Data Protection Managing a Data Protection Breach

Offas Dyke Riding Club must assess and log all personal data breaches and report serious breaches to the Information Commissioner's Office (ICO) within 72 hours of being discovered.

Failure to notify the ICO of a personal data breach can lead to fines of €10m.

- 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

There are four key stages to managing a data protection breach:

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

Offas Dyke Riding Club Data Protection Lead (DPL) is responsible for deciding whether a breach needs to be reported to the ICO. In making this decision, the following factors should be considered:

- 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.

The process for managing a data breach

1. Member of staff - report the breach to the DPL

2. DPL - investigate the breach

3. Inform the Senior Management Team

4. Develop and implement a containment and recovery plan, considering what needs to happen to contain the breach and limit damage

5. Consult the Senior Management Team

6. Inform the Police if appropriate

7. Assess the risk of damage and distress caused to individuals affected

8. Recommend to the Senior Management Team whether to report the breach to the ICO, based upon the results of the risk assessment

9. Prepare the breach notification if appropriate and forward to Senior Management Team for approval

10.Forward breach notification to the ICO once approved by the Senior Management Team

Stage 1 - Containment and recovery

Putting together and implementing a containment and recovery plan is likely to require input from other teams such as IT, HR and Senior Management. In some cases, it may also be necessary to involve external stakeholders and suppliers.

Firstly, there is a need to establish what needs to happen 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.

It may be necessary to inform the police.

Stage 2 - Assessment of ongoing risk

The DPL should assess the risks which associated with the breach and the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following points should be considered:

• What type of data is involved?

• How sensitive is it? 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 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?

Where there is significant actual or potential harm because 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 DPL will consider the facts of each case and recommend to the Senior Management Team whether 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 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 said person 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 what Offas Dyke Riding Club 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

• 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 Offas Dyke Riding Club 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. This guidance is available at https://ico.org.uk/for-organisations/guide-to-data-protection/ principle-7- security/

The ICO will assess the nature and seriousness of the breach that Offas Dyke Riding Club reports 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 Offas Dyke Riding Club 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 GDPR, a monetary penalty notice requiring Offas Dyke Riding Club to pay a fine of an amount determined by the ICO which could be up to €10m.

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

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 DPL with the Senior Management Team and addressed.

If you would like further information on managing a data protection breach please click Notification of Data Security Breaches to the Information Commissioner's Office to see the ICO's guidance