RESPONSE PLAN FOR PERSONAL DATA BREACHES

Equality

In accordance with the Equality Act 2010, we will make any reasonable adjustment necessary to assist those with a protected characteristic or disability to engage fully with the Commission. If you require any assistance with this document please let us know.

We are also a member of Happy to Translate (HTT) and can provide language assistance with this document or make it available in alternative formats if required upon request.

☎ 0141 270 7030

info@sccrc.org.uk

1.0 Introduction

1.1 The Commission takes appropriate measures against the unauthorised or unlawful use of the personal data that it processes and against the accidental loss and destruction of, or damage to, such data. However, if any such personal data breaches occur, the Commission has adopted this response plan.

2.0 Definition

2.1 A personal data breach may be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. This means that a breach is more than just losing personal data.

2.2 Personal data breaches can include:

- Unauthorised third-party access to personal data
- Deliberate or accidental action (or inaction) by a data controller
- Sending personal data to an incorrect recipient
- The loss or theft of computing devices containing personal data

- Alteration of personal data without permission
- Loss of availability of personal data

3.0 Containment and recovery

3.1 The Commission will try to contain the breach, and will assess the potential adverse consequences for individuals, based on how serious or substantial those are, and how likely they are to happen.[1]

3.2 It will decide who should take the lead in investigating the breach, and will make sure that he or she has the appropriate resources to investigate the breach.

3.3 It will establish who needs to be told about the breach and what they are expected to do to assist in the containment exercise (which could be closing a compromised section of the network, finding a lost piece of equipment or simply changing an access code).

3.4 It will establish whether there is anything it can do to recover any losses and to limit the damage the breach can cause (which might involve the physical recovery of equipment or the restoration of the lost or damaged data).

3.5 It will inform the police, where appropriate.

4.0 Notification of breach

4.1 When a personal data breach has occurred, the Commission will establish the likelihood and severity of the resulting risk to people's rights and freedoms. It will assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of that occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher.

4.2 In assessing the risk to people's rights and freedoms, the Commission will focus on whether there are any potential negative consequences for individuals, which could include emotional distress, and physical and material damage,[2] and it will make such an assessment on a case-by-case basis. That is to say, it will assess whether such a breach, if unaddressed, is likely to have a significant detrimental effect on individuals, resulting in, for example:

- Discrimination

[1] Recital 87 of the General Data Protection Regulation (GDPR) makes clear that, when a security incident takes place, an organisation should quickly establish whether a personal data breach has occurred and, where it has, promptly take steps to address it, including telling the Information Commissioner's Office (ICO) if required.

[2] Recital 85 of GDPR provides: "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, identity 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."

- Damage to reputation
- Financial loss
- Loss of confidentiality or any other significant economic or social disadvantage.

4.3 Where it is likely that there is such a risk, the Commission will notify the Information Commissioner's Office (ICO) about the breach.

4.4 Where it notifies the ICO about a data breach, the Commission will do so without undue delay, and not later than 72 hours after it became aware of the breach.

4.5 When reporting a breach, the Commission will provide a description of the nature of the personal data breach, including:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the Commission's data protection officer
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

4.6 Where a breach is likely to result in a high risk[3] to the rights and freedoms of individuals, the Commission will inform those individuals concerned directly and without undue delay. In assessing whether the breach is likely to result in such a high risk, the Commission will assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of that occurring.

4.7 Where it decides to tell individuals about a breach, the Commission will describe, in clear and plain language, the nature of the breach and will provide the following information:

- The name and contact details of the Commission's data protection officer
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

[3] A "high risk" means the threshold for informing individuals is higher than for notifying the ICO.

The law enforcement purposes

4.8 Where it is processing data for the law enforcement purposes, in terms of Part 3 of the Data Protection Act 2018 (DPA), and there is a breach of such data, the Commission will apply the relevant provisions concerning notification to the ICO and the data subjects, namely ss67 and 68, the terms of which largely mirror the above-mentioned steps concerning notification.

4.9 The Commission's obligation to tell the ICO about a personal data breach does not apply where the breach is unlikely to result in a risk to the rights and freedoms of individuals.[4] Its obligation to tell the data subjects about the personal data breach does not apply where, for example, the Commission has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach.[5]

5.0 Evaluation and response

5.1 The Commission will record all breaches, regardless of whether it reported them to the ICO. It will record the following information about a personal data breach:

- The facts relating to the breach
- Its effects
- The remedial action taken[6]

5.2 The Commission's Audit Committee will have responsibility for oversight of all data breaches including:

- Receiving reports from the Commission's data protection officer on all data breaches
- Considering the cause of individual breaches, and action taken in compliance with this policy
- Identifying any additional control actions to minimise the risk of future breaches.

5.3 The Commission will evaluate the effectiveness of its response to any breach and will carry out the following procedures in order to prevent a recurrence of the breach:

- Re-examining what, where and how personal data are held
- Establishing where the biggest risks lie, and identifying further potential weak points in its existing security measures
- Making sure that the methods of transmission of data are secure and that it discloses only the minimum amount of data necessary
- Providing the appropriate staff training

Date first approved	16 August 2013
Date of last review	24 July 2026
Date of next review	24 July 2027

[4] Section 67(2) of DPA.
[5] Section 68(3)(a) of DPA.
[6] See Article 33(5) of GDPR; see also ss67 and 68 of DPA.