



Notification of Data Security Breaches to the Information Commissioner's Office

All data controllers have a responsibility under the Data Protection Act 1998 to ensure appropriate and proportionate security of the personal data they hold. (DPA 1998 7th Principle). There are also specific requirements in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the Regulations) for public electronic communications service providers to take appropriate technological and organisational measures to safeguard the security of their services.

From 26 May 2011 public electronic communications service providers have a requirement to notify the Commissioner, and in some cases individuals themselves, of personal data security breaches. For more information about the specific breach notification requirements for service providers see:

http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/security_of_services.aspx

There is no legal obligation in the DPA for data controllers to report breaches of security which result in loss, release or corruption of personal data, the information Commissioner believes serious breaches should be brought to the attention of his Office. The nature of the breach or loss can then be considered together with whether the data controller is properly meeting his responsibilities under the DPA.

“Serious breaches” are not defined. However the following should assist data controllers in considering whether breaches should be reported:

The potential harm to data subjects:

The potential harm to individuals is the overriding consideration in deciding whether a breach of data security should be reported to the Information Commissioner's Office.

Ways in which harm can occur include:

- o exposure to identity theft through the release of non-public identifiers eg passport number
- o information about the private aspects of a person's life becoming known to others eg financial circumstances.

The extent of harm, which can include distress, is dependant on both the volume of personal data involved and the sensitivity of the data. Where there is significant actual or potential harm as a result of the breach,

whether because of the volume of data, its sensitivity or a combination of the two, there should be a presumption to report.

Where there is little risk that individuals would suffer significant harm, for example because a stolen laptop is properly encrypted, or the information that is the subject of the breach is publicly available information, there is no need to report.

The volume of personal data lost / released / corrupted:

There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. It is difficult to be precise what constitutes a large volume of personal data. Every case must be considered on its own merits but a reasonable rule of thumb is any collection containing information about 1000 or more individuals.

An example we would expect to be reported would be the theft / loss of an *unencrypted* laptop computer or other *unencrypted* portable electronic / digital media holding names and addresses, dates of birth and National Insurance Numbers of 1000 individuals.

An example we would not expect to be reported would be the theft / loss of a marketing list of 500 names and addresses or other contact details where there is no particular sensitivity of the product being marketed.

However it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high perhaps because of the circumstances of the loss or the extent of information about each individual. If the data controller is unsure whether to report or not, then the presumption should be to report.

The sensitivity of the data lost / released / unlawfully corrupted:

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial harm. This is most likely to be the case where that data is *sensitive personal data* as defined in section 2 of the DPA. As few as 10 records could be the trigger if the information is particularly sensitive.

An example we would expect to be reported would be a manual paper based filing system (or *unencrypted* digital media) holding the personal data relating to 50 named individuals and their financial records.

An example we would not expect to be reported would be a similar system holding the trade union subscription records of the same number of individuals where there were no special circumstances surrounding the loss.

Reporting

Serious breaches should be notified to the Information Commissioner's Office by email using the address casework@ico.gsi.gov.uk, or by post to our office address: *Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF*.

The notification should include:

- The type of information and number of records
- The circumstances of the loss / release / corruption
- Action taken to minimise / mitigate effect on individuals involved including whether they have been informed
- Details of how the breach is being investigated
- Whether any other regulatory body has been informed and their response
- Remedial action taken to prevent future occurrence
- Any other information you feel may assist us in making an assessment

Guidance on how to manage a data security breach can be found here:

http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx

What will the Information Commissioner's Office do when a breach is reported?

The nature and seriousness of the breach and the adequacy of any remedial action will be assessed and a course of action determined. We may:

- Record the breach and take no further action
- Investigate the circumstances of the breach and any remedial action which could lead to:

- 1) no further action
- 2) a requirement on the data controller to undertake a course of action to prevent further breaches
- 3) formal enforcement action turning such a requirement into a legal obligation
- 4) Where there is evidence of a serious, deliberate or reckless breach of the DPA, the serving of a monetary penalty notice requiring the organisation to pay a

monetary penalty of an amount determined by the Commissioner up to the value of £500,000

Where a breach has been voluntarily reported to the ICO, we will take this into consideration when deciding on the most appropriate course of action.

Will a reported breach be made public?

We do not see it as our responsibility to publicise security breaches not already in the public domain or to inform any individuals affected. In so far as they arise these are the responsibilities of the data controller.

However, the ICO may recommend the data controller to make a breach public where it is clearly in the interests of the individuals concerned or there is a strong public interest argument to do so.

Where the Information Commissioner takes regulatory action, it is policy to publicise such action, unless there are exceptional reasons not to do so. This policy on publication extends to any formal undertakings provided to the Commissioner by a data controller.

However the Commissioner will not normally take regulatory action unless a data controller declines to take any recommended action, he has other reasons to doubt future compliance or there is a need to provide reassurance to the public. Such a need is most likely to arise where the circumstances of the breach are already in the public domain.

Further information on the ICO's regulatory action strategy can be found here:

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_regulatory_action_policy.pdf

More information on monetary penalties can be found here:

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf