INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

France's CNIL to conduct more audits and step up enforcement

400 inspections expected in 2011, most in the private sector. **Julia De Oliveira** reports from Paris.

Yann Padova, Secretary General of the *Commission nationale de l'informatique et des libertés* (CNIL), France's Data Protection Authority, announced details of the commission's new enforcement strategy for the coming year, at *Privacy Laws & Business* Privacy Officers' Network (PON) Roundtable in Paris on 6 April.

CNIL audits have increased from around 100 in 2005 to an expected 400 in 2011 and will continue to increase. Padova listed video surveillance and health data as its top priorities for 2011. The CNIL aims to carry out at least 150 inspections in the area of video surveillance, given its stronger powers in the area following adoption of a new law on 14 March this year. In relation to health data processing, the CNIL sees the

Continued on p.3

EU Justice Commissioner outlines DP reforms

By **James Michael**.

In three speeches in March, Viviane Reding, Vice-President of the EU Commission and Justice Commissioner, gave more indications about what will replace the EU DP Directive. It seems increasingly clear that there will be at least one Regulation to replace the Directive, with greater use of EU-wide Binding Corporate Rules (BCRs), and less compulsory notification of data processing.

On 16 March she said that reform of data protection rules was her "top legislative priority."

To enhance individuals' control over their own data, she said that peoples' rights need to be built on four pillars:

1. the "right to be forgotten";
2. transparency;
3. privacy by default; and
4. protection regardless of data location.

Continued on p.5

Issue 110 **April 2011**

and the US global standard setters and the world compass for values in action."

Consistent application of EU law

In another speech on 31 March to the European People's Party (EPP – the largest political group in the European Parliament) called "Who pays for Data Protection?", she commented that the US "do not track" initiative and the announcement of "a privacy bill of rights" were signs "very clearly that the US is approaching the EU regulatory model." She also gave more hints about what will replace the Directive. In order to "help businesses to cope with high data protection standards" she set out five priorities.

The first is to "reduce this fragmentation [of national data protection laws] and increase the harmonisation of data protection rules within the EU." This almost certainly increases further the likelihood of a single uniform Regulation rather than another Directive.

The second is to increase "trust if you want to open market possibilities for a product and reach consumers by gaining their acceptance." As she attributes citizens' "lack of trust in the digital environment and fears about possible misuse of their data" to the "current inconsistent application of EU law", this also points toward a Regulation.

Third, she wants to "create a one-stop shop for all cross-border businesses by simplifying the rules of applicable law" avoiding the "simultaneous application of different laws to a same company active in several Member States." This sounds like a Regulation to extend the Binding Corporate rules Club from the present 19 to all 27 EU Member States.

Her fourth proposal "to facilitate international data transfers and to streamline and improve the procedures for exporting data" would be done by "expanding the scope of…intra-business rules to 'groups of companies' and introducing "intra-company standards rules officially in the new legislation", particularly by "introducing the 'mutual recognition' principle: once approved by a data protection authority in one Member State, the standard would be automatically recognised in other Member States." This further points to EU-wide BCR recognition, which would be extended to groups of companies.

Her fifth pro-business measure is to cut red tape, and to "drastically simplify the current system of notifications to data protection authorities. The general obligation to notify data "This would adopt at EU level the trend already noted in several states to reduce or abolish the general notification duty, although "…concerning the more delicate personal data, there will be still rules in place."

Publication of the detailed plans for replacement for the 1995 Directive is expected in November/December this year.

Korea adopts new DP Act and prepares for implementation

By Professor **Whon-il Park**.

Since 2004, there has been much talk but little action regarding a new data protection bill. Finally, a new full-fledged Data Protection Act has been promulgated (29 March, 2011), and will come into force on 30 September 2011. In the intervening six months, both the entities regulated, and the public, will prepare for the changes to the law.

The new Act will replace the existing Public Agency Data Protection Act in whole and the Act on Promotion of Information and Communications Network Utilisation and Information Protection, etc. in part. Until now, these two acts have provided for data protection in the public and the private sector, respectively.

Preparing for change

When the new Act is implemented, more than 3.5 million public entities and private businesses will be regulated in relation to the collection and use, processing and destruction of personal information by common criteria and principles. But a number of changes in regulation and practice will mean that these entities and businesses will need to be alert and to watch out for any possible violation of the new law. So the government is going to make the changes public during the preparation period prior to its enforcement.

In this respect, the Ministry of Public Administration and Security (MOPAS) is setting up a task force team for the implementation of the new law, and a DP Working Group composed of scholars and specialists well-versed in privacy policy and technologies. The task force team will be assigned to make implementation rules and regulations, upon the advice and suggestions made by the DP Working Group, and will also help establish the Data Protection Commission and the Secretariat.

In order to effectively enforce the new Act, the standardised processing of personal information and universal identifier, and implementation guidelines, the Data Protection Framework is to be revised every three years and its Action Plan will be worked out in due course. Also the explanatory guidebook regarding the new Act will be published along with promotional seminars.

Eight major changes in the new Act

The new Act will usher in important changes in data protection as follows:

First, all data processors, regardless whether public or private, will be regulated by the new Act. The Act will cover not only personal information electronically processed but also that which is manually processed, which have been beyond the scope of application of the existing laws.

Second, the Data Protection Commission, composed of 15 members including one chairperson and one standing commissioner, will be established under the Presidential Office, like the National Human Rights Commission. It will deliberate on important policy issues and laws and regulations on privacy and data protection, functioning independently within the government organisation.

Third, standardised safeguards for personal data in the course of collection, use, transfer to a third party, and destruction will be formulated. In particular, sensitive data and universal identifiers like the resident registration number, as regulated by the law, will be prohibited in principle without the specific consent of data subjects or authorisation by the law. Therefore, a data processor, as regulated by Presidential Decree, will be required to provide an alternative ID for the sign-up of users on its website.

Fourth, notification to the data subject will be required of the source of personal data other than the data subject. Data processors conducting marketing based on their own database are required to obtain the data subjects' consent in an explicit manner. Data subjects shall be notified of the option of refusing consent to collection or processing, and no disadvantage in case of refusal is allowed.

Fifth, visual data gathering devices like CCTV may be installed in public places only for the purpose of prevention of crime. Furthermore, in case of potential danger to data protection in the public sector, a Privacy Impact Assessment (PIA) shall be conducted by public institutions. The private data processors engaged in the build-up or expansion of personal data files, deemed to affect data protection, are encouraged to make such PIAs on a voluntary basis.

Sixth, data breach notification to the affected data subjects will be compulsory, while significant data breach beyond a certain scale shall be reported to the authorities concerned. And the data processor's efforts necessary to minimise the side effect are required. In this regard, any data subject complaining that his/her right or interest has been infringed upon by a data processor may report such infringement to MOPAS.

Seventh, the Personal Information Dispute Mediation Commission will cover both public and private sector disputes. Also collective mediation procedures may be invoked in consideration of large scale but minimal damages to data subjects. In addition, a consumer organisation's representative lawsuit will be allowed, but only for the suspension or injunction of activities infringing upon privacy and data protection subsequent to the mandatory collective mediation procedures. This is to avoid an avalanche of representative lawsuits.

Prospects

Whether the long-awaited law will be a champion of the citizens' right to privacy or an obstacle to businesses depends on the preparation for, and enforcement of, the new Act. But it is a long-awaited landmark in the development of data protection in Korea.

Editor's note: Specific aspects of this very important new legislation, such as data breach notification, will be examined in more detail in future issues.

AUTHOR

Whon-il Park is Professor of Law at Kyung Hee University, South Korea.

Changes to Spanish penalties

The Law of Sustainable Economy, in force since 5 March, introduced changes to the penalties provided by the Personal Data Act.

The amended law divides infringements into three categories; minor, serious or very serious. Serious infringements include obstructing the rights of access or rectification, or transferring personal data to countries without adequate level of protection.

Fines for minor infringements vary from €900 to €40,000. The DPA can impose fines between €40,001 to €300,000 for serious infringements, and very serious infringements can be punished by fines amounting up to €600,000. The Spanish Data Protection Agency believes that the reforms will provide greater legal certainty and help bring about greater accuracy in the application of the law.

- Later this year, or next, *PL&B's* Privacy Officers Network may organise a Roundtable in Spain to discuss these changes to its data protection law and their impact on business. If you or a colleague are interested, email glenn@privacylaws.com with "Roundtable in Spain" in the subject line.

Portugal's DPA implements electronic notification

Following the announcement by Portugal's Data Protection Authority – the *Comissão Nacional da Protecção de Dados* (CNPD) at *PL&B*'s Privacy Officers Network Roundtable on November 24 and 25 last year, the CNPD implemented, on 13 January, an electronic notification system for personal data processing.

On the website of CNPD at www.cnpd.pt, there are two electronic forms available – one of them specifically for notifications regarding the installation of a video surveillance system and another more generic one for all other data processing work.

The general form covers a wide range of fields, such as human resources, insurance, banking, telecommunications, pharmacovigilance, health and marketing, reports Baptista, Monteverde & Associados, a law firm in Lisbon.