The Highland & Western Isles Valuation Joint Board

Personal Data Breach Policy

Document Control

Document last saved: 11 June 2018

Version	Changes	Author	Date
1.0	First release	M Thomson	11/06/18
1.1	Review	W Gillies	13/06/18

Overview

From 25 May 2018, the Data Protection Act 2018 introduces a duty on all organisations to report certain types of personal data breaches to the Information Commissioners Office (ICO) where this may pose a risk to people. Organisations must inform the ICO within 72 hours of becoming aware of the breach, where feasible. This policy, which is based on the ICO guidance on personal data breaches, outlines what action should be taken in the event of a personal data breach.

This procedure applies to personal data breaches involving The Highland & Western Isles Valuation Joint Board, the Assessor for Highland & Western Isles and the Electoral Registration Officer for Highland & Western Isles data.

What is a personal data breach?

A personal data breach means 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. This means that a breach is more than just losing personal data. Examples of personal data breaches include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of 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 e.g. when it has been encrypted by ransomware, or accidentally lost or destroyed.

Reporting

All data security breaches or suspected data security breaches should be reported immediately to the Data Protection Officer (DPO) and the Assessor. The DPO is currently Lanarkshire Valuation Joint Board.

Details of the breach should also be recorded on the Personal Data Breach log held within Central Admin. The log should record the date of the breach, date of notification of the breach, nature of the breach and any appropriate action taken.

Containment and Recovery

The DPO or delegated investigating officer should:

- Confirm the nature of the information lost, and in particular whether the information consists of sensitive personal data (medical information, details of convictions or alleged criminality etc.) or information of use in carrying out identity theft (such as bank account details, national insurance numbers etc.);

- Prevent any further loss of information and if possible any further dissemination of the information which has been lost or compromised.

All staff must cooperate fully with any investigation. It is essential for staff involved in any data loss to be completely frank so that the DPO can assess the risks and take appropriate mitigating action.

The DPO or investigating officer will determine who needs to be made aware of the breach and what they need to do to contain the breach; this may include notifying affected individuals without undue delay and reporting the loss to the ICO.

Assessing the Risks

The DPO will determine the risks associated with the loss. The risks associated will be dependent on:

- The type of data involved;
- How sensitive the information is;
- Whether there were any protections in place, e.g. encryption of a portable device;
- What has happened to the data, if known;
- The categories and approximate number of individuals concerned;
- The categories and approximate number of personal data records concerned;
- What harm can come to those individuals whose data has been lost;
- Whether there are any wider consequences to the loss of the data;

The assessment will be immediately communicated to the Assessor.

Notification of breach

Recital 85 of the General Data Protection Regulation (GDPR) explains that “a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identify theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned”.

If a personal data breach has occurred the Board will need to establish the likelihood and severity of the resulting risk to people’s rights and freedoms. If it is likely that there will be

a risk then the ICO should be notified, however if risk is unlikely, there is no requirement to notify the ICO. If a breach is not reported then the decision not to report should be documented in the Personal Data Breach log.

If a decision is taken to notify individuals of the breach, the notification will tell them how and when the breach occurred and what data was involved. The notification will also tell the individual what has and is being done by the Board to respond to the breach. The decision to notify individuals will normally be taken by the DPO or, for large scale notifications, by the Assessor. Decisions on notifying the ICO will be taken by the DPO in conjunction with the Assessor.

Where appropriate, third parties such as the police, banks or professional bodies will be contacted for advice on reducing the risk of financial loss to individuals.

If the Information Commissioner requires to be notified, the DPO will do this as soon as possible following the breach via the following link:

https://ico.org.uk/for-organisations/report-a-breach/

Data Processors

Where we use data processors such as external print contractors they are required under Article 33(2) of the GDPR to inform the Board without undue delay as soon as they become aware of any personal data breaches.

Evaluation and response

Part of the overall breach response will be to investigate the causes of the breach and also the effectiveness of the Board's response to the breach.

Simply containing the breach is not acceptable, particularly if the breach was caused (even in part) by a systematic or ongoing problem. Action must be taken to rectify the underlying problem. A review will be conducted by the DPO and reported to the Management Team. A report on the review must be made available to the Assessor within three weeks of the incident and must address issues which caused the incident and make recommendations as to the steps necessary to prevent or minimise such an incident recurring.

Any data loss reported to the ICO will be reported to the next meeting of the Management Team.