Data Breach Procedure

Overview

This procedure has been developed to enable an effective response to personal data breaches in line with the GDPR. Where a personal data breach has been identified, we will in the first instance:

- Log the date, time and nature of the breach
- Begin remedial activity to secure the breach
- Assess and document the risk posed to the privacy of individuals by the breach (using previous risk assessments carried out in line with the data inventory)
- Identify who we need to notify about the breach based on criteria set within the GDPR (this depends on the role we are playing), and document the decision along with supporting rationale

Where we are the Data Controller

Risk

If our assessment identifies it is likely there is a risk to individuals 'rights and freedoms' then we must communicate details of the breach to the Information Commissioner's Office (ICO)/supervisory authority within 72 hours of discovering the breach. Reports to the ICO can be made in the following ways:

- By phone – 0303 123 1113
- By email – casework@ico.org.uk

Where submitting a breach report electronically, the following form should be used:

https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc

Reports to the ICO/supervisory authority should include the following pieces of 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
    - The name and contact details of the Data Protection Officer or other contact points 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, including, where appropriate, the measures taken to mitigate any possible adverse effects

Where not all of this information is available within the 72 hour period, we will explain delays and provide outstanding information as quickly as possible, keeping the ICO/supervisory authority informed as to progress.

High Risk

Where our risk assessment identifies there is a high risk to an individual's rights and freedoms, we will contact them to inform them of the breach as quickly as possible so they can take steps to defend themselves from any potential damage. As a minimum we will provide the following:

- The name and contact details of the Data Protection Officer (or appropriate contact) or other contact points 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, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If we decide not to notify Data Subjects, the rationale needs to be captured.

Where we are the Data Processor

We will notify all personal data breaches to the relevant Data Controller as quickly as possible. This will include as much of the following information as possible to allow the Data Controller to carry out their own assessment to risk:

- 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
    - The name and contact details of the Data Protection Officer (if your organisation has one) 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, including, where appropriate, the measures taken to mitigate any possible adverse effects

For security purposes this will be done via telephone initially, then the secure transfer of subsequent information can be agreed. Communication to the Data Controller will be

logged and stored as part of the breach investigation to ensure it is available for interested parties.