Guidance on Managing Data Breaches

This guidance covers what to do if you believe there has been a data breach and when it should be notified to the Commissioner.

This guidance relates to both the Data Protection (Jersey) Law 2005 and the Data Protection (Bailiwick of Guernsey) Law, 2001 ("the Law").

Where the Laws differ and to show differences between the two jurisdictions the page will be split as shown below.

Jersey	Guernsey
Commissioner = Information Commissioner a = article within the Law	Commissioner = Data Protection Commissioner s = section of the Law

Where numbering of passages from the Laws are the same it will be shown as a/s.

April 2016

Table of Contents

Introduction

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.

This guidance note sets out some of the things an organisation needs to consider in the event of a security breach. This note 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.

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:

- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response

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.

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.

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.

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

- Are there any legal or contractual requirements? Organisations have no legal obligation to notify the Commissioner of a security breach, however the circumstances of the breach 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 Commissioner.

- 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 Commissioner 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

- 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 Commissioner 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 Commissioner and what action is being taken. The Commissioner will not normally tell the media or other third parties about a breach notified to us, but we may advise you to do so.

Further information about when the Commissioner should be informed of a breach and what organisations can expect from us on receipt of their report as found towards the back of this document.

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.

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 Data Protection notification with the 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.

When should a breach be reported?

All data controllers have a responsibility under the Data Protection Law to ensure appropriate and proportionate security of the personal data they hold. (7th Principle).

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 Commissioner believes serious breaches should be brought to the attention of her 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 Law.

"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 Commissioner's Office.

Ways in which harm 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 harm, which can include distress, is dependent 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 Commissioner 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 Social Security 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 Commissioner 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 a/s 2 of the Law. 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 Commissioner using the details located at the back of this document.

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

What will the Commissioner 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 (formal undertaking)
    3. formal enforcement action turning such a requirement into a legal obligation

Where a breach has been voluntarily reported to the Commissioner, 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 Commissioner 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 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, she 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.

Contact the Commissioner

Breach Reporting, Enquiries and Publication Requests

Jersey

Office of the Information Commissioner
Brunel House
Old Street
St Helier
Jersey
JE2 3RG

T: +44 (0)1534 716530
W: www.dataci.org
Email: enquiries@dataci.org

Guernsey

Office of the Data Protection Commissioner
Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey
GY1 2LQ

T: +44 (0)1481 742074
W: www.dataci.org
Email: enquiries@dataci.org