|  |  |
| --- | --- |
| your logo here | [Company Name] |

# Breach Notification Procedure Template

Prior to carrying out this procedure it is important to understand and identify a data breach. The following has been outlined by the ICO: A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. 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, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

* 1. **Procedure Steps**

| **Step** | **Description** | **Person** |
| --- | --- | --- |
| Assessing the personal data breach | When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people’s rights and freedoms.  All personal data breaches need to be reported to the ICO unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.  If you decide you don’t need to report the breach, you need to be able to justify this decision, therefore you should document it. | *Click here to enter text.* |
| Likely to risk people’s rights and freedoms | You have **72 hours** to report a data breach to the ICO from the moment it is discover. If the ICO are notified outside of this time, you must provide a justification for the delay. | *Click here to enter text.* |
| Compile information for the ICO | * A description of the nature of the breach. * The categories of personal data affected. * Approximate number of data subjects affected. * Approximate number of personal data records affected. * Name and contact details of the Data Protection Officer / GDPR Owner. * Consequences of the breach (those that have occurred or and likely to occur) * Any measures taken to address the breach. * Any information relating to the data breach. | *Click here to enter text.* |
| More time required? | It may not always be possible to provide all of the above information within 72 hours, therefore you can phase the provision of this information (without undue delay) if you keep the ICO informed. | |
| Breach notification form | The information which needs to be compiled can be filled out using the ICO breach notification form. This can be found [here](https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc). | Click here to enter text. |
| Assess whether or not the individuals affected need to be contacted | * If you believe there is a high risk to the data subject, they should be informed immediately. * You must notify the data subject using clear and plain language * If the breach affects a high number of data subjects and it is not possible to notify them individually, you must look to make a public communication or a similar measure to inform those affected.   When communicating to individual’s you must do the following:   * Ensure you describe, in clear and plain language, the nature of the personal data breach * Provide a name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained * Provide a description of the likely consequences of the personal data breach * Outline 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. | Click here to enter text. |
| ICO contact details | The contact details of the supervisory authority can be found here: <https://ico.org.uk/for-organisations/report-a-breach/> | |

|  |  |  |
| --- | --- | --- |
| **Step** | **Description** | **Person** |
| Record of communication with ICO | It is recommended to record communications you have with the ICO post breach notification.  Record the following:   * Full name of contact assigned from the ICO * Which means you used to report the breach * What confirmation did you receive of the breach notification | Click here to enter text. |