GDPR: DATA BREACH POLICY

Aim

The GDPR requires that we must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. This policy sets out how we deal with a data security breach.

What is a personal data breach?

The Information Commissioner's Office states that a personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Action to be taken in the event of a data breach

Containment and recovery

The immediate priorities are to:

- Contain the breach;
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope.

In the event of a security incident or breach, staff must immediately inform the data protection officer

The data protection officer will take the lead on investigating the breach. Steps to take where personal data has been sent to someone not authorised to see it:

- Inform the recipient not to pass it on or discuss it with anyone else;
- Inform the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so;
- Explain to the recipient the implications if they further disclose the data; and
- Where relevant, inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.

Steps to take where personal data has been obtained by someone not authorised to see it

- Inform the recipient not to pass it on or discuss it with anyone else;
- Inform the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so;
- Explain to the recipient the implications if they further disclose the data; and

Where relevant, inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.

Assessing the risk

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.

We will consider

What data is involved and how sensitive is it?

If the data has been lost or stolen are there protections in place such as encryption?

What has happened to the data? – ie. If it has been stolen or lost, could it be used for purposes which are harmful to the individual to whom the data relates?

Who are the individuals whose data has been breached? – This 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?

Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause

Notifying the ICO and individuals, where relevant

Who is responsible?

In our business, the data protection officer is the point of contact for staff and the ICO on this policy and on all matters relating to data protection.

The data protection officer is also responsible for notifying the ICO and individuals (where applicable) of relevant personal data breaches.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it.

If we decide we don't need to report the breach, we need to be able to justify this decision, and we should document it.

When to notify the ICO and dealing with delays

Notifiable breaches must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

If we don't comply with this requirement, we must be able to give reasons for the delay.

In some instances it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Where that applies we should provide the required information in phases, as long as this is done without undue further delay.

Breach information to the ICO

When reporting a breach, we will provide the following information:

- a description of 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;
- our data protection officer

- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Individuals

Where notification to individuals may also be required, the data protection officer will assess the severity of the potential impact on individuals as a result of a breach and the likelihood of this occurring. Where there is a high risk, we will inform those affected as soon as possible, especially if there is a need to mitigate an immediate risk of damage to them.

Information to individuals

The data protection officer will consider who to notify, what we are going to tell them and how we are going to communicate the message. This will depend to a large extent on the nature of the breach but will include the name and contact details of our data protection officer (where relevant) or other contact point where more information can be obtained; a description of the likely consequences of the personal data breach; and a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The breach need not be reported to individuals if:

- We have implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach;
- We have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- It would involve disproportionate effort (in this case a public communication may be more appropriate).

In the case of a breach affecting individuals in different EU countries, we are aware that the ICO may not be the lead supervisory authority. Where this applies, the data protection officer should establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.

Third parties

In certain instances the data protection officer may 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.

Document all decisions

The data protection officer must document all decisions that we take in relation to security incidents and data breaches, regardless of whether or not they need to be reported to the ICO.

Evaluate our response and mitigation steps

We investigate the cause of any breach, decide on remedial action and consider how we can mitigate it. As part of that process we also evaluate the effectiveness of our response to incidents or breaches. To assist in this evaluation we consider:

- What personal data is held, where and how it is stored
- Risks that arise when sharing with or disclosing to others

- This includes checking the method of transmission to make sure it's secure and that we only share or disclose the minimum amount of data necessary

- Weak points in our existing security measures such as the use of portable storage devices or access to public networks

- Whether or not the breach was a result of human error or a systemic issue and determine how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps

- Staff awareness of security issues and look to fill any gaps through training or advice

- The need for a Business Continuity Plan for dealing with serious incidents

- The group of people responsible for reacting to reported breaches of security

5. Review

This document will be reviewed regularily