INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

BCR mutual recognition club of nine formed

Agreement will expand use of BCRs.
By **James Michael**.

After its meeting on 1 October, the EU Article 29 Data Protection Working Party announced that nine countries have agreed to give mutual recognition to approval of Binding Corporate Rules for Data Protection. The countries are France, Germany (federal and Länder), Ireland, Italy, Latvia, Luxembourg, the Netherlands, Spain and the UK. The countries have agreed to recognise BCRs sent to them through the BCR coordination procedure.

Mutual recognition is a policy commitment rather than a legal change, as the countries' legislative systems are all based on the Directive. The essence of mutual recognition is that the DPAs commit themselves that once the Lead Authority circulates a consolidated draft with a positive opinion that it meets the required standard, other DPAs accept this opinion as sufficient basis for providing their

Continued on p.3

China to pass DP law to strengthen information industry

This report is based on a speech by **Zhou Hanhua** at this month's 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg, France.

Although China has been stepping up privacy law-making in recent years, such as the incorporation of a privacy protection clause into the Penal Code Amendment (draft) (see p.8), there is no doubt that there is a big gap between China and developed countries (especially the EU countries) in this regard. For this reason, we have been pushing for relevant initiatives, including the drafting of a unified Personal Information Protection Law (*PL&B International*, February 2008, p.1, and April 2008, p.11).

According to our experiences and observation in recent years in China, we do believe that privacy protection is an asset rather than an obstacle for economic growth. The reasons are as follows:

Firstly, the emerging of the information society makes the importance of information resources, including personal information, more and more obvious and crucial. However, lack of protection of personal information has hurt the confidence of the public and this will influence the free flow of information. Currently, due to a lack of confidence, many individuals do not like to provide true personal information. The *People's Daily* made a survey last November regarding

Continued on p.3

Issue 95 **October 2008**

NEWS

ANALYSIS

LEGISLATION & REGULATION

MANAGEMENT

INTERNATIONAL newsletter
ISSUE NO 95 October 2008

EDITORIAL DIRECTOR & PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

EDITOR
James Michael
james.michael@privacylaws.com

DEPUTY EDITOR
Laura Linkomies
laura@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

NEWSLETTER SUBSCRIPTIONS
Glenn Daif-Burns
glenn@privacylaws.com

CONTRIBUTORS
Zhou Hanhua
Chinese Academy of Social Sciences, Beijing
Hans Gliss
Beratungsbüro Gliss & Kramer KG, Germany
Whon-Il Park
Kyung Hee University, South Korea
Pablo A Palazzi
Allende & Brea, Buenos Aires, Argentina
Peter Ford
Australian National University
Chris Connolly
Galexia, Sydney, Australia
Claro Parlade
Parlada Hildawa Parlada & Eco Law, Manila, the Philippines
Eugene Oscapella
PL&B Consultant
Stuart Lynch
PL&B Consultant

PUBLISHED BY
Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200, Fax: +44 (0)20 8868 5215
Website: www.privacylaws.com

The *Privacy Laws & Business* International Newsletter is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of the newsletter. Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given. No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior permission of the publishers.
Design by ProCreative +44 (0)20 8429 2400
Printed by Hendi +44 (0)20 7336 7300
ISSN 0953-6795

comment

Self-regulation is not enough

The commissioners of privacy and data protection have met again (for the 30th time) and called, in a sort of Montreux II resolution, even more vigorously for globally enforced standards of data protection. Self-regulation, they said more emphatically than ever, is not enough, in the resolution at the end of their 15-17 October conference in Strasbourg (p.10). Whether the global standards are to be those of the European Union Directive and Council of Europe Convention (which non-European countries are now invited to join, *PL&B International*, August 2008, p.1), or the APEC model, the commissioners did not specify. There are 60 of them, after all, and some lean more towards Europe, and some towards APEC. The Convention is changing and may soon have an independent commission of its own (p.5). Consider the argument that those critical of the APEC model do so on the basis of "myths" about it (p.11), and compare another Asian regional model for data protection (p.13), one member of which, the Philippines, is very close to adopting a European-model law (p.17).

In the European region, the increasing use of Binding Corporate Rules takes a major step with the formation of the Group of Nine countries to give mutual recognition to each other's BCRs (p.1), although there are still obstacles to a Euro-wide BCR system (p.23).

News of failing financial institutions worldwide tends to overshadow the virtual flood of data breaches that can lead to expensive fines and onerous compliance (p.4). The commissioners also resolved that social networking websites should remind users that future employers may be looking at the youthful postings of job applicants (p.10). This point is illustrated by the example of would-be lawyers in the US. Everyone can learn from the comment on a survey that "What you put on a social networking site… [is] not very likely to get you into a law school, but it could keep you out."

PL&B is proud to introduce our correspondent from China, Professor Zhou, who reports (on p.1) on developments in that country and, perhaps more importantly, on the reasons for change there. He says: "In China, we do believe that privacy protection is an asset rather than an obstacle for economic growth," and "Personal information protection is one of the pillars of economic development."

James Michael, Editor

Contribute to PL&B newsletters

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact James Michael on Tel: +44 (0)20 8868 9200 or e-mail james.michael@privacylaws.com.

China: leaking personal data crime proposed

Selling or illegally disclosing personal data in China could become a criminal offence under a draft amendment to the Criminal Law.

The amendment was submitted on 25 August to the Standing Committee of the National People's Congress (NPC). Staff with access to personal information, such as those working in government offices, financial, medical and educational institutions and transport, and communications departments, who sell or leak personal data, could face up to three years in jail. People who illegally obtain personal data would also incur criminal penalties.

Personal reputation and privacy are protected under the general provisions of China's civil law, but personal data, especially mobile phone numbers and consumption records, are often leaked.

People often receive anonymous ad text messages on their mobile phones. According to a national survey by *China Youth Daily* in December 2007, more than 90% of Chinese people worry that their private details are too easily divulged and misused, and 74% of 4,003 respondents said there should be tougher laws on privacy infringement.

• *Source:* China Daily.

HK Commissioner overruled on air crew data

On 28 August Cathay Pacific Airways won a Hong Kong court battle over its policy of requiring cabin crew to release personal medical histories or face disciplinary action. Two High Court judges overturned a decision against the airline by the privacy Commissioner.

The Privacy Commissioner for Personal Data, Roderick Woo Bun, had earlier (*PL&B International*, February 2007, p.15) found that Cathay acted "unfairly" by asking staff with high records of absence to supply evidence of their medical condition, and ordered the company to halt the practice.

The judges said both the Commissioner and the Administrative Appeals Board had based their findings on an "incorrect construction" of the true meaning and intent of the Personal Data (Privacy) Ordinance, which says personal data may be collected by lawful and fair means. They said the Commissioner should have taken into account that Cathay has a duty in law to monitor the health of its cabin crew, and that the collection of medical data sprang directly from that duty and the data sought was not excessive.

"More than that, he [the commissioner] would also have taken into account that the means employed were lawful."

The judges also cited an example of workers in a nuclear power station who may be asked to attend regular medical checks and to disclose the results to ensure they are not contaminated by radiation to protect both the interest of the employee and the public. Equally, the airline is under an obligation to ensure all cabin crew are medically fit when on duty.

"In our view, in circumstances when disclosure of personal data is properly rendered mandatory, it is necessary to advise the data subject of the adverse consequence of failing to disclose, that advice does not thereby constitute a threat or the exertion of undue influence.

"In this regard, it is to be remembered that Cathay's disciplinary procedures are not only for the protection of Cathay's interests but ensure also that a member of the cabin crew staff is not in any way prejudiced in his or her employment without a full and fair investigation."

South Koreans fear for privacy in a stranger's call

Many South Koreans will hang up on receiving a telephone call from a stranger because most such calls are spam messages for direct marketing. Sometimes, a stranger's voice horrifies hearers because he or she seems to inform them of a traffic accident involving the hearer's children. The caller usually demands that some amount of money be sent immediately to a certain bank account owned by a hospital for quick treatment or dispute settlement. This is a notorious method of swindling called "voice phishing", based on the knowledge of the name and telephone number of a victim. Recently South Koreans are getting more and more sensitive and nervous about their personal information kept and used by a third party.

Leakage of personal data

It is an everyday incident. In early September, DVDs containing more than 11 million customers' names, residence registration numbers, addresses and telephone numbers were found in a trash box in Seoul. They were found to have leaked from the database managed by a data processing company dealing with GS Caltex gas stations. A few days later, the suspects were arrested by police. They admitted having planned to blackmail the company. Five months ago, a database of over 10 million customers of an Internet auction company was found to have been snatched by a foreign hacker for unlawful use.

As a result, those victims are seeking appropriate compensation with the help of lawyers. In Korea, where class actions are not allowed, except in the limited case of securities fraud, only those participating in lawsuits could be provided with judicial redress. It has become a social phenomenon for a lawyer or law firm to establish an Internet site inviting lawsuits against those businesses which mismanage or misappropriate customers' personal

information.

At present, a number of lawsuits against GS Caltex and its data processing subsidiary have been filed in a Seoul court for damages up to one thousand dollars per victim. Until now the courts used to order reasonable damages to be given to the victims for mental distress even with no evidenced actual damage.

Another stranger's call causing fear

Nowadays a stranger's call might come from a lawyer's office. They say, "Your MP3 files or pictures posted on your homepage have infringed upon the copyright of our client" or "Your replies added to an Internet bulletin board have violated cyber-defamation law" and so on. They asked a handsome amount of money for an out-of-court settlement.

Sometimes a policeman might call, claiming the person answering did wrong by posting vicious messages on the Internet or making unwanted calls to innocent businessmen. At the beginning of September, an entertainer committed suicide allegedly because of the failure of his business. However, it was pointed out that a number of netizens may have conducted cyber-terror because his wife, a TV/FM radio personality, allegedly criticised the candle-light demonstrators concerning US beef imports during her program. Angry netizens demanded she quit the TV/radio programmes on the broadcasting company's Internet bulletin board and that sponsors stop the advertisement for her program. Some of them actually conducted a boycott campaign against the entertainer couple's businesses. It is said that the netizens' organised campaign amounted to cyber-terrorism toward the couple, and it may have led to his suicide.

Against these backdrops, the ruling party is considering amending the current law in order to punish those who intentionally and habitually post vicious messages on the Internet and violate the cyber-defamation law, in addition to the existing fines for such violations. But this initiative is stirring controversy over constitutional freedom of speech. The media and public opinion criticise and oppose such legislation. Critics say the government is attempting to control the Internet, and thus control the media. The issue is unresolved.

Corporations are on the alert for data protection

As a large-scale leakage of customers' personal data poses not only unexpected risk to business operations, but also punishment of top management, corporations are increasingly on the alert for data protection.

They pay careful attention to the security of membership registration on the Internet against possible hacking or other incidents in cyberspace. For example, it is increasingly the case that encryption of personal information databases is required and personal storage devices like USB sticks or laptop computers are prohibited from being carried off the premises.

As the numbers of victims and damages increase, more corporations seem to be on the alert for information security.

AUTHOR

Whon-il Park, Associate Professor of Law, Kyung Hee University, email: onepark@khu.ac.kr

New Argentine regulations, new Uruguay law

In September the Argentina Data Protection Agency issued Disposition 5/2008 detailing the procedure to perform audits in data controller premises. The purpose of Disposition 5/2008 is to regulate how audits are going to take place and to describe their stages. Under this new regulation the data protection agency will send a note with a questionnaire to the company several days before the inspection. In a later stage, the DPA could visit the premises and request access to the databases and verify compliance with security regulations, registrations and other requirements of the law.

The Data Protection Agency also has approved at Disposition 7/2008 the "Guidelines for good data protection practices in personal databases of the public sector". The Guidelines explain the application of data protection rules in public sector databases. The Guidelines also include a sample confidentiality agreement for the public sector. In these Guidelines, the DPA also explains the relationship between data protection law and the freedom of information regulations. The agency has postponed the deadline for security measures. By Disposition 9/2008, the deadline to implement medium and critical security measures under the data protection law and its regulations (Disposition 11/2006) has been postponed for one year. Basic security measures were not postponed. In addition the DPA has published a document that can be used as a template to implement the Security and Privacy Policy that each data controller must have already in place.

Uruguay's new DP law

The law was approved by the Senate on 16 July 2008 and finally enacted by the Executive Power in August 2008. The law is based on the European model of data protection laws. It contains a full set of data protection principles including consent, notices, limitations on certain transfers of personal data and a provision banning the transfer of personal data to destinations lacking adequacy. Finally there are special provisions for sensitive data, commercial and credit reports, telecommunications data, and marketing and outsourcing services. The law also creates a regulatory authority in charge of applying the law and policing databases.

The adoption by Uruguay of EU-modelled privacy protection standards consolidates a trend in the region: Argentina, Chile, Colombia, Paraguay and Peru have all adopted similar legislation. Only Argentina has so far been accepted by the EU as providing "adequate" protection. Uruguay is likely to apply soon to the EU for a determination that its law is "adequate"