Grampian Assessor & Electoral Registration Officer

Data Security Breach Procedure

On behalf of Grampian Valuation Joint Board

Version Control Table

Version	Originator	Summary of Changes	Date
V 1.0	Gavin M Oag	New Procedure	June 2018

Overview

In terms of the Data Protection legislation, organisations that process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data. This procedure, which is based on the Information Commissioner's guidance on data security breach management, outlines what action should be taken in the event of a data security breach.

This procedure applies to data breaches involving data under the control of the Grampian Assessor and ERO and the Grampian Valuation Joint board (collectively referred to below as GAERO)

A data security breach can happen for a number of reasons including:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- Blagging offence where information is obtained by deceiving the organisation that holds it

1. Reporting

All data security breaches or suspected data security breaches should be reported immediately to your supervisor and the Security Officer or, in his absence, the Assessor. The Security Officer or Assessor will inform the Data Protection Officer (DPO).

The Security Officer is the Depute Assessor (Aberdeenshire).

The DPO is the Depute Assessor for the Dunbartonshire and Argyll & Bute Valuation Joint Board.

Details of the breach should also be recorded on the Data Security Breach log by the Security Officer or Assessor. The log should record the date of the breach, date of notification of the breach, nature of breach and action taken.

2. Containment and Recovery

The Security Officer or Assessor and, where appropriate, in conjunction with the DPO should:

1. Confirm the nature of the information lost and, in particular, whether the information consists of special category personal data such as medical information, racial or ethnic origin, trade union membership or information where the loss results in a high risk to the individual e.g. information that could be used to carry out identity theft.

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

All staff including any staff employed by a data processor of GAERO must cooperate fully with any investigation. It is essential for staff involved in any data loss to be completely frank so that the Security Officer/Assessor and DPO can assess the risks and take appropriate mitigating action.

The Security Officer/Assessor and DPO 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 and reporting the loss to the Information Commissioner.

3. Assessing the Risks

The Security Officer/Assessor and 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, including whether it is special category information
- Whether there were any protections in place, e.g. encryption of a portable device
- What has happened to the data, if known.
- How many individuals' personal data are affected by the breach.
- What harm can come to those individuals whose data has been lost.
- Whether there are any wider consequences to the loss of the data.
- If individual's bank details have been lost, consideration will be given to contacting the banks for advice on preventing fraudulent use.

The assessment will be immediately communicated to the Assessor, when appropriate.

4. Notification of breach

Informing people and organisations that GAERO has experienced a data security breach is an important part of GAERO's breach management procedure.

Consideration will be given to:

- Who will be notified (police, banks, media etc),
- Notifying any parties to contractual or Data Sharing Agreements
- What we will be notifying them of, and
- How we are going to notify them.

If a decision is taken to notify individuals of the breach, the notification will tell them, in clear and plain language, 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 GAERO to respond to the breach and the contact details for the DPO. The decision to notify individuals will normally be taken by the Security Officer after considering any advice from the DPO. Decisions on notifying the Information Commissioner will be taken by the Security Officer/Assessor after considering any advice from the DPO.

If the Information Commissioner requires to be notified, this should be done without undue delay and within 72 hours of becoming aware of it. This should happen even if the breach assessment is not yet completed. 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/

5. Evaluation and response

Part of the overall breach response will be to investigate the causes of the breach and also the effectiveness of GAERO'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 re-occuring.

Based on "lessons learned", policies and procedures will be reviewed and updated if required.

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