MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD SINCE THE 26TH MEETING OF THE T-PD (1-4 JUNE 2010)

Portugal has the honor to convey to the T-PD the following legislative developments, deserving some attention that took place between the 2010 T-PD meeting and November 2011.

We will also make reference to some decision of the Portuguese Data Protection Authority regarded by the CNDP as being the most significant during that period.

Legislative Developments

In what the legislation is concerned, it is to be noted that no changes to 1998 personal data protection law itself where introduced during that period, therefore what is reported here is legislation that in specific fields or for specific purposes created, detailed, developed personal data protection rules.

- **Decree-Law no. 48/2011 regarding de access and exercise of economical activities**
The purpose of this law is to facilitate de exercise of some economical activities by eliminating or simplifying administrative procedures connected with the attribution of licenses or other forms of authorization.
The administrative bodies authorized to process personal data are indicated (article 22). Those administrative bodies are responsible for the security of personal data entrusted with them (article 23). Personal data will be kept for as long as the economical activity is being exercised and after that for a specific period determined by law.

- Several **bilateral agreements in fiscal matters between Portugal and the Principat D'Andorra, Cayman Islands, the Bermuda, Jersey, Gibraltar, Saint Lucia and the Isle of Man**, have been published in the official journal this year (2011). Those agreements provide for the exchange of information between the Parties. Confidentiality and protection of personal data is assured in the following manner (equal in all those agreements):

"Article 8
Confidentiality
1 — All information provided and received by the competent authorities of the Parties shall be kept confidential.
2 — Such information shall be disclosed only to persons or authorities (including courts and administrative bodies) concerned with the purposes specified in article 1, and used by such persons or authorities only for such purposes, including the determination of any appeal. For these purposes, information may be disclosed in public court proceedings or in judicial decisions.
3 — Such information may not be used for any purpose other than for the purposes stated in article 1 without the expressed written consent of the competent authority of the Requested Party.
4 — Information provided to a requesting Party under this Agreement may not be disclosed to any other jurisdiction.
5 — Personal data may be transmitted to the extent necessary for carrying out the provisions of this Agreement and subject to the law of the Requested Party.
6 — The Parties shall ensure the protection of personal data at a level that is equivalent to that of Directive no. 95/46/EC, of The European Parliament and of the Council, of 24 October, and shall comply with the guidelines established by the United Nations General Assembly Resolution no. 45/95, adopted on the 14th December 1990."

- **Law no. 19/2011 modifies the 2000 law regarding minimum banking services**
Minimum banking services are those related to the creation and administration of a banking account, the attribution of a debit card, the access to ATM machines, home banking services and to banking services provided in the facilities of the concerned banks or credit/debit card issuer companies. The bank operations included are: deposit, withdrawal, payment of services and goods, direct debits and transfers between banks within the Portuguese territory, availability of information about bank operations regarding the bank account in question.
The access to the minimum banking services must be done through a bank that have adhered to "minimum banking services" chosen by the person interested in that kind of access and only through the bank in question.
The access to the persons banking information is allowed to other banks or businesses that manage debit or credit cards in order to confirm that the services above mentioned being requested to them have not also be requested or offered by other banks or debit/credit card companies.
The companies offering their bank and, or, debit/credit card services within the "minimum banking services" must guarantee to their clients of those services the right to access information about the quality of data subject to consultation, the finality of that consultation as well as the rights of access, rectification and elimination of data about them, this without prejudice of the application of the general personal data protection legislation.

- **Agreement between the Portuguese Republic and the United States of America to reinforce cooperation in the field of prevention and fight to crime**
This agreement was signed in 2009 and approved by the Decision of the Parliament no. 128/2011 of the 17th October.
It is an important text.
The Agreement defines:
"Personal data" in the following manner: "«Personal data» shall mean any information relating to an identified or identifiable natural person (the «data subject»)" (par. 3 of article 1); and

"Processing" of personal data is defined: "«Processing of personal data» shall mean any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, combination or alignment, blocking, or deletion through erasure or destruction of personal data" (par. 4 of article 1).
The agreement has to do with the supplying of DNA and fingerprint data. Other personal data can be provided "in order to prevent criminal and terrorist offences". "The personal data to be supplied shall include, if available, surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, nationality, passport number, numbers from other identity documents, and fingerprinting data, as well as a description of any conviction or of the circumstances giving rise to the belief referred to in paragraph 1" (par. 2 of article 11).
There are dispositions on "handling and processing of personal data" (article 12); "limitation on processing to protect personal (…) data" (article 13); "correction, blockage and deletion of data" (article 14); "data security" (article 16); and, "information to data subjects" (article 17), among others (please see the text annexed to this document).

- Co-operation Agreement Between the Portuguese Republic and Ukraine in the Fight Against Crime

This agreement signed in 2008, was published in the official journal and enters into force into 2010.
The aim of this Agreement is "to prevent, detect and prosecute crime and particularly the forms of organized crime, through the collaboration between their competent authorities" (Art. 2 Par. 1)[1].
This agreement has dispositions concerning confidentiality[2], confidential information, documents and personal data[3], use and transfer of personal data[4].

---

[1] "Article 2
(…)
2 — To this end, the Parties shall co -operate with each other in the fight against crime, in particular:
a) Illicit traffic in narcotic drugs and psychotropic substances, including precursors;
b) Money laundering;
c) Illicit trafficking in and use of nuclear materials and other radioactive substances, explosives and toxic substances, arms and ammunition;
d) Terrorism, participation in a criminal organization and in a terrorist organization as well as its financing;
e) Aiding illegal immigration, including the fraudulent use of identity and travel documents;
f) Trafficking in human beings, commercial sexual exploitation by third persons, and particularly sexual exploitation of children;
g) Theft of and trafficking in vehicles as well as alteration of their identity data;
h) Illicit trafficking in cultural or historical goods;
i) Corruption, economic and financial crime as well as counterfeiting of trademarks and patents;
j) Tax offences."

[2] "Article 7
Confidentiality
1 — The requested Party, if so requested, shall keep confidential the request for assistance, its content as well as the supporting documents.
2 — The requesting Party shall not use the information and other elements obtained as a result of the execution of the request for other purposes than those specified in it, without prior consent of the requested Party."

[3] "Article 8
Confidential information, documents and personal data
1 — The Parties shall, in accordance with the applicable international and domestic laws and based on this Agreement, keep confidential the information, documents and personal data that have been disclosed orally or in writing and that have been obtained for the purpose defined in this Agreement.
2 — The requested Party shall notify the requesting Party that the information given pursuant to this Agreement is considered confidential under the applicable international and domestic laws.

- **Law 33/2010 - law regarding the use of technical means of control at a distance**

The electronic surveillance of individuals is applicable by judicial decision and aims to ensure the respect for: a coercion measure of home detention; the execution of a prison sentence at home; the adaptation to conditional release from prison; other situations to which such surveillance is or may be applicable according to the law.

The monitoring can be done by telematic position, voice verification and other means that become acceptable.

This kind of surveillance must be done with respect for human dignity and other legal interests not affected by the judicial decision.

A database will be created with the following data: complete name, affiliation, civil state, sex, place of birth, nationality and place of known residence; citizen and tax identification cards numbers of the suspect or convicted under electronic surveillance; indication of the preventive measure or sentence being served; indication of beginning, suspension and end of the electronic surveillance; indication of the Court responsible for the decision and case number under which the decision was taken; indication of crimes for which the person is being investigated or was convicted; description of relationship between the defendant or convicted and the victim in case of crimes falling in the concept of domestic violence, or similar; date when the crimes were committed; place where the electronic device was putted on the person; electronic surveillance monitoring registration.

The right of access and rectification of data, the "transmission of data"; the storage of data (kept during 18 months while active and then removed from the network, but kept during three years, except when the application of the electronic surveillance was done to suspects during the investigation, because in those cases data will be immediately removed upon the end of investigation without accusation being formulated or when the accused is the object of an absolution sentence); as well as security of information are also regulated.

Deliberations of the CNDP

---

3 — Confidential information, documents and personal data received by the competent authorities of the Parties within the framework of this Agreement shall not be transferred to a third party without the prior consent of the requested Party and the appropriate legal safeguards for the protection of personal data, in accordance with the applicable international and domestic laws."

[4] "Article 9
Use and transfer of personal data
1 — The data used and transferred within the framework of this Agreement shall, in accordance with the applicable international and domestic laws, be:
a) Obtained for the purposes specified in this Agreement and shall not be further processed in any way incompatible with those purposes;
b) Adequate, relevant and not excessive in relation to the purposes for which they are collected, transferred and then processed;
c) Accurate and, where necessary, kept up to date; all reasonable steps should be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or corrected;
d) Kept in a form that permits identification of the data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed; they shall be erased after that period.
2 — If a person whose data are transferred requests access to them, the requested Party shall grant that person direct access to those data and correct them, except where this request may be refused under the applicable international and domestic laws."

Subsequently are mentioned some significant deliberations of the Portuguese DPA, during the period concerned in this information (as indicated by the CNDP). These decisions are important not because decisions on these subjects did not exist in the past, but because with those deliberations de CNDP decide to review and establish its doctrine on those subjects for its own future orientation.

It is not possible to detail those decisions here and, unfortunately at this time they are not yet available either in English or French.

Three deliberations deserve the attention:
1 – Principles applicable to the processing of personal data within the recording phone calls (Deliberation no. 629/2010)[5];
2 – Processing of personal data within the framework of the management of work health and security services (Deliberation no. 840/2010)[6];
3 – Personal data processing for the purpose of preventive and curative medicine in the field of control drugs, including alcohol, in the working environment (Deliberation no. 890/2010).
To refer just a few aspects mentioned in that decision it seems interesting mention the categories of data that's processing is considered to be adequate:
. Identification of the worker;
. Heath data related with consumption, including therapeutic plan;
. Substances object of detection/control;
. Information about detection tests;
. Identification of health professionals involved in the detection (subject to professional secrecy);
. Frequency of control and its justification;
. Dates of each control;
. Results;
. In case of a counter control being done, its results;
. Action adopted in case of a positive result.

[5] The recording of phone calls by "call centers" is in question in this deliberation.
Law no. 41/2004 – about the processing of personal data in the sector of electronic communications, determines that businesses offering networks and, or, services of electronic communications must guarantee the inviolability of communications and respective traffic data.
The exceptions are:
1 – Previous users express consent, with some exceptions;
2 – When, provided respected some conditions:
a) Those communications take place within the framework of commercial legitimate practices in order to document a commercial transaction;
b) They take place within a contractual relation;
c) The data subject was previously informed;
d) The data subject gave is consent.
3 –When the record of the telecommunications from and to public services take place in situations of urgency.
The CNDP reminds principles such as finality, transparency, respect for private life, respect for individual rights and freedoms, also the general law principle of good faith, and proportionality.
Consent must be free (means without any kind of coercion), specific (must address some specific fatuality), informed and express (within the contract because resulting from the accepting of contractual dispositions).
The DPA considers the recording of phone calls only for the purposes of monitoring the quality of the service to be disproportionate.
[6]Somes key notes:
- In what health information is concerned, the employer should only be informed of the results necessary to take his decision about the employment relationship through the "apt/non apt" information.
- Health information must be of restricted access to the medical specialist in work health problems or, under his direction and control, to other health professionals equally obliged to the professional secrecy.

Security measures also apply to manually processed data.

The access to medical records is reserved to doctors and other medical personnel obliged by professional secrecy, the information provided to the employer being "approved", "not approved", or "approved with restrictions".

The respect for data protection principles is, of course, approached as referred in the other Deliberations.

Lisbon the 23rd of November 2011