INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Data breach notification duty added to Austria's DP Act

Dr Rainer Knyrim explains what this new provision means to organisations. Will Germany and Austria set a trend for Europe?

As Austria follows Germany in amending its data protection law to include a specific data breach requirement, the EU is also following this path (p.6) and France may do so. Other countries' DPAs, such as Denmark, are already interpreting their data protection laws' security provisions to require breach notification.

Austria's Data Protection Act 2000 (ADPA) has seen its biggest amendments since its introduction in 2000. These include the introduction of an explicit Data Breach Notification Duty which came into force on 1 January 2010 as well as provisions on video surveillance, and more and stronger powers for the Data Protection Commission (also in force since 1 January). Furthermore, a fully computerised and completely automated notification system will be introduced for the Austrian Data Processing Register by 1 January 2012.

Breach notification duty

Austria is the second country in the European Union after Germany to

Continued on p.3

France to discuss mandatory appointment of DP officers

Nathalie Métallinos looks at the role of the *Correspondant* under the current law and the advantages and disadvantages associated with this proposed change in the law.

On 6 November 2009, Senators Yves Détraigne and Anne-Marie Escoffier introduced a private member's bill[1] into France's Senate that would impose the obligation to appoint a Data Protection Officer (DPO) in each government body and most[2] large private sector companies.

This measure is accompanied by other substantial proposed amendments to France's Data Protection Act of 1978[3]: a general obligation to notify security breaches, increased transparency of data processing, prior information on retention periods, increased civil penalties by the CNIL and systematic publicity given to the CNIL's sanctions.

The bill also addresses the question of IP addresses and cookies. IP addresses, defined as "any address or identifier of the terminal equipment connected to a communication network" would be expressly qualified as personal data and an express consent (opt-in) regime would be required for cookies unless they are needed for communication purposes or to permit access to an online

Continued on p.4

Issue 103 **February 2010**

INTERNATIONAL newsletter
ISSUE NO 103 FEBRUARY 2010

PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

EDITOR
Laura Linkomies
laura@privacylaws.com

LEGAL EDITOR
James Michael
james.michael@privacylaws.com

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

NEWSLETTER SUBSCRIPTIONS
Glenn Daif-Burns
glenn@privacylaws.com

CONTRIBUTORS
Dr Rainer Knyrim
Preslmayr Attorneys
Nathalie Métallinos
Société Générale
Mili Bach
Israel's Law, Information and Technology Authority
Tanguy Van Overstraeten and Richard Cumbley
Linklaters LLP
Julia de Oliveira
Consultant
Dan Cooper
Covington & Burling LLP
Dr Hiroshi Miyashita
Surugadai University, Japan
Whon-il Park
University of Seoul, South Korea
Hong Xue
Beijing Normal University

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 Printflow Ltd +44 (0)20 7689 8697

ISSN 0953-6795

comment

Data breach notification creeps across Europe

The new duty for organisations in Austria to notify individuals of data breaches (p.1) follows Germany last year and broader plans at EU level. In the US, the Congress may adopt a federal data breach law (p.21).

European Commissioner Viviane Reding clearly supports revision of the EU Data Protection Directive (p.6). Areas needing new rules include transfers of personal data from the European Economic Area to non-adequate countries. Adoption of the Lisbon Treaty paves the way for changes in the directive's scope, as our Legal Editor, James Michael explained when giving evidence on European issues to the UK House of Commons Justice Committee on 19 January, (see www.parliamentlive.tv/Main/Player.aspx?meetingId=5641).

We continue to watch closely Asia-Pacific developments: the government's plans to amend Australia's DP Act (p.15), change to a consumer supervisory authority in Japan (p.22), progress towards more class actions in South Korea (p.23), recognition of privacy as a civil right in China (p.24), and plans for ID cards in India (p.25).

We report from Washington DC on Safe Harbor developments (p.11) and ask: how far is the system working? There are no plans to use this Safe Harbor model in any other country. It would be helpful if the EU's Data Protection Working Party gives adequacy opinions on more countries following its positive opinions on Israel and Andorra (p.8). Israel's DP Authority has a formidable enforcement model (p.9) of conducting an investigation as a criminal investigation and imposing a fine if necessary. An organisation can accept the DPA's decision and pay a fine or challenge the evidence, refuse to pay, and face a criminal proceeding in court.

Progress has been made on EU controller-processor model contracts, approved by an EU Commission decision (p.10) on 5 February. This is a welcome decision that will provide for more flexibility for global processing and outsourcing.

Another issue that concerns companies operating both in the US and the EU, is e-discovery (p.17). Which legislative regime should you follow if caught in this jurisdictional conflict?

Stewart Dresner, Publisher
PRIVACY LAWS & BUSINESS

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 Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

policy for the service:

1) Google will consult with the local governments before they start the service.
2) Google will establish a contact point so that the residents can ask the Google to erase the pictures or images.
3) Google will take images from a lower level (2.05m; it used to be 2.45m).

This reaction against the Google Street View service has now calmed down, but the service stimulated a discussion about views towards privacy and sensitivity in Japan.

• *This article does not represent the official government view.*

AUTHOR

Dr Hiroshi Miyashita
Advisor for the Office of Personal Information Protection, Consumer Affairs Agency, and Lecturer, Faculty of Law, Surugadai University
Email: hmiyashita@surugadai.ac.jp

Wind of change in privacy cases in South Korea?

A hacker accessed 10.8 million records on an e-commerce website. But the courts do not yet accept a class action by the affected individuals. By **Whon-il Park**.

Two years ago, Internet users in South Korea were surprised to hear the personal information of some 10.8 million users of Auction, Korea's largest e-marketplace, was leaked by a hacker. The Cyber Terror Response Center of the National Police Agency disclosed that a user with an overseas IP address had hacked into the company's website by using a computer worm.

The damage to Auction users could be immense, as the leaked personal data included names, residence registration numbers, telephone numbers, and, in some cases, bank account details. But Auction's response was swift, contrary to expectations. Auction urged the affected users to change their IDs and passwords as soon as possible, and to be cautious in using their existing telephone numbers and bank accounts.

Lawyers became busy in encouraging the victims to join their actions for damages up to 150 billion won (U$133 million). The lawyers promoted massive lawsuits against Auction in Internet cafes and blogs. The plaintiffs eventually exceeded 145,000.

On 14 January 2010, the Seoul Central District Court ruled that Auction is not to blame. The court ruled, "There's no evidence that Auction was lenient about its security measures against hacking." The court added: "It was not legally mandatory for companies to set up firewalls for their websites, considering that there was low credibility over installing firewalls among businesses at that time." Also, the court was believed to have taken into account how Auction swiftly handled the incident to prevent a possible attack in the future.

The final result of the Auction case must wait for the higher courts as a number of victims are willing to appeal. The appellate court, however, needs to consider the following questions:

(i) Have the Internet service providers (ISPs) observed the managerial and technological measures required by the relevant laws to safeguard the personal data? In particular, have ISPs established reliable firewalls and other security measures against possible hacking incidents?
(ii) Does it cost too much to install anti-hacking technologies in view of the latest hacking skills?
(iii) Have ISPs discharged their duty to prevent possible attack or threat in the future?
(iv) How many users are affected by the incident and how large could the actual damage to the victims be?

There are similar cases before the court. One is the action for damages against GS Caltex where employees of a GS-affiliated data processor leaked personal information of customers for profit. Another one is the case where a mobile telephone company, formerly Hanaro Telecom, transferred the list of seven million customers to a telemarketing company, and the angry customers filed a collective suit for damages.

> At present in South Korea, US-type class action applies only to securities fraud cases.

In the past, Korean courts used to rule in favour of users who sued a company for information leaks by hacking or secretly selling customers' data to others. So it remains to be seen whether the wind of change in this court ruling will prevail.

At present in South Korea, US-type class action applies only to securities fraud cases. So the data protection victims in this case had to file the lawsuits individually. The attorneys as well as the court need to confirm the plaintiffs one by one, and it took a huge amount of paperwork and time. Accordingly, to ensure full-fledged data protection and compensation for the victims, it will be necessary to introduce a real class action, where several representatives may file suit to compensate a class of victims of the same incident.

AUTHOR

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