SCoR

THE SOCIETY & COLLEGE OF RADIOGRAPHERS

Data Protection

Data Breach Procedure

April 2018

DATA BREACH PROCEDURE

Contents

DATA BREACH PROCEDURE

Version control

Version number	Date	Reason for change
0.1	September 2017	
0.2	January 2018	Update by Eugene

Introduction

The General Data Protection Regulation (GDPR) requires that all organisations report certain types of data breach to the relevant supervisory authority (the Information Commissioner's Office), and in some cases to the individuals affected.

Failing to notify a breach when needed can result in a significant fine of up to €10m.

Employees must report potential data breaches that they become aware of to the SCoR Data Protection Officer immediately.

What is a personal data breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Data security breaches can happen for a number of reasons including:

- 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

When to notify the ICO of a breach

It is necessary to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, a loss of customer details where the breach leaves individuals open to identity theft must be reported. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, should not be reported.

The SCoR's CEO and Data Protection Officer are responsible for deciding whether a breach needs to be reported to the ICO. In making this decision, the following factors should be taken into account:

- The potential harm to individuals which could arise from the breach; and
- The volume of personal data lost, released or corrupted; and
- The sensitivity of the data lost, released or corrupted.

When to notify individuals of a breach

Individuals concerned directly must be notified if a breach is likely to result in a high risk to their rights and freedoms.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the ICO.

Information to be included in a breach notification

1. The nature of the personal data breach including, where possible:
   - the categories and approximate number of individuals concerned; and
   - the categories and approximate number of personal data records concerned;
2. The name and contact details of the data protection officer;
3. A description of the likely consequences of the personal data breach; and
4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Timescales for reporting a breach to the ICO and public

Notifiable breaches must be reported to the ICO within 72 hours of becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within this time-period and allows for information to be provided in phases.

We must notify the public without undue delay if a breach is sufficiently serious to warrant notification to the public.

The process for managing a breach

Any member of staff that becomes aware of a loss or theft of personal data, unauthorised access, disclosure or release of personal data or corruption of personal data, must inform the SCoR Data Protection Officer immediately.

1. Member of staff - report the breach to the Data Protection Officer
2. Data Protection Officer investigate the breach
3. Data Protection Officer inform the CEO and relevant directors
4. Data Protection Officer develop and implement a containment and recovery plan, considering what needs to happen to contain the breach and limit damage

5. Data Protection Officer consult the CEO and relevant directors
6. CEO inform the Police if appropriate
7. Data Protection Officer assess the risk of damage and distress caused to individuals affected
8. Data Protection Officer recommend to the CEO and relevant directors whether or not to report the breach to the ICO, based upon the results of the risk assessment
9. Data Protection Officer prepare the breach notification if appropriate and forward to CEO for approval
10. Data Protection Officer forward breach notification to the ICO once approved by the CEO.

The Data Protection Officer's four stages for managing a breach

Stage 1 - Containment and recovery

Firstly it is necessary to establish what is required to contain the breach and whether there is anything that can be done to recover any losses and limit the damage the breach can cause. For example, in the event of a breach involving financial information it would be appropriate to purchase identity insurance as soon as possible for affected data subjects. This is likely to require input from other SCoR teams such as IT, HR and Senior Management. In some cases it may also be necessary to involve external stakeholders and suppliers.

It may be necessary to inform the police.

Stage 2 - Assessment of ongoing risk

It is necessary to assess the risks associated with the breach and in particular the potential adverse consequences for individuals, how serious or substantial these are and the likelihood of them actually happening.

The following points should be considered:

- What type of data is involved?
- Is it sensitive?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If it has been stolen, it could be used for purposes which are harmful to the data subjects; if it has been damaged, this poses a different type and level of risk
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached? Whether they are staff, supporters, 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 the SCoR?

Where there is significant actual or potential harm as a result of the breach, whether because of the volume of data, its sensitivity, the type of data subject affected or a combination of these, the breach should be reported.

The Data Protection Officer must consider the facts of each case and recommend to the CEO whether or not to report the breach to the ICO. If the there is any uncertainty as to whether to report or not, then the presumption should be to report.

Stage 3 – Notification of breaches

People and organisations affected by a data security breach should be notified of the breach only if there is a clear purpose for doing so. For example, to enable them to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

The following points should be considered when deciding whether or not to notify people whose personal information was affected by a breach:

- Are there any legal or contractual requirements?
- 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 it is decided to notify the individuals concerned the notification should include a description of how and when the breach occurred, what data was involved, details of what has already been done to respond to the risks posed by the breach and details of how to contact the SCoR for more information on the matter, via a helpline or specific area of the website.

It may also be appropriate to give specific and clear advice on the steps they can take to protect themselves and also what the SCoR is willing to do to help them.

The ICO website has a form to help with notification of breaches. See https://ico.org.uk/for-organisations/report-a-breach/

When notifying the ICO the following details should be provided:

- The type of information and number of records;
- The circumstances of the loss / release / corruption;
- Security measures in place such as encryption and procedures in place at the time the breach occurred
- Any action which has been taken to minimise / mitigate the effect on individuals involved where information has been lost / stolen / damaged including whether they have been informed of the breach;
- How the breach is being investigated;
- Any remedial action which has been taken or will be taken to prevent future occurrence; and
- Any other information which may assist the ICO in making an assessment.

The ICO also asks that they are informed if the media are aware of the breach so that it can manage any increase in enquiries from the public.

The ICO will not normally tell the media or other third parties about a breach notified to them, but it may advise the SCoR to do so.

The ICO has produced guidance for organisations on the information it expects to receive as part of a breach notification and on what organisations can expect from them on receipt of their notification.

The ICO will assess the nature and seriousness of the breach and the adequacy of any remedial action taken before deciding on a course of action. This may be:

- Recording the breach and taking no further action; or
- Investigating the circumstances of the breach and any remedial action which could result in:
  - no further action;
  - a requirement for the SCoR to take steps to prevent further breaches;
  - formal enforcement action (i.e. a formal legal obligation to take steps to prevent further breaches);
  - where there is evidence of a serious, deliberate or reckless breach of the Act, a monetary penalty notice requiring the SCoR to pay a fine of an amount determined by the ICO.

When deciding on the most appropriate course of action the ICO usually takes into account when a breach has been voluntarily reported.

Stage 4 - Evaluation and response

If it is thought that the breach was caused, even in part, by systemic and ongoing problems or by inadequate policies or training, or a lack of a clear allocation of responsibility then these issues must be raised by the Data Protection Officer with the CEO and directors, and addressed.

Recording and storing data breach issues

Data breach notifications may come in through e-mail, phone calls or in person. It is important to keep a record of the notification, handling, and resolution efforts. A log of activity should be stored on a shared organisational Server (N:\Information\Data Protection\Breaches).