responsibility of the NCDP. In terms of the labour law, the NCDP is clearly aware of the need to establish a balance between employees and employers in this sensitive area. A list of guidelines has been approved to minimise disputes.

[96]. The crimes committed intentionally, and not because of simple negligence, are more severely punished more severely. The penalties described above show the exact differences in terms of sanctions applied.

5. Rights Awareness

[97]. The NCDP marked the European Day for the Protection of Data with a public presentation of the DADUS Project[13] at a ceremony which took place in the Auditorium of the Assembly of the Republic.

[98]. This project was developed by the NCDP within the scope of a protocol signed in 2007 with the Ministry of Education, through the Directorate-General of Innovation and Curricular Development, in order to raise awareness among primary and secondary school pupils about issues of data protection and privacy, to promote conscientious use of the new technologies and to develop civic conscientiousness among young people. The DADUS project was launched at the end of January 2008 in the mainland's state schools and will later be extended to the autonomous regions of the Azores and Madeira, as well as to the private and cooperative education systems.

[99]. The DPA developed a basic data protection program outlined in thematic units, to be worked with the pupils in the classroom. Each unit contains a summary with the main issues to be approached and working suggestions[14]. All the didactic material for the project created by the NCPD can be accessed in the website www.cnpd.pt.

[100]. Any teacher can use this material just by entering his/her name.

[101]. The Dadus Project is targeted to young people aged 10-15 years. It is a pioneering work designed for children born in the digital era and aims to make them aware of their fundamental rights.

[102]. There is an extra-curricular component consisting of a blog (see www.cnpd.pt) where pupils can find games, stories and comics as well as share experiences, express doubts and submit work related to the project.

[103]. The project can be considered a success: the number of visits to the site in the first year was 42.627. The number of pages accessed was 178.423 and the number of countries from which people visit the site was 67, including Brazil, the Portuguese speaking countries in Africa, South Africa, the USA, Egypt, Russia and allthe EU countries, inter alia.

---

[13] http://www.cnpd.pt/ (18/01/09).

[14] http://dadus.cnpd.pt/ (18/01/09). A complete explanation of the project can be seen is Clara Guerra, "Give a new generation a Chance" in http://www.datospersonales.org/ (18/01/09).

6. Analysis of deficiencies

[104]. The problems related to data protection in Portugal are the ones explained in the next number.

[105]. The greatest problem in implementing the existing legislation is the lack of qualified personnel to monitor what is happening and carry out investigations. Enforcement of the law is therefore the great problem. A great effort has been made to create a front office that can answer to all queries and explain the basics of data protection to the public.

[106]. Police services are covered by the Data Protection Law, in spite of the fact that the Directive does not refer to these bodies. Intelligence Services are not subject to the same law.

[107]. Data Protection does not need further laws to be effective. The Portuguese general law on data protection (Law 67/98) is adequate and is in fact supplemented by specific legislation in several areas. The problem lies in acquiring the resources to achieve better results in practice.

7. Good Practice

[108]. A prize has been set up for the best essay on data protection matters each year (2007)[15].

[109]. The nature of the authorisation granted by NCDP is not merely an administrative act, but involves an explanation of the particular procedures that authorised each case.

[110]. The NCDP form part of the Ibero-American network of data protection experts and authorities which promotes an exchange of points of view on this issue.

[111]. The NCDP and the Spanish *Agencia* organise a meeting every year. The venue alternates between Portugal and Spain. It is an informal meeting where the most important developments in data protection are discussed by members of each authority.

[112]. Some common actions organised by the Portuguese authority and its Spanish counterpart were carried out in the area of clinic tests.

[113]. The Commission has adopted guidelines on various topics related to data protection, which are available on its website[16].

[114]. The Commission has organised a meeting with all Portuguese speaking countries where it was possible to discuss issues related to data protection. The other countries involved were African Portuguese speaking countries – Angola, Mozambique, Cape Verde, Sao Tome and Principe and Guinea-Bissau - and Brazil.

[115]. The Commission accepts students and recent law graduates to do a practical training period in this area in order to familiarise them with the work of the Commission.

[116]. Members of the Commission also often give lectures at universities and in high schools.

[117]. A specific 2-month course in data protection was organised (2005) by Ordem dos Advogados (*The Portuguese Bar Association*). The course director was a member of the NCDP.

[118]. The NCDP has published reports and statistics that are available through the Internet[17].

[15] http://www.cnpd.pt/bin/relacoes/premio_ensaio.htm (18/01/09).
[16] http://www.cnpd.pt/bin/orientacoes/orientacoes.htm (18/01/09).

[119]. Every year the NCDP commemorates the European day of data protection, which falls on 28 January.

[120]. Some seminars were held on electronic commerce (2000), privacy in the workplace (2002) and electronic voting (2006), and general issues of data protection (1997 and 1998). In 2004, a seminar to commemorate the 10th anniversary of the NCDP was held.

[121]. In the late 1990's a campaign to make people aware of their rights in the Schengen space was launched.

[122]. The Dadus project is a pioneering experience (see 5).

[17] http://www.cnpd.pt/ (18/01/09).

8. Miscellaneous

Statistics

[123]. The National Statistical System has its general basis approved under Law 22/2008, of 12 May 2008.[18] According to this Act, entities considered as statistical authorities are empowered to require information (mandatory and free from charge) from all departments or agencies, individuals and legal entities, any necessary elements to make the official statistics, and may set up data collection that is invested of statistical importance.

[124]. All personal data collected by the authorities, for statistical purposes, are considered confidential, and are protected by professional secrecy, either by employees or others who became aware of them by means of their professional duties related with the official statistical activity.

[125]. The breach of confidentiality is considered a very serious administrative offense (violation of professional secrecy implies criminal responsibility).

[126]. The public dissemination of data can not allow the direct or indirect identification of subject involved. It is also forbidden that statistical individual data becomes available without the data subject's consent. Exceptions to this rule must be based upon public health reasons as long as such data are made anonymous.

Health

[127]. Rules and principles on collecting, processing and storage personal data on health are established by Law 12/2005, of 26th January.[19] According to this Law, personal health information must be kept confidential and stored in a secure health unit. Access to this data is granted to the data subject but must be communicated to the patient by a health care professional. Third parties are not allowed to have access to this data without the data subject's consent.

18 http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2008.92&iddip=20081084 (13/01/09).
19 http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2005.18A&iddip=20050264 (13/01/09).

[128]. Personal data on health also includes genetic information but the purpose of its collection and storage is strictly connected to health treatments and diagnosis. It is even pointed out that genetic information cannot be used or asked for the purpose of adoption of children, insurance contracts or contracts of employment.

[129]. According to Decree Law 267/2007 of 24th July,[20] data protection and confidentiality are granted in relation to blood donation and donors. Personal data related to them can only be used for therapeutic and public health purposes. The processing and combination of such data are protected by professional secrecy and adequate security measures.

[130]. It is guaranteed that the results of blood analysis and blood traceability as well as donor's health information are strictly confidential.

[131]. Third parties (public authority, agency or any other body) access to blood donors' personal data must be authorised by CNPD.

Education

[132]. The Law on students at basic and high schools – Law 3/2008 of 18th January[21] – states that the information included in a student's personal file (penalties, personal and family data) is strictly confidential and there is a secrecy duty for those who have access to them.

[133]. Decree Law 3/2008 of 7th January,[22] regulates issues related to students with special educational needs. It stipulates that all the information linked to technical and educational actions must be considered as personal data and processed according to Law 67/98 of 26th October. It is ensured that these data are confidential and those who have access to them have a secrecy duty.

Banking and Insurance

[134]. Decree Law 384/2007 of 19th November[23] creates a Central Register on life and personal incidents insurances and operations of capitalisation. The main purpose of this Register is to strengthen the beneficiary's position in case of the insured or subscriber's death. So

20http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2007.141&iddip=20072424(13/01/09)
21http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2008.13&iddip=20080147 (14/01/09).
22 http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2008.4&iddip=20080030 (14/01/09).
23http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2007.222&iddip=20073795(14/01/09).

it establishes the conditions for a third party to have access to the register of those products, while protecting personal data.

Public Administration

[135]. According to a public policy of reducing administrative burden, some ways of simplifying the relationship between citizen and Public Administration involve the consultation of personal data.

[136]. According to Decree Law 20/2007 of 23rd January,[24] one can authorise a public authority to consult his criminal record in order to facilitate the administrative process where that information is requested. Nevertheless such consultation merely returns a certificate of 'clean' record or not. So this simplification does not threat privacy and secrecy of personal data. Instead of going to another public service to request the certificate, citizens can request the public authority to disclose said information by electronic means.

[137]. A project on land registers aiming to create a unique central register is still being developed. Most of the data involved are not personal data but since processing of personal data is needed to some extent, the respect for legal rules concerning personal data protection is strictly guaranteed under Decree Law 224/2007, of 31st May.[25]

Social Security and Tax Administration

[138]. Since 2004, the alignment and combination of personal data is legally authorised, when correlating data in the social security filing system with data kept by tax administration. The processing of this data is strictly allowed to assure the compliance of tax and contribution duties, the fairness of social and fiscal benefits as well as to prevent fraud and tax evasion.

[139]. Decree Law 92/2004 of 20th April[26] refers to a combined data basis of those that belong to the services involved. The access to the data is restricted to accredited personnel using a code and personal password.

[140]. Any controllers and those who have access to personal data are under professional secrecy. Personal data must be kept only for as long as needed according to their purpose and, in any case, be destroyed five years after collecting.

---

24 http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2007.16&iddip=20070258 (14/01/09)
25 http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2007.105&iddip=20071983 (14/01/09).
26 http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2004.93A&iddip=20041069 (14/01/09).

[141]. Every year, technical audits certify that processing, transmission and combination of personal data are carried out in due respect for Law.

[142]. Involving all public services and the specific social security systems for public servants, Decree Law 309/2007 of 7th September[27] defines the purposes for which the combination of personal data kept by the mentioned public services is authorised. The possibility of correlating data in different filing systems is only open to certified personal and requires a password.

[143]. Decree Law 107/2007 of 10th April[28] defines some rules related to subsidised loans. In order to activate the subsidy and define the class of subsidised interest, credit institutions must communicate to the National Treasury some personal tax information provided by the borrower. However, the tax service is only allowed to combine these data with the information it disposes of about that citizen for the purpose signed. Since this combination only takes place within the service and if no breach of secrecy is committed, the respect for personal data protection rules is assured.

Citizen Card

[144]. The citizen card was recently adopted to substitute four other different cards each citizen should have. It is primarily a personal identity card, but it also contains a taxpayer number as well as a health care public services user number and a social security registration number. Rules about issuing and using this card were defined by Law 7/2007, of 5th February.[29]

[145]. As far as personal data protection is concerned, it is worth pointing out that the award of these four different numbers comes from four different filing systems which are separated and autonomous. Besides this, the issuing of this card does not generate a personal unique number as is constitutionally prohibited. This Law also prohibits any combination or correlation of data kept in those four different data bases or filing systems.

27 http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2007.173&iddip=20073022 (14/01/09.
28 http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2007.70&iddip=20071134 (14/01/2009.
29 http://www.dre.pt/util/getpdf.asp?s=dip&serie=1&iddr=2007.25&iddip=20070370 (14/01/2009)
.

Annex 1 - Tables and Statistics

Please complete the table below

	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of data protection authority (em Euros)	997.097	1.112.543	1.003.276	1.048.342	1.151.459	1424.030	1.431.080	2.183.929	2.390.650
Staff of data protection authority	10	13	16	17	16	16	19	23	27
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative Investigations	133	223	211	148	148	150	82	80	114
Number of procedures (investigations, audits etc.) initiated by data protection	19	18	28	40	35	30	24	35	40

authority at own initiative									
Number of data protection registrations	395	307	340	683	515	548	566	701	2483
Number of data protection approval procedures	296	317	988	1472	1088	1505	2803	3918	7821
Number of complaints received (and upheld) by data protection authority	153	184	162	173	156	183	177	200	227
Number of Opinions' requests on draft legislation received	37	23	15	49	42	41	45	55	59
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity:	Not available	Not available	Not available	Not available	Not available	Not available	Not available	Not available	Not available

settlement, warning issued, opinion issued, sanction issued etc.)									
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)				47 280.000	45 175.000	51 95.000	47 75.000	144 336.700	
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)	NA	NA	NA	NA	NA	NA	NA	NA	NA

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

Annex 2 – Case Law

Case title	Video surveillance at work
Decision date	20/02/2006
Reference details	Supremo Tribunal de Justiça (STJ) – Supreme Court of Justice Proc. Number 3139/05 – 4ª Sec
Key facts of the case	– A Trade Union came to Court to demand that a pharmaceuticals store was convicted to draw all the surveillance cameras (69) installed in the storehouse directed to employees' working places. – The defendant is frequently robbed and the stealers must be part of its staff. – The defendant asked CNPD authorisation to install 82 surveillance cameras in several places to prevent the past occurrences. – CNPD authorised videosurveillance since those recordings were to be kept for 5 days and used for criminal purposes.
Main reasoning/argumentation	– The Court of first instance did not uphold applicant's argument and a new appeal was made to the *Tribunal da Relação de Lisboa* (First Court of Appeal). The Court upheld the previous decision, and a new appeal was made to the Supreme Court of Justice. – Supreme Court of Justice made a costs/benefits analysis to decide upon principle of proportionality and uphold applicants' argumentation on illegitimacy of that video surveillance.
Key issues (concepts, interpretations) clarified by the case	– Principle of proportionality must help decide whether other interests are wealthier then fundamental rights such as the right to protect privacy of personal life or the right to likeness. This is the balance analysis requested to decide legitimacy of video surveillance. – Those fundamental rights shall be directly applicable to and binding on private persons and bodies including employers. – Preventive surveillance directed to specific individuals is a police measure so must be supported on a reasonable risk of crime events and be limited in time.

Results (sanctions) and key consequences or implications of the case	The Court decided that videosurveillance over each and every worker breached the principle of proportionality and was illegal. Cameras could be used by the employer but not at the storehouse where employees do their work. Those cameras should be removed.
Proposal of key words for data base	Principle of proportionality, videosurveillance, right to privacy, employment relationship

Case title	Informations on employees' health
Decision date	25/06/2006
Reference details	Tribunal Constitucional (Constitutional Court) Proc. Number 306/03
Key facts of the case	– President of the Portuguese Republic asked Constitutional Court to pronounce over some rules of Labour Code before its enactment. – Among the rules to be analysed by the Court was article 17/2 that stated that: "The applicant to work and the worker will not be demanded by employee to give information on health or pregnancy situation except when justified by specific requirements on the nature of professional activity and since there is a written reasoning". – CNPD was consulted over such rule after its approval and stated 17/2 in such words was unconstitutional.
Main reasoning/argumentation	– According to the President of the Portuguese Republic article 17/2 was doubtfully in accordance with articles 26 and 18/2 of Portuguese Constitution, violating principle of proportionality when restricting workers' right to privacy. – The same reasoning was adopted by CNPD that suggested some improvements to that rule in order to protect worker's privacy. – Constitutional Court uphold President's doubts based in the said argumentation.

Key issues (concepts, interpretations) clarified by the case	– Information on health and pregnancy are personal and included in worker's privacy. – The nature of professional activity doesn't justify employer's access to those information since only a doctor is able to certify whether that is accordance with the specific needs of the working activity. – If those information are only known by a doctor worker's privacy would be adequately respected.
Results (sanctions) and key consequences or implications of the case	The Court decided that article 17/2 of Labour Code was unconstitutional. In accordance to this judgement, the Labour Code enacted by the President and presently in force has an addition to that rule: "Such information above are to be given to a doctor who confirms or denies the worker's aptitude to work which is transmitted to employer (article 17/3).
Proposal of key words for data base	Principle of proportionality, right to privacy, health information, pregnancy, employment relationship .

Case title	Registry of check returned for lack of funds situations
Decision date	4/12/2008
Reference details	Tribunal Central Administrativo Sul (TCA-SUL) – (Central Administrative Court – South) Proc. Number 02240/98
Key facts of the case	– A bank's client presented a complaint to the CNPD based on the maintenance of his personal data related to check convention rescission in the bank's computerised data basis. – That information was no longer available at Portuguese Central Bank since prohibition from using checks has ceased. – CNPD determined that those negative references (of the complainer and generally of any costumer) should be erased as long as check convention rescission has ceased. – The bank requested for reconsideration but CNPD maintained the decision. – The bank then appealed to the administrative court.

Main reasoning/argumentation	– The bank argued that the data above mentioned are part of a commercial relationship (registry of a breach of contract situation) though are not under the constitutional provision related to right to privacy. Those data could be kept by the bank as long as there is a relationship with the client or a maximum of 10 years according to commercial law. – CNPD defined such data as personal and so it's up to the Commission to determine fr how long could them be kept by the bank.
Key issues (concepts, interpretations) clarified by the case	– Data on breaching check convention are personal data collected for the purpose of respecting the prohibition of using check. These negative data can't be kept as long as the prohibition itself has ceased. – Personal data must be collected for specified, explicit and legitimate purposes and not further processed in way incompatible with those purposes – At last, is for the Commission establishing the time for keeping the personal data according to their purpose.
Results (sanctions) and key consequences or implications of the case	The Court didn't uphold the administrative appeal, maintaining CNPD's decision on data protection. As a result of this judgement the bank is obliged to erase the client's data related to issuing checks with no funds as long as the register of sanctions enacted on that situation is no longer kept by Portuguese Central Bank.
Proposal of key words for data base	Maintenance of personal data register; check; banking; commercial relationship.

Case title	Telecommunication traffic data
Decision date	29/05/2002
Reference details	Tribunal Constitucional – Constitutional Court Proc. Number 241/02
Key facts of the case	– A worker was dismissed and came to Labour Court to attack that decision. – Employee asked the court to order the revealing of worker's telecommunication detailed bill and traffic data.

	– A court order in that sense was enacted and the operator did reveal those data. – Upon those the dismissal was legitimate. – Applicant made an appeal and second instance uphold the previous judgement. – Another appeal was made but for the Constitutional Court.
Main reasoning/argumentation	– Based on the duty of cooperation to the discovery of truth court issued an order to telecommunication operator to reveal traffic data and detailed bill. According to the Code of Civil Procedure (article 519/3b) that duty ceases when leading to breaching of personal privacy. Court of first instance argued that discover of truth would prevail. – On the contrary, Constitutional Court argued that secrecy of telecommunications evolves either its contents and the traffic data so there were personal data evolved that shouldn't be transmitted without the data subject's consent. – Evidence based on personal data obtained against the law are null.
Key issues (concepts, interpretations) clarified by the case	– Processing of personal data and protection of privacy in the telecommunications sector include either communications contents, traffic data and detailed bills. – Not even a judge can order the transmission of such data as evidence unless except for criminal procedure.
Results (sanctions) and key consequences or implications of the case	Constitutional Court uphold the appeal and judged unconstitutional the above mentioned interpretation of article 519/3b) of Code of Civil Procedure for breaching articles 26/1 (right to privacy) and 34/1 and 4 of Portuguese Constitution ("1- Personal homes and the secrecy of correspondence and other means of private communication shall be inviolable. / 4 - The public authorities shall be prohibited from interfering in any way with correspondence, telecommunications or other means of communication, save in such cases as the law may provide for in relation to criminal proceedings. ") First instance judgement was amended in due respect for Constitutional Court's decision.
Proposal of key words for data base	Right to privacy; telecommunications; traffic data; personal data; Labour procedure; evidence invalidity.

Case title	Sociedade Portuguesa de Informação Económica, S.A. (SPIE) Portuguese Society for Economical Information, SA

Decision date	4/07/2002
Reference details	Tribunal Central Administrativo (TCA) - Central Administrative Court Proc. Number 4621/00
Key facts of the case	– SPIE came to Court against a decision by CNPD that ordered the erasure of a data basis from their filing obtained through data collected by public registry of vehicles. – SPIE beeps several files authorized by CNPD as long as its corporate object includes marketing, statistical studies and market studies. – SPIE collected data (name, sex and address) of vehicles' owners.
Main reasoning/argumentation	– SPIES argued that public data (such as those in public registries) are no longer personal data though its protection is not CNPD jurisdiction. – The Commission contested that personal data may be public data if the medium involved is a public official document; public data as long as they are personal data are equally protected. – SPIE data collecting disrespects the specific purpose of initial collecting by public registry and it is unlawful. –
Key issues (concepts, interpretations) clarified by the case	– The principle of purpose of data collecting is applicable even when personal data are public official data. – Processing of personal data and transmission of data with combination should not be made by entities with different purposes.
Results (sanctions) and key consequences or implications of the case	The Court upheld the argumentation of CNPD and denied the requested annulment of its decision.
Proposal of key words for data base	Public official data; personal data transmission; collecting purposes; secondary data basis; register of vehicles.

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).