

Data Protection Ireland

Volume 2, Issue 6

November / December 2009

Headlines:

- Data sharing provision provokes Hawkes to get tough, p.14
- Ireland “modest” with spammers, p.15
- 1 in 5 Irish business experience data leak, p.15
- Review Group’s consultation closes, p.16

Inside this issue:

Editorial	2
The interaction of data protection and FOI law in Ireland	3
Using ISO 27001 to develop a security awareness program	7
PCI DSS compliance — meeting the requirements	10
News & Views	14

Data retention memo agreed ahead of law’s enactment

The government has controversially agreed a memorandum of understanding (‘MoU’) with the communications industry on how to implement data retention legislation in Ireland, ahead of the legislation’s enactment.

The parties to the agreement are four major players from the communications industry, as well as the Commissioner of An Garda Síochána, the Permanent Defence Forces, and the Revenue Commissioners.

A version of the Communications (Retention of Data) Bill 2009 was leaked earlier this year. One of the provisions was that communications

companies will hand over “names and addresses” of IP address users, email senders, and VoIP users.

However, the memo states that the communications companies will hand over “any available personal details.” Concerns have been raised over what seems to be an extension of what has been proposed so far in the published data retention bill. It has also been said that the memo represents a blatant disregard for proper democratic legislative process.

Paul Durrant, Manager at the Internet Service Providers Association of Ireland Ltd, one of the parties to the agreement,

told *Data Protection Ireland* “the EU Data Retention Directive which is being transposed in Ireland as the Communications (Retention of Data) Bill 2009, contains quite broad wording. This law will be passed soon, and ISPs and Telcos here (as well as all over Europe) will have to deal with it from a practical perspective. Communications equipment can’t deal with vague terminology; it uses digital technology, 1s and 0s. Either something is to be retained or not.

“The ISPs, Telcos, and State Authorities have taken a simple, pragmatic, route in agreeing on an interpretation of the
(Continued on page 14)

Report reveals gaping holes in data security at Bord Gais

A report into the thefts of four laptops from Bord Gais (‘BG’) has found that BG had breached its responsibilities under the Data Protection Acts on a number of counts.

One of the laptop computers stolen from the Dublin offices of BG in June contained the personal data of 93,857 Bord Gáis customers. The laptop, which was unencrypted, contained

bank account numbers, home addresses, and branch details of people who had switched their electricity supply from ESB as part of BG’s “big switch” campaign. The Office of the Data Protection Commissioner (‘ODPC’) investigated the incident, and has produced its report detailing recommendations.

Amongst the recommendations are that an imme-

mediate review of all access levels among staff members is undertaken; that an appropriate standing governance structure be put in place; and that it be made “abundantly clear to all staff that personal data should not be downloaded to local drives”.

In a written response to the ODPC, BG Managing Director, David Bunworth, described actions that BG has taken since