PORTUGAL ENACTS DATA PROTECTION LAW WITH NOVEL FEATURES

Portugal is the first country since 1988 to enact data protection legislation. It follows several years of preparation at both national and international level. Until April this year, Portugal's government representative, Dr. J. de Seabra Lopes, the Justice Ministry's Director, was Chairman of the Council of Europe's Committee of Experts on Data Protection. Portugal has thus been able to draw on the experience of other countries and also introduce some novel ideas into the legislation.

Legislative History

In 1984, the government proposed a data protection bill to the legislative assembly. The bill made no progress but the assembly approved ratification of the Council of Europe Convention (PL&B February 1987 p.20). This has had no effect yet as Portugal has not deposited its instrument of ratification at the Council of Europe's Secretariat General in Strasbourg. Since then, the constitution was amended on August 8th 1989 including a new clause on data protection and transborder data flows (PL&B September 1989 p.18).

When the legislature voted to adopt data protection legislation on February 19 this year, its vote related to the three different bills which had been proposed over the previous two years (PL&B August 1990 p.7):

1. the *Partido Socialista* version published on April 7 1989 (381/V)

2. the *Government's* version published on March 14, 1990 (135/V) and

3. the *Partido Renovador Democrático's* version published on April 18, 1990 (519/V)

A parliamentary committee synthesized these three texts into the new *Law for the Protection of Personal Data with Regard to Automatic Processing (Law 10/91).* The law was promulgated by the Parliamentary President on April 9, signed by the President of the Republic on April 12 and published in the official *Diário da República* on April 29 1991. It entered into force five days later.

Main Provisions

The new law covers the public and private sectors, although with some different rules for each sector; automated data only; physical persons only; has a central registration system similar to that in France and the UK; and requires prior notification for transborder data flows. The working of the law will be overseen by the National Commission for the Protection of Automated Personal Data (CNPDPI) which is established as an independent public body reporting to Parliament. The new law grants the usual rights, such as access and correction.

Novel Ideas

The law's novel or unusual provisions for a single data protection law relate to the powers of the Data Protection Authority; new rights; and the inclusion of computer crime provisions. These provisions:

- give the CNPDPI the *power to authorise the interconnection of automated data files* and data bases containing personal data (Article 8.1d) and to ban interconnection of personal data files, except when this law provides for it (Article 24.1)

- give the CNPDPI *the power to make binding decisions* which are contested or appealed to the Supreme Administrative Court directly without any intermediate stage (Article 8.2)

- permit *the automatic processing of specified sensitive data by public bodies* under the terms of the law on condition that it is done so "*with guarantees of non-discrimination and with prior consent of CNPDPI*" (Article 11.3)

- *require the destruction of data* "once the authorized term for the keeping of data has expired" (Article 23)

- *ban the use of a Personal Identification Number* to "interconnect personal data files

which contain information of a police, criminal or medical nature" (Article 24.2)

- require that where the law "in exceptional situations allows the interconnection of automated data files....[it] must clearly *define the type of interconnection authorised and its purpose*" (Article 26)

- require a file controller to *store data which has been wrongly omitted*, as well as the more common requirement to erase data which is excessive for its purpose (Art. 29)

- require file controllers and their staff to *maintain confidentiality of personal data even after they finish working in these positions* (Article 32.1)

- create the *offence* of breaking this law by "*creating, maintaining or altering the contents of an automated personal data file*" or causing such data to be processed (Article 34)

- create the *offence of gaining entry to a personal data information system* without due authorization (Article 38)

- create the *offence of unauthorized destruction or alteration of data* (Art. 39)

- create the *offence of violation of professional confidentiality* - revealing or divulging "personal data ....putting in jeopardy the reputation, honour and esteem or the intimacy of another individual's private affairs" (Article 41)

- state that an *attempt* to commit the above offences is *punishable* (Article 42)

- state that in addition to a fine and/or a prison sentence, a court may require *publicity about the sentence to be paid* wholly or partially *by the guilty party* in one or more instalments (Article 43).

Road Map of the Law

Chapter 1: General Provisions

Article 1 - General principle: "The use of automatic processing must be carried out openly and with strict regard for the fundamental privacy, rights, freedoms and guarantees of the individual."

Article 2 - Definitions

Article 3 - Scope. Main exemptions:

a) personal or domestic use

b) the processing of employees' salaries and other administrative procedures intended for management

c) the invoicing of sales or work carried out

d) the collection of members' fees.

Chapter 2: The National Commission for the Protection of Computerized Personal Data (CNPDPI)

Article 4 - The CNPDPI "to control the automatic processing of personal data with the highest regard for human rights and for the freedoms and guarantees established by the Constitution and by the law." The CNPDPI is independent and reports to Parliament.

Article 5 - The chairman and two other members are elected by Parliament; two others are magistrates; and two others are appointed by the Government.

Article 8 - Responsibilities of the CNPDPI are wide-ranging and include: giving its opinion on the creation of public data bases; authorizing or recording the creation of other data bases; issuing directives to guarantee the security of data whether stored on file or circulating in telecommunications networks; supervising the rights of access, correction and updating; enforcing this law; taking public complaints and requests; publishing an annual report; informing the Public Prosecutor of cases justifying legal proceedings; making binding decisions; and making suggestions to Parliament on data protection and privacy issues.

Article 9 - All public and private bodies must co-operate with the CNPDPI.

Article 10 - CNPDPI's members have a five year term.

Chapter 3: The automatic processing of personal data

Article 11 - Defined categories of sensitive data may not be processed automatically unless: the data is anonymized; is carried out by public bodies with guarantees of

non-discrimination and with prior consent of the CNPDPI; or the data has been voluntarily supplied by a data subject who is aware of where it is going and what it is going to be used for.

Articles 12-15 - Data subjects' rights including fair and lawful data collection, access, accuracy, and purpose limitation.

Article 16 - No decision which reflects on a person's behaviour may be based solely on the result of automatic processing.

Chapter 4: Automated personal data files, data banks and data bases

Article 17 - The processing of sensitive personal data must have the prior consent of the CNPDPI. For other personal data files, the CNPDPI must be informed by registration prior to processing.

Articles 18-19 - The CNPDPI's registration requirements which include "comparisons, interconnections, or any other way in which the information may be interrelated."

Article 20 - The CNPDPI's enforcement powers, such as the destruction of data files.

Article 21 - Standards for personal data security systems.

Chapter 5: Collection and interconnection of personal data

Article 22 - The information which must be given to individuals when collecting data.

Article 23 - The requirement to destroy data "once the authorized term for the keeping of data has expired."

Articles 24-26 - A ban on the inter-connnection of files and use of a Personal Identification Number with certain exceptions.

Chapter 6: Individual rights and guarantees

Articles 27-32 - The right of access; the file controller's duties to correct and store data; an individual's right to "request that his name and address be erased from data address files used for direct mailing;" a time limit of 30 days for a file controller to respond to individuals' requests; and file controllers' and staffs' duty of confidentiality.

Chapter 7: Transborder data flows

Article 33 - The law applies to international data transfers by any medium in automated format or collected with the intention that they will be automatically processed. The CNPDPI may authorize international transfers of personal data "if the State to which they are being sent can ensure the same protection as that offered by this law." Transborder data flows of personal data are prohibited "if there is good reason to believe that its transfer to another State is carried out in order to avoid any bans or prohibitions foreseen by law or to make possible its unlawful use."

Chapter 8: Infractions and violations

Articles 34-43 - Penalties of imprisonment and fines for a number of infringements of the law including: illegal use of data; refusing data subjects their rights; illegally interconnecting personal data files; supplying false information to the CNPDPI; gaining unauthorized access to a personal data information system; destroying or altering a personal data information system without authorization; not obeying CNPDPI instructions or behaving uncooperatively; revealing personal data; and attempting any of the above. An additional penalty is publicity about the court's sentence, paid for by the guilty party.

Chapter 9: Final clauses

Article 44 - Public bodies to prepare implementing regulations within six months and the Government to prepare implementing regulations within one year.

Article 45 - Public and private bodies processing non-sensitive personal data to register with the CNPDPI within 90 days for existing data bases and one year for new data bases. The CNPDPI must give its response within 60 days of a request for registration. The CNPDPI may ban or have personal data files destroyed if file controllers of existing files do not register by the due date.