Competition and Markets Authority's data breach policy

Unauthorised disclosure or loss of personal data

1. The Competition and Markets Authority (CMA) is required under the Data Protection Act 1998 to ensure the security and confidentiality of all the personal and sensitive personal data it processes including that processed by third parties acting on its behalf. Every care should be taken by staff to protect the personal data they work with and to avoid the unauthorised disclosure or loss of personal data.

2. This policy applies to all personal and sensitive personal data processed by the CMA or anyone acting on behalf of the CMA, as defined by sections 1 and 2 of the Data Protection Act.

Legislative framework

3. There are eight Data Protection Principles contained in the Data Protection Act which must be complied with when processing personal data. Failure to comply with any of these Principles is a breach of the Data Protection Act.

Seventh Data Protection Principle

4. This policy is concerned with the Seventh Data Protection Principle:

   'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

5. Examples of a breach of this Principle would include:

   - personal data accidentally being sent to someone (either internally or externally) who does not have a legitimate need to see it;
   - databases containing personal data being compromised, for example being illegally accessed by individuals outside the CMA;
   - loss or theft of laptops, mobile devices, or paper records containing personal data;

- paper records containing personal data being left unprotected for anyone to see, for example:-
  - files left out when the owner is away from their desk and at the end of the day;
  - papers not properly disposed of in secure disposal bins that can then be extracted or seen by others;
  - papers left at photocopying machines;
- staff accessing or disclosing personal data outside the requirements or authorisation of their job;
- being deceived by a third party into improperly releasing the personal data of another person; and
- the loss of personal data due to unforeseen circumstances such as a fire or flood.

The difference between a security breach and a data breach and the notification process to follow

6. A data breach relates to the loss of **personal data** and should be notified following the procedure described. A security breach relates to the loss of equipment containing personal data. Where a security breach has been notified that also involves personal data staff must also follow the data breach policy.

Action to be taken in the event of a data breach

7. On discovery of a data breach the following actions should be taken:-
   - Containment and recovery
   - Assessing the risk
   - Notification of breach to the Information Commissioner's Office (ICO)
   - Evaluation and response

Containment and recovery

8. **Who is responsible for action?** – The individual committing the breach, their staff manager (and work manager, if different).

Action to be taken

9. The immediate priority is to **contain the breach** and limit its scope and impact.

10. Where personal data has been sent to someone not authorised to see it staff should:

    - tell the recipient not to pass it on or discuss it with anyone else;
    - tell the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so;
    - warn the recipient of any implications if they further disclose the data; and
    - inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.

11. The Director responsible for the area where the breach occurred must be notified and they must immediately report it to Departmental Security Officer (DSO), the Deputy DSO and the Information Access Team providing the following information:

    - date and time of the breach;
    - date and time breach detected;
    - who committed the breach;
    - details of the breach;
    - number of data subjects involved; and
    - details of actions already taken in relation to the containment and recovery.

Assessing the risk

12. **Who is responsible for action?** – DSO or Deputy DSO.

Action to be taken

13. The DSO, Deputy DSO or a nominated person will conduct an investigation into the breach and prepare a report. This report will follow the ICO's guidance on Breach Management and will consider the following:

- How the breach occurred.
- The type of personal data involved.
- The number of data subjects affected by the breach.
- Who the data subjects are.
- The sensitivity of the data breached.
- What harm to the data subjects can arise? For example, are there risks to physical safety, reputation or financial loss?
- What could happen if the personal data is used inappropriately or illegally?
- For personal data that has been lost or stolen, are there any protections in place such as encryption?
- Are there reputational risks from a loss of public confidence in the service the CMA provides?

Notifying the Information Commissioner

14. **Who is responsible for action?** – The CMA Information Access Team.

Action to be taken

15. The DSO or Deputy DSO, the Senior Information Risk Owner, the Information Access Team and the Legal Service will determine whether the breach is one which is required to be notified to the ICO.

Who is responsible for notifying the ICO?

16. Responsibility for notifying the ICO rests with the CMA Information Access Team. They will complete a breach notification form.

Evaluation and response

17. **Who is responsible for action?** The managers in the area where the breach occurred, DSO and the Information Access Team.

Action to be taken

18. Once the breach has been dealt with the cause of the breach needs to be considered. There may be a need to update policies and procedures, or to conduct additional training.

The CMA Information Access Team

19. The CMA Information Access Team is responsible for providing guidance and training for CMA staff on data protection matters and is the central point of contact for CMA staff on this policy and on all matters relating to the Data Protection Act.