global privacy roundup

AUSTRIA

The Austrian Direct Marketing Association (DMA) has introduced a 'Fair Data' quality assurance label to help organisations demonstrate good data protection compliance. The mark is part of the association's Code of Conduct, which is designed to provide practical advice for compliance with the EU Data Protection and Privacy and Electronic Communications Directives.

The quality label has been described as a model for the rest of the Europe by the Austrian DMA. However, the initiative has already been criticised. According to *Heise News*, Hans Zeger, an Austrian data protection expert said that the project leaves publicly available data without any protection. For example, personal data published in telephone directories will not be covered. Zeger said that publicly available data can only be used for the purpose it was originally collected for. Any deviation from this is a breach of the EU Data Protection Directive, and FEDMA's European Code of Practice.

The Austrian DMA has introduced the privacy mark primarily for the use of its members. Other organisations that wish to follow its Code of Conduct will have to pay a yearly subscription fee of €360 to be able to display the privacy label. The Code, published at the beginning of September, addresses the use of e-mail addresses and SMS for direct marketing, but does not give detailed advice on rules for opt-in/opt-out requirements.

For further information, see the Austrian DMA's website at www.dmvoe.at, www.argedaten.at, and www.fedma.org.

AUSTRALIA

In August, the Federal Privacy Commissioner, Karen Curtis, announced she would be conducting a consultation into the operation of the 1998 Federal Privacy Act.

The Commissioner is expected to publish a consultation document in October allowing interested parties a two-month period to submit responses. A final report on the Privacy Act is due to be released in March 2005.

In August, credit reference bureau, Baycorp Advantage, agreed to remove from its records, the details of 65,000 payment defaults supplied by failed telecoms operator One.Tel.

An investigation carried out by the Federal Privacy Commissioner's office found that although One.Tel was passing bad debt information to credit reference agencies, it did not have systems in place to notify changes once the debts had been repaid. Commenting on the case, Privacy Commissioner Karen Curtis said, "I commend Baycorp Advantage for taking positive steps to comply with its obligations under the Privacy Act to maintain the accuracy of its credit records by removing the questionable defaults listed by One.Tel."

CANADA

Canada's Federal Privacy Commissioner, Jennifer Stoddart, has called for greater dialogue over the transfer of personal data by public and private sector organisations to US-based service providers.

Her announcement in August, follows an investigation by the Privacy Commissioner for British Columbia, David Loukidelis, into concerns that US authorities could use US anti-terrorism legislation to access data on Canadian citizens. See www.privcom.gc.ca for more information.

FINLAND

Finland implemented the Privacy and Electronic Communications Directive on September 1st. The new law covers electronic marketing and unsolicited communications.

The law states that consent is needed, generally speaking, when sending e-mail or SMS messages for commercial purposes to individuals.

If the recipients are business subscribers, consent is not required. However, in cases where marketing is sent to a business e-mail address which includes the name of the recipient (eg. name.surname@company.fi), the address will be regarded as belonging to the employee, and therefore consent is needed. If the recipient is targeted because of their job function, permission is not required. Whether this argument can be used depends on the nature of the marketing message, the product that is being offered, and the source of personal data being used (the source of the data has to be disclosed).

The law allows for marketers to contact consumers on an opt-out basis (eg. the soft opt-in option) if the following conditions are complied with:

1. Personal data has been obtained in the course of a sale of a product or a service.

2. Marketing is conducted by the same company offering similar products or services.

3. There is the opportunity to opt-out from further contact at the point of data collection, and when the marketing material is received.

For more information, see the Finnish Data Protection Authority's website: www.tietosuoja.fi.

FRANCE

France finally implemented the EU Data Protection Directive on August 7th, through amendments to the 1978 'Loi Informatique et Libertés'. It entered into force immedi-

ately, except for those provisions which will require the adoption of ancillary texts, such as the provisions on appointing data protection officers. See cover story for more details on France's new law.

INDIA

India's IT trade association body, NASSCOM (National Association of Software and Services Companies) announced in September that it would be carrying out security and privacy audits on its members in a bid to allay concerns over outsourcing to Indian service providers. Consultancy and audit firms PricewaterhouseCoopers, Ernst & Young, and Deloitte & Touche have been retained to carry out the audits (see p.8 for more on outsourcing to India).

IRELAND

Ireland's Data Protection Commissioner has released guidelines on how to publish online privacy policies in compliance with the Data Protection (Amendment) Act 2003. The guidelines cover the content required in privacy policies, whether policies can be included in 'terms & conditions' statements, and when to review existing policies.

The guidelines can be found at: www.dataprivacy.ie/images/PrivStatementGuidelines.pdf

ITALY

Italy has decided to permit the bulk transmission of SMS messages in cases of emergency situations, such as natural disasters, or threats to public security and health. Telecoms operators are allowed to send messages in these exceptional circumstances without the recipients' consent. A decision of March 12th by the Italian Data Protection Authority (Garante) was followed by a press release in July stressing the circumstances that allow for this type of mass transmission have to be truly exceptional, and that recipients of the messages must be able to identify the sender. For more information, www.garanteprivacy.it.

SWEDEN

A recent decision by a Swedish court states that a company registration number represents personal data if an individual behind it can be traced. As reported in the Swedish Data Protection Authority's magazine *Direkt*, the case involved two companies producing a similar product. Company A found out that a competitor, company B, had illegally copied its products. Company A then made this information public on its website, and included the registration number of company B.

Because company B is a sole trader, its company registration number is the same as the owner's identity number. Therefore, publishing the number had wider consequences than just naming the company. Company B made a complaint against company A under the Swedish Data Protection Act. Company A responded that they had merely published a company registration number in order to inform customers, and this would fall under the journalistic purposes exemption.

The court's decision was that, in this case, there was a breach of the Data Protection Act as personal data had been published without consent. Although company A claims it published the information for journalistic purposes, there was also a commercial reason behind the decision to go public. Company A was ordered to pay a fine of 900 kronas (€100). For further information: www.datainspektionen.se.

UNITED KINGDOM

In August, a trade union representing workers at UK bank Lloyds TSB, lodged a complaint with the Information Commissioner questioning the legality of the bank's outsourcing operations. The complaint raised the issue of whether the transfer of customer account details to India violates the Data Protection Act's requirements on cross-border transfers. To date, it has not been made clear whether the Information Commissioner's office will fully investigate the complaint (see p.6 for full story).

UNITED STATES

In August, US Democrat senator Liz Figueroa received backing from the California legislature for a new state outsourcing privacy bill. The bill (SB 1451) will extend state privacy protection worldwide and allow consumers to enforce their rights in Californian courts.

Commenting on the bill, Figueroa said: "No one should be able to avoid responsibility for violating California law just because they're in another country. If they violate our privacy, it will be our courts that make sure they are brought to justice."

The bill has now been handed over to California's governor for final approval.

In September, Primus Telecommunications agreed to pay $400,000 (€330,000) to settle an investigation by the Federal Communications Commission (FCC) into unsolicited telemarketing. It was claimed that Primus breached US telemarketing regulations which bans commercial cold calling to consumers who sign up to a national Do-Not-Call registry. Since its launch in June 2003, the Do-Not-Call registry has received over 60 million registrations. There have been around 430,000 complaints relating to alleged violations.

A survey published in August by Privacy & American Business claims US consumers are increasingly likely to actively protect their privacy. The survey found that 87 per cent of respondents had asked companies to remove their details from their marketing databases, a 29 per cent rise from 1999. 81 per cent said they had requested companies not to disclose their details to other companies, compared to 53 per cent in 1999.

The survey also noted that most consumers are reluctant to register their details with companies unless they were confident their privacy would be protected. 65 per cent of respondents - representing 94 million consumers, according to Privacy & American Business – said they would not register with companies that had unclear or complex privacy policies.