Guidance on data security breach management

Data Protection Act

Contents

The Data Protection Act 1998 (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 DPA can be found in The Guide to Data Protection:
https://ico.org.uk/for-organisations/guide-to-data-protection/

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

Overview

This guidance sets out some of the things an organisation needs to consider in the event of a security breach. It is not intended as legal advice, nor is it a comprehensive guide to information security. It should, however, assist organisations in deciding on an appropriate course of action if a breach occurs.

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Many organisations take the view that one of those measures might be the adoption of a policy on dealing with a data security breach.

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

However the breach has occurred, there are four important elements to any breach management plan:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

1. Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers. Consider the following:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.

- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the police.

2. Assessing the risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business. While these types of incidents can still have significant consequences the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following points are also likely to be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people

- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

3. Notification of breaches

Informing people and organisations that you have experienced a data security breach can be an important element in your breach management strategy.

However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

From 26 May 2011 certain organisations (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:

https://ico.org.uk/for-organisations/guide-to-pecr/security-of-services

Answering the following questions will assist other types of organisations in deciding whether to notify:

- Are there any legal or contractual requirements? Service providers have an obligation to notify the Commissioner in certain circumstances, in other areas sector specific rules may lead you towards issuing a notification.

- Can notification help you meet your security obligations with regard to the seventh data protection principle?

- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?

- If a large number of people are affected, or there are very serious consequences, you should inform the ICO.

- Consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.

- Have you considered the dangers of 'over notifying'. Not every incident will warrant notification and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work.

You also need to consider who to notify, what you are going to tell them and how you are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to your decision:

- Make sure you notify the appropriate regulatory body. A sector specific regulator may require you to notify them of any type of breach but the ICO should only be notified when the breach involves personal data

- There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation

- Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach

- When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them

- Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a helpline number or a web page, for example.

When notifying the ICO you should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures you had in place at the time the breach occurred. You should also inform us if the media are aware of the breach so that we can manage any increase in enquiries from the public. When informing the media, it is useful to inform them whether you have contacted the ICO and what action is being taken. ICO will not normally tell the media or other third parties about a breach notified to us, but we may advise you to do so.

The ICO has produced guidance for organisations on the information we expect to receive as part of a breach notification and on what organisations can expect from us on receipt of their notification. This guidance is available on our website:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

You might also need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

4. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of your response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if your response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience.

You may find that existing procedures could lead to another breach and you will need to identify where improvements can be made.

The following points will assist you:

- Make sure you know what personal data is held and where and how it is stored. Dealing with a data security breach is much easier if you know which data are involved. Your notification with the Information Commissioner will be a useful starting point.
- Establish where the biggest risks lie. For example, how much sensitive personal data do you hold? Do you store data across the business or is it concentrated in one location?
- Risks will arise when sharing with or disclosing to others. You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced
- Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether you need to establish a group of technical and nontechnical staff who discuss 'what if' scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions
- If your organisation already has a Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches
- It is recommended that at the very least you identify a group of people responsible for reacting to reported breaches of security

Other considerations

Additional guidance is also available if you need further information on data security breaches:

⇒ see Notification of data security breaches to the Information Commissioner's Office.

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 freedom of information or data protection, please Contact us: see our website www.ico.org.uk.