Breach Notification Guidance

There is an increasing trend among organisations to contact the Office of the Data Protection Commissioner directly as soon as they become aware of unauthorised or accidental disclosures of customer or employee personal information. In the public sector, recent guidance from the Department of Finance on data security advises departments and agencies to report data breaches immediately to this Office.

The trend towards voluntary disclosure is very welcome as an example of good practice. Such disclosure allows us to advise the organisation, at an early stage, how best to deal with the aftermath of a disclosure and how to ensure that there is no repetition. It also allows us to reassure members of the public that we are aware of the problem and that the organisation in question is taking the issue seriously.

The Minister for Justice, Equality & Law Reform has convened a working group to advise him on issues related to data breach incidents. This working group is expected to report to the Minister in the coming months. In the meantime, this note offers interim advice to organisations on what we consider to be best practice in this area.

Data Breach – What to Do

As soon as you find out that personal data for which you are responsible has been compromised – for example, through loss of a portable device, misaddressing of mailings or a "leak" from your organisation – we recommend that, as part of your response, you immediately notify us by phone (1890 252 231) or email (info@dataprotection.ie).

The first issue we will consider with you is the question of informing those persons directly affected by the loss (if you have not already done so) and how this might best be done.

Depending on the circumstances, we may ask you to provide a detailed report of the incident, including:

- the amount and nature of the data that has been compromised;

- what action (if any) has been taken to inform those affected;
- a chronology of the events leading up to the disclosure; and
- a description of measures being undertaken to prevent a repetition of the incident.

We will investigate the issues surrounding the data breach. The nature of such an investigation varies from case to case, depending on the circumstances and seriousness of the data breach. The investigation may include an on-site examination of systems and procedures and could lead to the use of the Commissioner's legal powers to compel certain actions. However, this is very much the exception and the experience to date suggests that investigations are conducted on a co-operative basis with the entity keen to respond on a voluntary basis to any recommendations that we make.

"Prevention is better than Cure"

Informing your customers and us of a data breach is no substitute for the proper design of systems to secure personal data from accidental or deliberate disclosure. Our general advice on data security is here. But we accept that, even with the best-designed systems, mistakes can happen. As part of a data security policy, an organisation should anticipate what it would do if there were a data breach. Some questions you might ask yourself:

- What would your organisation do if it had a data breach incident?
- Have you a policy in place that specifies what a data breach is? (It is not just lost USB keys/disks/laptops. It is also inappropriate access to personal data on your systems or the sending of personal data to the wrong individuals).
- How would you know that your organisation had suffered a data breach? Do staff at all levels understand the implications of losing personal data?
- Has your organisation specified whom staff tell if they have lost equipment containing personal data?
- Does your policy make clear who is responsible for dealing with an incident?

- Does your policy include informing affected customers? How would you do this? What information would you give them?
- Has a point of contact been designated for the public should a data security breach occur?
- Does your policy include informing the Office of the Data Protection Commissioner and, if appropriate, other regulatory bodies?