PL&B International data protection roundup

IN THE SECOND PART of this year's *PL&B International* Data Protection Roundup, we present an update on the developing privacy laws of eleven countries across the world.

AUSTRIA

In August this year the Austrian government issued new guidelines for the direct marketing profession that update regulations in effect since 1994. The new regulations essentially give individuals greater control over the data held on them by direct marketing organisations and list brokers.

Individuals must give written consent before marketers may transmit any information to third parties other than eight specific items - namely name, gender, title, degree, address, birth date, professional status and details of earlier presence on the lists.

The new rules also create a kind of "do-not-call" list (updated at least monthly) of those who choose not to receive any unsolicited advertising material whatsoever. To join the list, Austrians simply send a form to the Austrian direct marketing professional association in Vienna.

In January, Austrian authorities also updated the data processing registration and other forms, in addition to ensuring publication of all the relevant laws on its website. The authority encourages online applications and also provides guidelines for sight-impaired visitors.

Although most of the Austrian data protection website is in German, some of the basic information is translated (unofficially) into English and/or French.

Contact: Büro der Datenschutzkommission
Ballhausplatz 1
1014 Wien AUSTRIA
Tel: +43 (0)1 531 15 / 2525
Fax: +43 (0)1 531 15 / 2690
E-Mail: v3post@bka.gv.at
Website: www.bka.gv.at/datenschutz/

HONG KONG

Hong Kong's Personal Data (Privacy) Ordinance came into force on 20th December 1996. It covers both automated and manual data and applies to both private and public sectors.

The Data Protection Principles enshrined in the Ordinance are reflective of the EU's Data Protection Directive 95/46/EU on the collection, use and processing of personal data. These Principles are given statutory backing through an investigatory and enforcement process mandated by the Ordinance, where non-compliance of an enforcement notice may give rise to criminal sanction. Civil remedy arising from contravention is also provided for in the Ordinance.

To give greater clarity to the requirements under the Ordinance, and to assist data users in understanding the regulatory remit and principles applied by the regulator, the Privacy Commissioner is empowered to issue guidelines and codes of practice. The Commissioner has, pursuant to his statutory powers, issued codes of practice on Identity Card Numbers and other Personal Identifiers, Human Resource Management and Consumer Credit Data. The Commissioner has also approved other industry-specific code of practice and guidance notes. Contravention of provisions in a code of practice may give rise to statutory sanction under certain circumstances.

In March 2002, the Commissioner's Office published a public consultation paper with a Draft Code of Practice on Monitoring and Personal Data Privacy at Work.

Contact: Office of the Privacy Commissioner for Personal Data
Unit 2001, 20/F, Office Tower, Convention Plaza,
1 Harbour Road,
Wanchai, Hong Kong
Tel: +852 (0)2827 2827
E-mail: pco@pco.org.hk
Website: www.pco.org.hk

HUNGARY

The rights to protection of personal data and disclosure of data in the public interest were enshrined in Hungary's fundamental law in the 1989 amendment to the republic's constitution. In 1992, the National Assembly passed the Act on the Protection of Personal Data and the Disclosure of Data of Public Interest (DP&FOIA).

This single act regulates information-related rights and entrusts their supervision to a Data Protection Commissioner who is elected for a six-year term by a two-thirds majority of Parliament. The Commissioner files annual reports with the National Assembly, and spells out his position on issues in non-binding recommendations.

In 2000, the European Union declared that Hungary's data protection law provided protection on an equivalent level to the EU Data Protection Directive. Organisations may thus transfer personal data to Hungary without having to implement standard contractual clauses.

Regulation of personal data

In July 1999, the Act was emended to distinguish between data controllers and data processors, previously classified in the same category. The latter is now understood to be "any natural or legal person, as well as any organisation that processes personal data on behalf of the data controller". The data controller defines the purpose of using the information.

The DP&FOIA guarantees individuals' rights to access their personal data, and to request correction or (unless prohibited by law) deletion of that data. Data controllers must respond to requests within 30 days, and individuals may seek help from the Data Protection Commissioner or seek damages through court proceedings. Data controllers may not refuse to release information unless there is a legal exemption, and must inform the Commissioner annually of any refused requests.

Organisations must notify the Commissioner of any processing of personal data and include details on the Data Protection Register. The law specifies exceptions to the obligation to register (including employment and educational status, or the processing of personal information by the data subjects themselves for their own personal use). The function of the register is simply to record rather than to construct a legal basis for the processing. Registering data control does not in itself entail an investigation by the Commissioner into the legality of the reported activity.

Subject access to non-personal information

Information "of public interest' is any information processed by any authority that functions within the public sector. The person or body performing state or local government functions or other public duties (the "authority") must, within its jurisdiction, provide accurate and prompt information for the general public. The authority must regularly publish or allow access to the most important data about its activity-particularly those pertaining to its powers, competence, organisational structure, the types of data it possesses and any provisions regulating its operation. The name and official position of a person acting on behalf of the authority is considered public data and accessible to anyone, unless otherwise provided by law.

The authority must fulfil requests for disclosure of public interest data within 15 days, in writing. If it turns down the applicant, it must give notice in eight days. When the authority refuses or ignores a request, the applicant may seek remedy in court. In such cases, the court will act with a special fast-track procedure and order violators to supply the information sought by the plaintiff.

Current developments

Current developments concern modifying legal norms on enforcing information rights. The key elements aim to regulate the two information-related domains (data protection and freedom of information) in two separate acts under the Data Protection Commissioner's supervision. The Commissioner's powers will be extended by a law replacing the traditional ombudsman functions with a model mixing administrative features with those of an independent institution.

The new bill includes separate provisions for criminal records, and establishes that data in the public interest does not include all information processed by a public authority, only that pertaining to the authority itself.

Contact: Dr Attila Pêterfalvi,
Office of the Parliamentary Commissioner for Data Protection and Freedom of Information
1051 Budapest, Nâdor 22, Hungary
Tel: +36 (0)1 475 7186
Fax: +36 (0)1 269 3541
Website: www.obh.hu/adatved/indexek/index.htm (in English)

JERSEY

Jersey's Data Protection Registrar, Michael Smith is now working on the drafting of new data protection legislation implementing the requirements of EU Directive 95/46/EC, thus ensuring the Island, which is not in the EEA, is deemed adequate (as defined in Article 25) in terms of the transfer of personal data.

The current law dates back to 1987 so the Island has had experience of many years of effective data protection legislation. To further improve and strengthen the data protection authority, a Deputy Registrar, Compliance Officer and Administrative Assistant have recently been appointed.

The Island of Jersey is home to a thriving and reputable offshore finance industry that is responsible for over 500 billion dollars worth of assets from around the world. It is imperative that the Island maintains its reputation of being a well regulated and co-operative jurisdiction by ensuring compliance with all legislation. Jersey has to deal with a significant number of requests for the "exchange" of information in the global fight against financial crime. Responding in compliance with both the legislation that allows access to client information, as well as legislation designed to protect the privacy of the individual, will serve to preserve the Island's reputation and integrity, ensuring it remains an international finance centre with the highest regulatory standards, endorsed by a series of international evaluations.

The Registrar's Office has taken a proactive role in working closely with the Financial Services Commission of the Island to ensure a cohesive and professional approach. In addition, a number of presentations and training sessions are provided for the finance sector to raise awareness of privacy issues, and place data protection legislation within the context of other legislative requirements in areas such as money laundering.

A significant rise in the number of registrations under the Data Protection (Jersey) Law 1987, together with a noticeable rise in status of compliance/privacy managers in organisations, both public and private, clearly demonstrates Jersey's firm commitment to obtaining an adequacy status from the EU Commission.

Contact: Emma Martins, Deputy Data Protection Registrar
Morier House, Halkett Place
St. Helier, Jersey, JE1 1DD

Tel: +44 (0)1534 502344/502325
Fax: +44 (0)1534 502399
Email: e.martins@gov.je
Website: www.dataprotection.gov.je

KOREA

January 2001 saw the passage of Korea's Act on Promotion of Utilization of Information and Communication Network and Data Protection (No. 6360). It took effect in July 2001.

Last July, the government set up a Personal Information Protection Centre which was placed under the control of the Korean Information Security Agency (KISA). The centre's activities include evaluating a diverse range of information security systems, promoting the information security industry, and offering professional education on information security. The cyberprivacy organisation also conducts research and development on coding technology, develops system and network security technology, and studies information security technology standardisation.

The government has also launched a public awareness campaign on information security. On November 28th in Seoul, it will host an International Conference on Personal Data Protection. Speakers from several countries will discuss important and controversial privacy issues such as unsolicited e-mails, location-based services, surveillance in the workplace, and remedies for personal data infringements (see: www.cyberprivacy.or.kr/inter_01.htm, Tel: + 82 (2) 1336).

In addition, KISA has launched "Operation CYBER 118" to help Internet users prevent computer security breaches. CYBER 118 receives requests and provides advice on hacking and viruses via telephone, e-mail, and the Internet.

Contact:
Korean Information
Security Agency (KISA)
78 Garak-Dong,
Songpa-Gu,
Seoul, Korea 138-803
Tel: + 82 (2) 1336
E-mail: cert@certcc.or.kr
Website: www.kisa.or.kr/english

MALAYSIA

Upcoming Malaysian legislation on personal data protection is likely to include provisions to protect national and public security interests, according to Datuk Amar Leo Moggie, the Malaysian Energy, Communications and Multimedia Minister.

Moggie told local paper *The Star* that the Personal Data Protection law should enhance privacy rights but "it is important (also) to recognise that individual privacy rights are never absolute".

He said that the individual's privacy rights should always be balanced against competing public and private rights and interests, and indicated that exceptions would be made in enforcing the new law.

"The legislation…proposes several exemptions to meet the unique nature and requirement of certain activities and bodies," Moggie said in an address at a data protection seminar organised by Jagat Technology.

The law was due to be passed last year but there are still some policy issues that need resolving before the Personal Data Protection legislation can be tabled in Parliament, according to Chan Yoke Kin, of the Malaysian Ministry of Energy, Communications and Multimedia Communications and Multimedia.

"Some of the policy issues regarding this proposed legislation are highly sensitive and concern both government and private sector entities. We regret that it is not possible for us to disclose its current status to you at this juncture", wrote Chan Yoke Kin in an e-mail to PL&B International.

Contact: Zainal Abidin bin Mat –
Public Relations Officer
Ministry of Energy, Communications and Multimedia
1st Floor, Wisma Damansara
Jalan Semantan
50668 Kuala Lumpur, Malaysia
Tel: 03-20875000
Fax: 03-20957901
Website: www.ktkm.gov.my

MONACO

Monaco created the Commission de Contrôle des Informations Nominatives (Data Protection Commission) in 1999. It includes six members (three permanent and three alternates) appointed by a royal commission for a three-year term. Data protection clauses for the principality are found in law number 1.165 of December 23rd 1993, in the Code of Civil Practice and in the Constitution. The latter guarantees respect for privacy and secrecy of correspondence (Article. 22S).

In some cases, formal declarations to the Commission for both the private and public sectors can be simplified. These categories of personal data include:

- Processing supplier or customer files
- Maintaining staff payroll files
- Maintaining customer accounts and related information from banks
- Processing securities and other financial instruments
- Managing credits and loans provided to physical persons by credit institutions.

Although the law protects non-automated processing, it does not have to be declared to the Commission. Articles 21 and 22 allow for criminal penalties and fines in cases of violation.

Contact: Commission de Contrôle
des Informations Nominatives
7, rue du Gabian
98000 MONACO
Tel: +377 (0)97 70 22 44
Fax: +377 (0)97 70 22 45
E-mail: ccin@gouv.mc
Website: (in French) www.gouv.mc

POLAND

Passed in April 1998, Poland's Law on the Protection of Personal Data is based on two general provisions:

1. Any person has a right to have his/her personal data protected.

2. Personal data may be processed in the interest of the public, the data subject, or any third party, within the scope and subject to the procedure

stipulated in the act.

On May 23rd 2002, Poland ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS no. 108, January 28th 1981). The instrument took effect on September 1st 2002.

The government is now preparing an amendment to the Protection of Personal Data Act conforming with the European Commission's observations. The aim of the amendment is to ensure that Poland's data protection legislation complies fully with the EU Data Protection Directive.

From May 22-24th 2002, the Polish Data Protection Authority hosted peer review evaluation missions with support from the EU Technical Assistance Information Exchange Office. The missions covered the short-term technical assistance needed to implement and enforce Poland's strengthened data protection law, and the administrative capacity required to enforce it.

Contact: Igor Kowalewski – International Relations Officer, Biuro Generalnego Inspektora, Ochrony Danych Osobowych, Pl. Powstańców, Warszawy , 1 00-030 Warsaw, Poland
Website: www.giodo.gov.pl

ROMANIA

Three laws govern data protection in Romania:

1. Law no 677/2001 regulating the protection of persons concerning the processing of personal data and the free movement of the data (effective December 12th 2001),

2. Law no 682/2001 concerning the ratification of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (effective November 28th 2001), and

3. Law no 676/2001 concerning the processing of personal data and the protection of privacy in the telecommunications sector (effective March 14th 2002).

The first law (no 677/2001) guarantees and protects the right to privacy when processing personal data, and covers both computerised and manual records that form part of a relevant filing system.

The law governs processing carried out by Romanian or foreign organisations in both the public and the private sectors, and by data controllers established in Romania, or Romanian diplomatic missions or consular offices abroad. Also, the law covers processing by controllers not established in Romania, but using any transmission means that involves transit through Romanian territory. The law does not apply to:

• natural persons processing personal data exclusively for their own interests, and

• personal data processed and transferred in the frame of national defence and security, within the limits and restrictions stated by the law.

The right of access to information is stated by Article 31 of the Constitution of Romania and by the Law no. 544/2001 on freedom of access to information in the public interest, which took effect December 23rd 2001.

That law states that any person has the right to ask for and to obtain from public authorities and institutions, within the scope of the law, information in the public interest. The law includes a wide range of exemptions, such as records relating to:

• National defence, security and public order documents that are classified, and deliberations by public authorities;

• Discussion regarding the economic and political interests of Romania that are deemed to be classified information;

• Information regarding commercial or financial activities, if publishing the details will violate fair competition principles, and

• Procedures in criminal or disciplinary inquiries, should disclosures be prejudicial to the case; reveal confidential sources; endanger the life, physical integrity, or the health of a person; violate the guarantee of a fair trial, or damage the legitimate interest of any party in litigation.

The express or implicit refusal of a public authority employee, nominated to enforce the provisions of this law, is considered an infringement that can lead to disciplinary measures. Individuals who consider that a public authority has violated those legal rights may file a complaint at the administrative court of law (tribunal).

Contact: Professor Ioan Muraru, People's Advocate
Data Protection Directorate
Boulevard Iancu de Hunedoara no 3- 5 District 1
Bucharest ROMANIA
avp@avp.ro
Tel: + 40 21 231 5008
Fax + 40 21 231 5004
Website: www.avp.ro (in Romanian)

RUSSIAN FEDERATION

The Federal Law on Information, Informatisation and Protection of Information (adopted February 1995) requires the state (among others) to protect all forms of information. Information containing state secrets is exempted from this law and is governed mainly by the Federal Law on State Secrets of July 21st 1993.

The 1995 law establishes stricter requirements for state bodies' information resources. The state guarantees public access to certain types of information, including information of public importance. Access to the information is a civil rights objective under the Civil Code.

The Civil Code (in Article 139) generally defines commercial secrets as information that has real or potential value when not available to third parties, to which there is no free access on legal grounds, and that the owner of information takes measures to protect. Persons who gain access unlawfully to a commercial secret must cover incurred losses (such as actual damages and the loss of a competitive edge).

The same principle applies to employees and third parties in civil proceedings. The parties may list the information or state the criteria for considering it confidential, although it should be noted that certain corporate information may not be treated as confidential – for example, incorporation documents, licenses, tax payment information and annual reports.

Employees who disclose confidential information may be sanctioned by dismissal (Article 81.6 of the Labour Code) and/or by criminal liability (Article 183 of the Criminal Code).

Article 29 of the Constitution provides that everyone has the right to freely seek, receive, convey, produce and disseminate information (excluding state secrets) by any lawful means. It also guarantees freedom of the mass media. The law on the media, adopted in 1991, spells out press freedom in greater detail. It covers such issues as the status of media and journalists, freedom of the press guarantees, limitations on dissemination of information and state regulation of the media industry.

Privacy laws

The Constitution of the Russian Federation (Article 23) states that everyone has the right to privacy, including personal and family privacy and protection of his/her honour and goodwill. This specifically includes privacy of correspondence, telephone conversations, mail, telegraph and other communications, except when required by a court decision. Article 24 prohibits gathering, storage, use and dissemination of private personal information without the individual's consent. State and municipal bodies and officials must enable everyone to gain access to official documents and materials that directly concern their rights, unless otherwise provided by law.

The Russian Federation draft Law on Information of Personal Character, and the Law on the Right to Information, based on the Council of Europe Convention 108, have been on the Russian parliamentary (Duma) agenda for several years. However, it may take some time before they come into force. Once adopted, the laws will establish a regulatory body governing personal data protection and complete the basic legal framework for protecting personal data in Russia. The effectiveness of these laws, and of the almost 500 others dealing with information protection in Russia, will depend on their applicability to each of the recently introduced SORM directives (which regulate the media, archival protection and state secrets), in addition to further amendments to the legislation foreseen by the draft Law on Information of Personal Character and Law on the Right to Information.

The Duma has yet to consider some of the legislation and substantial changes to the drafts are expected.

Report submitted by
Kathryn E. Szymczyk
and Oxana Iatsyk,
Gowlings International, Inc.,
14 Prechistensky Pereulok, 4th Floor,
Moscow, Russia 119034
Tel: +7 (0)501 787 2070

SLOVAKIA

The Slovak freedom of information legislation (Act no. 211/2000) came into effect on January 1st 2001.

The basic principle of the act is "everything that is not secret by law is public." The principle requires that officials' discretion be kept to a minimum. Exceptions are clearly defined by other laws governing personal data protection and state secrets.

The act regulates the terms, procedures and scope for access to information. A wide range of organisations are obliged to provide access to information, including public authorities, organisations managing public funds, and any organisations/individuals that have been given the legal power to make decisions on the rights and responsibilities of individuals/organisations in the area of public administration.

The authority must not provide access to the requested information if the law deems it a state or professional secret (or subject to protection of information by encryption) and the applicant is not authorised to access the information.

Personally identifiable information (which includes personal letters, sound and image recordings) relating to an individual or his/her views shall be provided only if so stipulated in a special act or with the prior consent of the individual. Should the individual have died, a relative or close friend may give consent.

The authority must provide information on an individual's personal data processed by information systems as set out under the conditions of a special act only if stipulated by a special act, or if the individual has given prior written consent. Should that person be legally incapacitated, an appropriate legal representative may give consent. If the person is dead, a relative or close friend may give consent.

Contact: Zuzana Babicova – Lawyer
Urad vlady SR Nam. Slobody,
1 813 70 Bratislava, 1 Slovakia
Tel: +421 (0)2 593 79 261
Fax: +421 (0)2 593 79 266
E-mail: Zuzana.Babicova@pdp.gov.sk
Website: www.dataprotection.gov.sk
(in Slovak)

Part two of PL&B International's data protection roundup was compiled by Judith A Sullivan. For the first section of the roundup, see PL&B Int, Jan 2002, p.8.

The PL&B editorial team wishes to express its appreciation to all the contributors who gave their time and effort to making this feature possible.

Reference to further information about each country is available in the index published anually by Privacy Laws & Business and in the newsletter section of the Privacy Laws & Business website (www.privacylaws.com) where, in both cases, references are given by country, subject and by company.