

18th June 2010

Dear Commissioner,

Some Members of the Irish Computer Society and I met last week to discuss the draft data security breach code of practice. I am writing to you with our collective views. Members in attendance were employed in the health sector, third level education, central government, private sector HR and Security consultancy and the finance sector.

I hope you find this contribution useful. If you require further input please do not hesitate to contact me.

Yours sincerely,

Tom O'Sullivan.

General Observations

All in attendance welcomed the progress that had been made in publishing the draft code. The general conclusion of the group was that the intent of the code was good, however there are a small number of ambiguities and, in some areas, it did not go far enough. There was widespread agreement that resourcing within the Office of the Data Protection Commissioner will have a bearing on what is achievable, and a hope that this were not so.

The group was concerned that the exceptions to the reporting rule would allow repeated breaches to go unreported. A systemic failure in an organisation that resulted in repeated small breaches could go undetected by the ODPC unless reported by a third party. Also, as mentioned in the submission by ICS Members to the Review Group in December, relatively small breaches can have very serious consequences for data subjects. For these reasons, we recommend mandatory reporting in all cases.

There was agreement that the use of encryption should be encouraged but it shouldn't excuse a controller from reporting. It might however excuse the controller from any repercussions, as they may have demonstrated best efforts in securing data.

A majority of the group believes that the code, and its implementation, should be used to encourage and develop best practice, and should not be viewed as a means of penalising commerce. It was discussed that there might be an economic benefit to be derived from having a superior privacy culture in organisations and wider society.

List of recommendations

1. Implement streamlined reporting mechanism (e.g. web-based form) that
 - a. is supported by analytics to allow ODPC to determine the level of investigation or remediation required
 - b. requires basic information to begin with (within 48 hours of becoming aware).
 - i. Nature – personal, sensitive personal or personal financial (if defined)
 - ii. Volume – number of subjects affected
 - iii. Medium – laptop, usb device etc
 - iv. Encryption – Not encrypted, Encrypted (128, 256 etc)
 - c. requires complete report within 14 days (using standard template)
 - d. ODPC may begin investigation during 14 day period if severity warrants it
 - e. mandates varying levels of detail depending on severity of breach and actions taken.
2. Publish how the Office will respond to different levels of breach i.e. graduated responses based on criteria (nature, volume, encryption). For example:
 - a. If data is strongly encrypted (define), low volume and has not occurred frequently in the past – no further action, no publication in annual report
 - b. If data is sensitive, low volume and not occurred before – no enforcement action but requirement to document cause and remedial action taken
 - c. If breach is high volume or has occurred many times (define) – full investigation by ODPC, publication of investigation results, possible further enforcement actions.
3. Publish recommended levels of encryption, and other security guidelines, that will mitigate
4. Implement quarterly publication by ODPC of summarised, anonymised statistics of nature and volume of breaches, perhaps by industry (where relevant).
5. Implement a method and guidelines for reporting of data breaches by individuals; data subjects or others.
6. Implement “whistleblower” legislation to protect individuals (e.g. employees within a DC) who report incidents but with published consequences for mischievous or malicious reports

Changes to exceptions

7. Remove all exceptions to the obligation to report to Office of the Data Protection Commissioner **OR**
8. Remove exceptions 1 and 2 (encryption exceptions) **AND/OR**
9. Clarify definition of personal financial data in exception 3

Changes related to notification of data subjects

10. Add requirement to *always* notify the data subjects **OR**
11. Add requirement to *either* notify the data subjects or explicitly request the ODPC to decide whether to notify (based on information reported in 1.b)

Changes related to notification of third parties

12. Remove vague direction to notify third party organisations e.g. Gardai, Financial Institutions etc **OR**
13. Make explicit when controllers should notify 3rd parties **OR**
14. Make it a function of the ODPC to identify 3rd parties to be informed