

DATA PROTECTION ROUNDUP

Data Protection Roundup is a completely revised and updated version of this feature summarising the status of data protection legislation now extended to 35 countries. It is up to date as at mid-October. The 1987-1994 index will give references to reports by country and subject.

AUSTRALIA passed a Commonwealth (federal) Privacy Act in November 1988. The Act applies mainly to the Commonwealth public sector, and not to State government agencies nor as a whole to the private sector. However, the Act controls both the public and private sectors in their use of the Tax File Number, backed by guidelines enforced by the Privacy Commissioner. The Act covers physical persons and both automated and manual records. It came into force on January 1st, 1989.

The Privacy Amendment Act was enacted on December 24th, 1990, expanding the legislation and the Privacy Commissioner's jurisdiction to credit information. On January 23rd, 1991, the Data-matching Program (Assistance and Tax) Act was enacted which provides legal authority for a matching programme to be carried out by the Department of Social Security, other agencies and the Taxation Office under the scrutiny of the Privacy Commissioner.

AUSTRIA's Data Protection Act was passed on October 18th, 1978 and came into force in stages from January 1st, 1980. It was amended in July 1986 with the new provisions, for example, on international transfers of data coming into force on July 1st, 1987. The law covers physical and legal persons, and mainly automated data in both public and private sectors. It has a central registration system.

The need for further amendment of the Act has been recognised, but any action has been postponed awaiting the final adoption of the EU Data Protection Directive.

The Telecommunications Act, containing specific provisions on data protection entered

into force on April 1st, 1994. Also, the Genetic Engineering Act, with a very strict data protection regime, was passed in June 1994 and will come into force on January 1st, 1995.

BELGIUM adopted the *Act on the Protection of Personal Privacy in the Area of Personal Data Processing* on December 8th, 1992. Two Royal Decrees, containing details about the entering into force of the different sections of the Act, accompany the text of the new law. The final date for all provisions of the Act to enter into force was originally December 1st, 1994. However, full implementation has been delayed by six months.

In this way Belgium was able to ratify the Council of Europe Convention 108 on May 28, 1993 and it came into force on September 1st, the same year.

The new law contains uniform rules for public and private sectors and covers both automated and manual data. It is based on a system of registration and the Commission for the Protection of Personal Privacy has been appointed to monitor and control compliance with and application of this Belgian law.

CANADA has a Privacy Act passed in 1982. It came into force in 1983 and covers only the federal government and federal agencies. The Privacy Commissioner's jurisdiction has been extended to State owned companies, although Air Canada and Petro Canada are exempt.

On the provincial level, most Canadian provinces have passed privacy legislation. However, except for Quebec, these laws apply only to public sector activities. Most provincial legislation combines both public access to government information and privacy at the provincial and local level of government. Quebec is the first and only province where privacy principles have been extended to private sector organisations. Quebec's Protection of Personal Information in the Private Sector Act was passed in June 1993 and entered into force on January 1st, 1994.

CZECH and SLOVAK REPUBLICS
The Protection of Personal Data in Information Systems Law was approved by the former

federal government of Czechoslovakia on April 29th, 1992 and the law entered into force on June 1st the same year.

The law covers physical persons in the public and private sectors and automated data only. The registration system is envisaged for sensitive data only. A special regulatory body in each of the two new states will be responsible for enforcement. However, up to now, the regulatory bodies have still not been appointed in either state. The grant of licenses for transborder data flows will be the subject of secondary legislation.

DENMARK has separate Public Registers and Private Registers Acts, both passed in June 1978 and which came into force on January 1st 1979.

The Private Registers Act covers automated and manual records and applies to both physical and legal persons. Three types of organisation are required to register with the Data Surveillance Authority: credit reference bureaux, data processing service bureaux and blacklist registers, for example concerning bad credit risks. Amendments were passed in June 1987 strengthening the data subject's right of access, and entered into force in April 1988.

In January 1991, the government introduced a bill to amend the Public Registers Act to make the control of public files less bureaucratic. The bill was approved by the legislature in late May and entered into force on September 1st, 1991.

A sectoral Act on Media Information Databases was adopted on May 26th, this year and it entered into force on October 1st.

FINLAND passed a Personal Data Files Act on February 4th, 1987 which came into force on January 1st, 1988. The Act has been amended with effect from July 1st, 1994 to give some exemptions to specific, for example, editorial and genealogical, data bases.

The Act covers automated and manual records of physical persons and applies to both public and private sectors. It also requires companies to notify the Data Protection Ombudsman if they are processing certain types of name-linked data, for example, credit

information. The Data Protection Board may give permission for the export of "mass delivery" or sensitive data to countries that do not have legislation corresponding with the provisions of Finland's Personal Data Files Act.

Finland's Act should be read together with the Personal Data File Decree which entered into force on January 1st, 1988, as the latter makes specific references to the Personal Data File Act.

Finland ratified the Council of Europe Convention on December 2nd 1991 and it entered into effect on April 1st 1992.

FRANCE has a Data Processing, Data Files and Individual Liberties Act passed on January 6th 1978 and which entered fully into force on January 1st 1980.

The Act covers automated and manual records in both public and private sectors and provides for a central registration system. France's data protection law's right of access was extended to legal persons on July 3rd 1984 by an administrative decision of the CNIL, France's Data Protection Authority.

The direct marketing industry, after negotiations with the CNIL, published a Code of Conduct in December 1993. This is the first case of voluntary self-regulation through a code of practice by a particular sector since the enactment of the Act in 1978.

GERMANY The Federal Data Protection Act was passed on January 27th, 1977 and came fully into force on January 1st, 1979. The law covers physical persons' automated and manual records in both public and private sectors. Public sector name-linked files have to be registered with the Federal Data Protection Commissioner, while certain private sector files have to be registered with the Lander (state government) data protection supervisory bodies. In addition, the Lander have separate data protection laws covering access to name-linked data held by them and institutions owned by them, like banks.

The Data Protection Act was amended in late 1990 and the amendments entered into force on June 1st, 1991. The scope of the new

law has been extended to include audio-visual media, to strengthen provisions on compensation for damages and to explicitly introduce the principle of purpose limitation.

The specific Act on the Central Register of Foreigners, regulating the storage and transfers of personal data on foreigners living in Germany, asylum seekers and certain other categories, entered into force on October 1st, 1994.

GREECE introduced a data protection bill into the legislature in November 1987 but it was withdrawn by the Justice Minister a few months later for further consideration. The bill covers physical persons, automated and manual data in both the public and private sectors and has a central registration system.

Activities on the proposed bill have slowed down awaiting the outcome and final adoption of the EU Data Protection Directive.

GUERNSEY passed its Data Protection Act on July 30th, 1986, which came into force on November 11th, 1987. It covers physical persons and automated data in the public and private sectors. Unlike the UK, Guernsey has no Data Protection Registrar. The Advisory and Finance Committee oversees the law with the help of a Data Protection Officer who combines this work with other responsibilities.

HONG KONG Law Reform Commission's Privacy Sub-committee submitted its Final Report on the Reform of the Law Relating to Information Privacy in Hong Kong to the Law Reform Commission in summer 1994. The Report, published in August this year, is a result of public debate over the earlier Consultative Document published in March 1993. The Consultative Document was open for public debate and the Sub-committee has received over 80 submissions from interested parties in Hong Kong and abroad.

Depending on the government's decision in November as to the future of the proposal, Hong Kong could have a law in place by 1996.

The proposal applies to both automated and manual data and covers private and public sectors. Supervisory powers are given to a Privacy Commissioner. The proposal also

recognises the need for sectoral codes of conduct.

HUNGARY was the first country in Eastern Europe to pass data protection legislation. The law was enacted on October 27th, 1992, and was combined with a general right of public access to government information. The Act on the protection of personal data and disclosure of data of public interest entered into force on May 1st, 1993.

The Act covers automated and manual data of physical persons and has a limited registration system for some types of data. The law provides for the establishment of a Data Protection Commissioner, but until now, the Commissioner has not been appointed.

A new draft law on the protection of medical data is going to be submitted to the government next year.

Hungary signed the Council of Europe Convention 108 in May 1993, but has not yet ratified it.

ICELAND's Act Respecting Systematic Recording of Personal Data was passed in 1981 and came into force on January 1st, 1982. It covers both automated and manual records, physical and legal persons in both public and private sectors and has a central registration system. Unusually, the law was drafted with a clause that required it to be abrogated after three years. From January 1st 1986 and again from January 1st 1990, a new law with minor amendments came into force. However, this latest law is not limited to a fixed term.

Iceland ratified the Council of Europe Convention on March 25th 1991 and it entered into force there on July 1st 1991.

IRELAND's Data Protection Act was passed on July 13th, 1988. The Act covers physical persons and automated data in both the public and private sectors. The Act requires the registration of certain categories of data, such as sensitive data, all personal data held by public bodies and all personal data held by financial institutions, and agencies for credit reference, debt collecting or direct marketing.

ISLE OF MAN passed its Data Protection Act on July 16th, 1986. The law fully entered into force on October 17th, 1990 on the same date as the Isle of Man's ratification of the Council of Europe Convention. The Act is similar to the UK Data Protection Act, except that the exemptions have been widened to exclude many small businesses. Other differences include registration requirements and costs.

ISRAEL's Protection of Privacy Law was passed in February 1981 and entered into force on September 11th, 1981. It covers physical persons and automated records in both public and private sectors and has a central registration system. The law was amended on March 4th, 1985 to regulate the transmission of information between public bodies.

Chapter One of the law is exceptional in creating a civil law offence of infringement of privacy which covers 11 categories of behaviour including spying on a person; listening in; photographing a person in the private domain; publishing a person's photograph under such circumstances that the publication is likely to humiliate him or bring him into contempt; using a person's name, appellation, picture or voice for profit; and publishing any matter relating to a person's intimate life, state of health or conduct in the private domain.

In August, this year, Israel's Supreme Court made a decision supporting a ruling of the Registrar of Data Bases. The Registrar had refused to register a blacklist of people who had written cheques, not supported by adequate funds, when the data had not been collected for that purpose.

ITALY A Data Protection Bill was originally submitted to the Parliament in September 1992 and updated and amended in March 1993. However, it has now again been delayed by the recent general elections. The new Government is currently working on a revised Bill.

JAPAN The law on Protection of Computer Processed Personal Data held in Administrative Organs was enacted on

December 16th, 1988 and came into force in stages starting on October 1st, 1989. Chapter 3 of the law covering individual rights, such as access and correction of personal data, came into force on October 1st, 1990.

The Act covers automated data in national government departments. It is based on several data protection principles, but is subject to a number of exceptions, for example, civil servants have no right of access to personal data on themselves. The central co-ordinating body for this legislation is the Management and Co-ordination Agency in the Prime Minister's Office which does not have the status of an independent Data Protection Authority.

Government departments have strongly encouraged parts of the private sector, such as finance, telecommunications and credit information to establish codes which reflect the OECD Guidelines.

JERSEY, a self-governing entity within the UK, passed a Data Protection Law on April 30th, 1987. This is similar to the UK's Data Protection Act, covering both public and private sectors and using a central registration system. It came into effect from November 11th, 1987, the same date as the UK law became fully operational.

LUXEMBOURG's Act regulating the use of name-linked computer data was passed on March 31st, 1979 and entered into force on October 1st, 1979. The law covers the public and private sectors, automated records and legal persons, and has a central registration system. Amendments of September/October 1992 concerned police files and medical data. The law has had a fundamental review by the seven person Data Protection Commission. Publication of the EU Data Protection Draft Directive has meant that its proposals to amend the Luxembourg law have been postponed until final adoption of the Directive.

MALTA's application for membership of the European Community has helped to move data protection up the list of priorities for legislation. The government had been preparing a data protection and freedom of information bill when the legislature was

dissolved in February 1992 for a general election. Work on a new Bill has been going on ever since and the Draft Information Practices Bill is being studied by the *ad hoc* Cabinet Committee set up for the purpose.

THE NETHERLANDS's Data Protection Act was adopted by the Upper House of the States General (legislature) on December 27th, 1988 and received royal assent the following day. It entered fully into force on July 1st, 1990, which also served as a deadline for registration.

The Act covers physical persons and gives legal persons some rights. It applies to both private and public sectors and automated and manual records. Unusually, the Netherlands' law requires registration of manual personal data. The law works on a system of public declarations of name-linked files which have to be notified to the Registration Chamber.

The law encourages each sector to develop its own code of conduct which it must discuss with a representative consumer organisation before submitting it to the Registration Chamber for approval. The first industry codes of conduct approved by the Registration Chamber were from the Recruitment and Staff Selection Agencies' Association, the Information Technology Trade Association, and the Mail Order Association.

Comprehensive rules on the processing of sensitive data are contained in the Royal Decree on sensitive data which was signed in February 1993 and entered into force on June 1st, the same year.

In August 1993, the Netherlands ratified the Council of Europe Convention 108 which subsequently entered into force on December 1st, the same year.

NEW ZEALAND's Privacy Act was assented to on May 17th, 1993 and entered into force on July 1st, the same year. The Act repealed and consolidated the Privacy Commissioner Act of 1991 and included comprehensive new provisions.

The new law applies to both public and private sector "agencies." The jurisdiction and powers of the Privacy Commissioner,

originally appointed under the Privacy Commissioner Act, have been extended to cover both sectors and include complaints.

A particular feature of the Privacy Act is that it contains comprehensive rules on data matching between public sector agencies.

Also, the Act provides for sectoral codes of practice. These codes, which are formulated through a process of public notification and consultation and issued by the Privacy Commissioner, may set up either a more or a less strict regime than the one envisaged by the Act. Codes of practice are binding and enforceable. The first code issued under the Act was the Health Information Privacy Code of June 28th, 1994 containing 12 health information privacy rules which substituted the 12 information privacy principles of the Act. Work is under way on several other codes of practice in the following areas: superannuation schemes, motor vehicle registry, Police and Justice Department information. Also private sector organisations have commenced work on sectoral codes of practice, such as in the credit reporting sector.

NORWAY's Personal Data Registers Act was enacted in June 1978 and came into force on January 1st, 1980. It applies to both the public and private sectors, manual and automated records and covers physical and legal persons. The law also provides for a central registration system. On October 1st, 1987, the Act was strengthened regarding direct mail, telemarketing and consumer credit.

The law's notification system is currently under review. A bill has been prepared on video surveillance in public places which aims at regulating, *inter alia*, the protection of personal data obtained from video images.

POLAND has been working on specific legislation on data protection in recent years. A draft Data Protection Act is being currently examined by the Council of Ministers

There are some data protection provisions in other legislation, such as the Civil Code. In April 1993 a new order of the Ministry of Health on the storage of medical information

including provisions on the protection of medical data, became effective.

PORTUGAL The Assembly passed the Protection of Personal Data Act which was published on April 29th, 1991 and entered into force on May 4th, the same year. There were further amendments to the Act in August 1994 regarding the conditions of processing sensitive data and the rules on transborder data flows.

The Act covers automated data of physical persons and envisages a registration system similar to the UK. Supervisory powers are given to a seven-member National Commission for the Protection of Automated Personal Data which was established in January this year.

The National Commission has powers to limit the export of name-linked data, implementing section 35-6 of Portugal's 1989 constitution. In addition to the sanctions in the new law, infringements of the constitution's provisions may lead to the penalty of imprisonment under article 181 of the Penal Code.

The Council of Europe Convention 108 was ratified on September 2nd, 1993 and it entered into force on January 1st, 1994.

SLOVENIA's first Personal Data Protection Act was passed in March 1990. This law has been substantially revised and on the recommendation of expert opinion of the Council of Europe given in April this year, a new proposal has been prepared. The new Bill, covering both public and private sectors, is still in the first stage of the parliamentary procedure. The Legal Informatics department of the Ministry of Science and Technology, the initiator of data protection legislation, is currently being reorganised and will form a part of the Ministry of Justice.

Slovenia has ratified the Council of Europe Convention 108 on May 27th, this year and it came into force on September 1st, 1994.

SPAIN's Data Protection Act entered into force in February 1993, after being adopted by the legislature on October 8th, 1992 and being signed by the King on October 29th, 1992. The Act covers automated records in the public and private sectors. Although manual files are not

included within the scope of the Act, it authorises Government to extend its provisions to manual files, after consultation with the Data Protection Agency.

The Data Protection Agency is an independent public authority with control and enforcement powers. The latest general elections and the dissolution of the Parliament delayed the establishment of the Data Protection Agency to the end of July this year when the Agency became fully operational.

SWEDEN adopted the world's first national data protection law, passed on May 11th, 1973, which has since been amended several times. It covers physical persons, automated records in both the public and private sectors and has a central registration system supervised by the Data Inspection Board.

Discussions about major changes of the law have been going on for some time without a decision. Pending new legislation, the Government has proposed empowering the Data Inspection Board to issue general rules of conduct for individual sectors. Those complying with the rules will be exempted from applying for a licence from the Data Inspection Board. A final decision on the proposed system has been delayed following the general elections in September this year.

SWITZERLAND adopted a Data Protection Act on June 19th, 1992 and it entered into force on July 1st, 1993.

The new Swiss law contains uniform rules for public and private sectors and covers both automated and manual data. The Act is not restricted to protection of personal information of individuals, but covers legal persons also. The Act has introduced a registration system for certain categories of name-linked data.

A Federal Data Protection Commissioner has been appointed to monitor and control the implementation of the Act. The Commissioner has already published three guidelines explaining the rights and duties envisaged by the Swiss Act and is preparing a fourth one on data security.

Switzerland has neither signed nor ratified the Council of Europe Convention 108. Ratification is expected at the earliest in 1996.

TURKEY A Data Protection Bill has been prepared and it is still in the parliamentary procedure.

THE UK's Data Protection Act was passed in 1984 and it entered fully into force on November 11th, 1987. The law covers automated records of physical persons in both public and private sectors and has a central registration system.

In the Innovations decision of 1993 the Data Protection Tribunal upheld the Data Protection Registrar's position on and interpretation of the fair obtaining principle. The Tribunal concluded that individuals should be informed of the non obvious purposes, for which data will be used, at the time of collection.

THE USA's Privacy Act was passed in 1974 covering the federal government only. Each agency has to publish in the *Federal Register* at least annually a notice of the existence and character of its system of records and how data subjects may gain access. Several states, such as New York and California have similar laws covering access to records held by state agencies.

There is also sectoral federal data protection legislation for example, the Federal Fair Credit Reporting Act, The Family Educational Rights and Privacy Act of 1974, and the Video Privacy Protection Act passed in 1988. In late 1988, the US Computer Matching and Privacy Protection Act became law. It covers federal agencies and requires them to follow certain standards when carrying out computer matching to ensure that individuals are not harmed by unauthorised use of name-linked information, or refused government benefits because of inaccurate data.

On December 21st, 1991, the Automated Telephone Consumer Protection Act to regulate telephone marketing was adopted and it entered into force on December 20th, 1992.

While there is little prospect of the United States following the European lead on adopting comprehensive data protection legislation, the US congress has held hearings on a few privacy issues. In April 1992, the US House of Representatives' Committee on Government Operations published a report - *Designing Genetic Information Policy: The Need for an Independent Policy Review of the Ethical, Legal and Social Implications of the Human Genome Project*. In May 1992, a public hearing was conducted on the Privacy Implications of the US Postal Service Address Correction Services by the Government Information, Justice, and Agriculture Subcommittee. In May this year, the US House of Representatives' Information, Justice, Transportation and Agriculture Subcommittee of the Committee on Government Operations held public hearings on the Fair Health Information Practices Bill (H.R. 4077).

The Executive Branch's current main interest in privacy issues is expressed in the context of the National Information Infrastructure. This is an initiative led by Vice-President Al Gore and has a Working Group on Privacy which has drafted some *Principles for Providing and Using Personal Information*. The chair for this group was the Acting Director of the US Office of Consumer Affairs which organised public meetings early this year in Sacramento, California and Washington DC. The new chairperson is the Information Systems Privacy Advocate at the Internal Revenue Service.

This report has been updated by Bojana Bellamy, a *Privacy Laws & Business* consultant.