Notification of data security breaches to the Information Commissioner's Office (ICO)

Data Protection Act

Contents

The Data Protection Act 1998 (the DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

An overview of the main provisions of the DPA can be found in The Guide to Data Protection at:

http://www.ico.org.uk/for_organisations/data_protection/the_guide.aspx

This is part of a series of guidance, which goes into more detail than the Guide, to help organisations to fully understand their obligations and to promote good practice.

This guidance explains to organisations when and how to report a data security breach to the ICO, and what will happen next.

Overview

- Report serious breaches of the seventh principle
- Consider:
  - Potential detriment to individuals
  - Volume of data affected
  - Sensitivity of data
- Use 'security breach notification form'
- What happens next

What the DPA says

All data controllers have a responsibility under the DPA to ensure appropriate and proportionate security of the personal data they hold. The seventh principle of the DPA says that:

'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

Reporting a breach

Although there is no legal obligation on 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 detriment to data subjects:

The potential detriment to individuals is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriment includes emotional distress as well as both physical and financial damage.

Ways in which detriment can occur include:

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

The extent of detriment likely to occur is dependent on both the volume of personal data involved and the sensitivity of the data.

Where there is significant actual or potential detriment 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 detriment, 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 about what constitutes a large volume of personal data. Every case must be considered on its own merits.

Example	**☑ Reportable**	**☒ Not reportable**
	Theft or loss of an *unencrypted* laptop computer or other *unencrypted* portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of 100 individuals	Theft or loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the product being marketed

However, it will 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 or not to report, the presumption should be to report.

The sensitivity of the data lost / released / 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 detriment, including substantial distress.

This is most likely to be the case where that data is *sensitive personal data* as defined in section 2 of the DPA. Even a single record could be the trigger if the information is particularly sensitive.

Example	**☑ Reportable**	**☒ Not reportable**
	A manual paper-based filing system (or *unencrypted* digital media) holding the personal data relating to 50 named individuals and their financial records	A similar system holding the trade union subscription records of the same number of individuals, where there are no special circumstances surrounding the loss

Method of reporting

Serious breaches should be notified to the ICO using our DPA security breach notification form which should be sent to the email address: casework@ico.gsi.gov.uk, or by post to our office address: *Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.*

The security breach notification form can be found here:

http://www.ico.org.uk/for_organisations/data_protection/lose.aspx

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

http://www.ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx#security

What happens when a breach is reported

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

We may:

- Record the breach and take no further action, or
- Investigate the circumstances of the breach and any remedial action, which could lead to:
    - no further action;
    - a requirement on the data controller to undertake a course of action to prevent further breaches;
    - formal enforcement action turning such a requirement into a legal obligation; or
    - where there is evidence of a serious breach of the DPA, whether deliberate or negligent, 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.

More information on the circumstances in which the Commissioner will take regulatory action can be found here:

http://www.ico.org.uk/what_we_cover/taking_action/dp_pecr.aspx

More information specifically on monetary penalties can be found here:

http://www.ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx#monetary

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 that the data controller make a breach public where it is clearly in the interests of the individuals concerned or if there is a strong public interest argument to do so.

Where the Information Commissioner does take regulatory action, it is our 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.

More information

This guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of data protection, please Contact us: see our website www.ico.org.uk

Note also that there are specific requirements in the Privacy and Electronic Communications (EC Directive) Regulations 2003, as amended, for public electronic communications service providers to take appropriate technological and organisational measures to safeguard the security of their services.

From 26 May 2011, such service providers have an obligation 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 such service providers, see:

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