Personal Data incident and breach reporting procedure

Procedure purpose

{NAME OF ORGANISATION} (hereafter we/us/our/the organisation) is committed to ensuring that all personal data we process, including that of colleagues and customers, is managed appropriately and in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as "DP legislation").

In particular we are committed to ensuring that all personal data breaches are swiftly identified and reported within the organisation and, where appropriate, to the Information Commissioner's Office and affected individuals.

This procedure applies to all colleagues, contractors and volunteers within {NAME OF ORGANISATION}.

Negligent or malicious non-compliance with this policy may be dealt with through the disciplinary process.

Please note – This procedure only relates to the *reporting* of personal data incidents. It does not replace other relevant procedures for incident management and mitigation which must be followed in addition to this procedure.

Document control

Document title:
Version number:
Author:
Owner:
Approval Date:
Review Date:
Version history:

Related documents

- Data Protection Policy
- Information Security Policy
- Personal Data Breach Log

Other useful documents:

- ICO Information Security Guide: https://tinyurl.com/y8az28o5
- ICO Guidance on Personal Data Breaches: https://tinyurl.com/yaf8xdnu
- A29WP Guidelines on Breach Notification: https://tinyurl.com/y8h4xckq
- Act Now Blog Post: https://tinyurl.com/hcghlfj

Responsibilities

- The **Chief Executive** has overall responsibility for deciding whether to report personal data breaches to the ICO and/or to affected individuals.
- {Some organisations may choose to designate a **Senior Information Risk Owner** at executive level with oversight of data protection and other aspects of information governance}.
- The **Data Protection Lead** has day-to-day responsibility for monitoring compliance with this procedure, receiving and processing incident reports, assessing risk and advising the Chief Executive accordingly, and liaising with the ICO and the public as appropriate. {*This assumes that the organisation does not meet the criteria under GDPR for mandatory designation of a Data Protection Officer. Should that be the case, replace all references to Data Protection Lead with Data Protection Officer.}*
- **Heads of Department** are responsible for ensuring that all staff are aware of their responsibilities to report incidents; for assisting the DP Lead in their duties through providing all appropriate information and support relevant to an incident; for continuing with appropriate incident management and mitigation. {Some organisations may choose to designate a specific role of **Information Asset Owner** at senior management level with accountability to the Senior Information Risk Owner.}
- **All colleagues** are responsible for immediately reporting any incident or breach affecting personal data held by the organisation.

See also ICO Guidance on personal data breaches and European Data Protection Board Guidelines for Personal Data Breach Reporting

---

Initial report of personal data incident

Any security incident *or near miss* which may impact on the **confidentiality, integrity or availability** of personal data held by us **must be reported immediately** to the Data Protection Lead by {DESCRIBE PROCESS FOR REPORTING INCIDENTS WITHIN THE ORGANISATION – FOR EXAMPLE, PHONE CALL, RAISING A TICKET ON AN INCIDENT LOG, EMAIL TO SPECIFIC MONITORED ACCOUNT.

Such events could include: {ADAPT TO ORGANISATION SPECIFIC EXAMPLES)

- Loss of records, laptops or media containing personal data;
- Unauthorised access to information systems containing personal data;
- Access of personal data with no justifiable business need;
- Personal data being misdirected to an incorrect recipient;
- Loss of access to systems containing personal data.

All reported incidents will be recorded to ensure appropriate mitigation measures are in place and to identify lessons or necessary improvements.

As far as possible the initial report should include details of:

- the nature and scope of the breach;
- when the breach occurred and when the organisation became aware;
- the people who have been or may be affected by the breach;
- what mitigation steps have been and will be taken.

If you are in any doubt as to whether an incident should be reported to the DP Lead, please err on the side of caution and report.

Please note. The relevant Head of Department is responsible for ensuring that all appropriate mitigation and recovery steps are taken as soon as possible, regardless of reporting outcomes.

Assessment of personal data incident

The Data Protection Lead will consider whether the event meets the GDPR definition of a personal data breach.

The Data Protection Lead will then conduct a risk assessment of the impact and likelihood of impact on the rights and freedoms of the affected individuals (data subjects) using the organisation's risk management approach.

This will consider risks to the affected individuals arising from the personal data breach including adverse impacts on their:

- privacy
- personal financial interests
- other material damages
- health and safety
- emotional wellbeing
- other non-material damages

In considering the risk, the Data Protection Lead will have support and advice from the relevant Head of Department and other colleagues as required and consider the content of existing Data Protection Impact Assessments.

Factors to be considered include:

- the type of breach
- the nature, volume and sensitivity of the personal data
- how easy it is to identify individuals
- the potential consequences for individuals
- any special characteristics of the data subject (for example, that they are children or otherwise vulnerable).

Having assessed the risk, the Data Protection Lead will record the outcome in the Personal Data Incident Log.

Reporting personal data breaches to the ICO

All reported incidents will be recorded to ensure appropriate mitigation measures are in place and to identify lessons or necessary improvements.

The Data Protection Lead will consider whether the incident meets the GDPR definition of a "personal data breach" which presents a risk to individuals. He/she will present a report to the Chief Executive {or SIRO where designated} including a recommendation on whether to report the matter to the Information Commissioner's Office.

If the Chief Executive {or SIRO where designated} decides that an incident constitutes a reportable data breach, the DP Lead will report the incident to the ICO and liaise as appropriate.

If a data breach presents a high risk to the data subjects, the DP Lead will ensure that they are also notified of the breach.

The DP Lead will be prepared to provide:

- the DP Lead's name and contact details;
- the nature and scope of the breach;
- when the breach occurred and when the organisation became aware;
- the people who have been or may be affected by the breach;
- what mitigation steps the organisation has taken and will take.

If the report takes place outside office hours, it can be made using the ICO Personal Data Breach reporting template:

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

Please note: The initial report *must* be made to ICO within 72 hours of the organisation becoming aware of the personal data breach.

Reporting personal data breaches to the affected individuals

If the Data Protection Lead considers that the personal data breach presents a *high* risk to individuals, s/he will present a report to the Chief Executive {or SIRO where designated} including a recommendation on whether to report the breach to the affected individuals.

If the Chief Executive {or SIRO where designated} decides that a breach should be reported to the affected individuals, the DP Lead will liaise with the relevant Head of Department and Corporate Communications (and Human Resources if the affected individuals are employees or contractors) to identify the most appropriate means of communicating the breach to the affected individuals, in plain language, and providing any appropriate support.

Contact

If you have any questions about this procedure, please contact:

Data Protection Lead

{NAME OF DATA PROTECTION CONTACT}

{ADDRESS}

{EMAIL}

{PHONE NUMBER}