Data Breach Policy

Please refer to our 'GDPR Overview' document for definition of terms, outlines of policies and the context in which this policy is set.
This document is part of our Data Protection Policy Portfolio and is to be used in conjunction with the other documents.

1 – What a data breach is
GDPR requires we must ensure appropriate measures are in place to limit unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

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 data breach whenever any 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.

Our procedures in relation to a data breach are outlined below.

2 – Summary of steps taken after a data breach
The initial priorities after a data breach are to:

- Contain the data breach;
- Asses the consequences of the data breach;
- Limit the scope of the data breach; and
- Notify the ICO and/or individuals, where relevant.

In the event of a data breach the Data Protection Manager of the firm will be informed. The Data Protection Manager will then begin the investigation into the data breach. If the Data Protection Manager is absent, then their appointed deputy will begin the investigation into the data breach.

3 – Breach containment
The Data Protection Manager will immediately try to contain the breach, this may involve any or all of the following:

- Removing the infected computer(s)/server(s) from the network;
- Informing the unintended recipient of data to destroy and/or delete the data, and under no circumstances to discuss the data with anyone else; and
- Ensure the method used to initiate the breach cannot be used again.

4 – Assess the consequences of the data breach
After a data breach the Data Protection Manager will consider the following:

- **What type of data is involved?** – How sensitive is it? Is it encrypted? Is it already publically available?
- **What has happened to the data?** – If it is stolen, what purposes could it be used for? If it is lost or damaged, what will the effect be?
- **Which individuals are/will be affected by the data breach?** – Who are the individuals? Are they customers/staff/suppliers?
- **What harm can come to the individuals?** – Are there risks to physical safety? Will reputation be affected? Will there be financial loss? Is there a risk to the wider society, such as risk to public health? What can we do to limit the damage?

The above questions will allow the Data Protection Manager to determine the seriousness of the data breach and as such act accordingly.

5 – Notifying the ICO and/or individuals, where relevant
In our business, the Data Protection Manager is the point of contact on all matters relating to data protection.

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

When do we need to notify the ICO about a data breach?
We are required to notify the ICO of a data breach if there is likely to be a risk to people's rights and freedoms, if this is unlikely, then we are not required to report the data breach.

The risk to people's rights and freedoms will be determined by the questions in paragraph 4.

We will always document our rationale for not reporting a breach to the ICO.

How soon will we notify the ICO?
After determining that a data breach should be reported to the ICO, we must report to them without under delay, but not later than 72 hours after becoming aware of the data breach.

If our reporting of the data breach is later than 72 hours then we must be able to justify 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.

What information do we report to the ICO about a data breach?
When reporting a breach, we will provide the following information:

1. a description of the nature of the data breach including, where possible:
    a. the categories and approximate number of individuals concerned;
    b. and the categories and approximate number of personal data records concerned;
2. our Data Protection Manager;
3. a description of the likely consequences of the data breach; and
4. a description of the measures taken, or proposed to be taken, to deal with the data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

What data breaches do we notify the individuals concerned?
The Data Protection Manager will determine the seriousness of the data breach, using paragraph 4 as a guide. Where a risk to individual's rights and freedoms are deemed to be high then the Data Protection Manager will inform those affected as soon as possible, especially if there is a need to mitigate an immediate risk of damage to them.

A data breach will not be reported to individuals where:

- We have implemented appropriate technical or organisational measures and those measures were applied to the data affected by the data breach;
- We have taken appropriate measures to ensure the high risk to individuals rights and freedoms will no longer materialise; or
- It would involve disproportionate effort (a public communication maybe more appropriate).

What information will be given to the individuals?
The Data Protection Manager will consider who to notify, what information is to be given and how the message is to be communicated. This will depend on the nature of the data breach, but will include the name and contact details of the Data Protection Manager; description of the likely consequences; and a description of the measures taken, or proposed to be taken, to mitigate any possible adverse effects.

Will any other third parties be notified?
In certain circumstances the Data Protection Manager may be required to report to other third parties, such as the police, insurance companies or professional bodies to assist in reducing the risk of financial loss to individuals.

Documentation of the data breach
The Data Protection Manager will document their decisions in relation to the data breaches, whether they are reported to the ICO or not.

6 – Evaluation of our response and steps to mitigate risk

We will investigate thoroughly any data breach, decide on remedial action and consider how we can mitigate it in the future. We actively try to ensure our data is as secure as can possibly be, and systematically check our systems are working as expected.