Ombwdsmon
Ombudsman
Cymru • Wales

Information Security Incident Management Policy & Procedures

Mae’r ddogfen hon hefyd ar gael yn y Gymraeg.

This document is also available in Welsh.

Contents

1. Introduction and definitions

1.1 The PSOW holds a large amount of personal data and special category information. Every care must be taken by all staff to protect this information. If data is lost or shared inappropriately, we must take appropriate action to minimise any associated risks.

1.2 The loss or inappropriate sharing of data, whether actual or suspected is referred to in this document as an ‘information security incident’ (ISI).

1.3 This document sets out PSOW’s procedure for considering incidents leading to a potential personal data breach of the Data Protection Act 2018 (DPA) or the UK General Data Protection Regulation (GDPR) and associated laws. The process is based on ICO guidance[1] and guidance issued by the Article 29 Data Protection Working Party[2].

1.4 An information security incident can affect the confidentiality, integrity or availability of data. An incident must be assessed quickly to establish if there has been a breach of personal data.

1.5 A personal data breach is defined as:

> …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. It also means that a breach is more than just about losing personal data.[1]

1.6 An assessment may conclude the incident was not a personal data breach. However, the assessment provides an opportunity to review organisational and technical measures to mitigate possible future risks.

[1] ICO's Guide on personal-data-breaches

[2] Article 29 Working Party: Guidelines on personal data breach notification under Regulation 2016/679 (Revised and Adopted 6 Feb 2018)

2. Types of incidents

2.1 Examples of incidents can include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction).
- Sending personal data to an incorrect recipient or without proper authorisation.
- Devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data, for instance because it it has been encrypted by ransomware, or accidentally lost or destroyed.

3. Considering risks

3.1 There are individual and organisational risks that need to be considered when investigating an incident. Compromise of information confidentiality, integrity, or availability of data could result in:

- reputational damage,
- detrimental effect on service provision,
- harm to individual(s),
- legislative non-compliance, and/or
- financial costs.

3.2 When considering the possible negative consequences for individuals Recital 85 of the 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 the [individual]…”

3.3 The GDPR Recital provides a list of possible consequences for the individual:

- Loss of control for over their personal data.
- Limitation of their rights.

- Discrimination.
- Identity theft or fraud.
- Financial loss.
- Unauthorised reversal of information that was pseudonymised.
- Damage to reputation.
- Loss of confidentiality.
- Any other significant economic or social disadvantage.

3.4 This Procedure aims to mitigate these risks by ensuring:

- All staff, contractors and third-party users are aware of the procedure for reporting incidents and their responsibility to promptly report any observed or suspected incident, or information security concern.
- Reported incidents or concerns are promptly followed up in accordance with this procedure.

- That following recovery from the incident existing controls are examined to determine their adequacy, and corrective action is taken to minimise the risk of similar incidents occurring.
- There are mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified, monitored, and reported.

4. The procedure

4.1 PSOW's procedure for assessing information security incidents is split into the following four steps:

i) Containment and recovery.
ii) Assessing the risk.
iii) Notification.
iv) Evaluation and response.

4.2 An incident Investigation Form should be completed to demonstrate the steps taken.

4.3 The group of people responsible for reacting to reported incidents includes:

• The Chief Operating Officer & Director of Improvements (COODOI).
• The Chief Legal Adviser and Director of Investigations (CLADOI).
• The Head of IT Services (Head of IT).
• A relevant Manager for the service.
• The Information Governance Manager (IGM).

4.4 Any incident should be reported to the IGM and a member of the Management Team as soon as it comes to light using the incident Investigation Form. Any cyber security issues must be reported to the Head of IT immediately, for example if an email phishing link was clicked on in error or any unauthorised risk. IT needs to take urgent action to protect the PSOW network.

4.5 The IGM and / or relevant Manager should notify the COODOI and CLADOI as soon as possible to ensure they are aware of the matter.

4.6 The incident will be logged centrally by the IGM, who will monitor progress with the management and investigation of the incident.

4.7 The incident Investigation Form is available from the Information Governance Helpdesk pages on The HUB.

5. **Containment and recovery** (step 1)

5.1 The member of staff, IGM or a member of the Management Team should take immediate steps to contain the incident, based on the nature of the breach. Actions should be recorded on section 1 of the incident Investigation Form.

5.2 An example of action taken to recover / contain the incident is provided below.

If the incident relates to misdirected post, contact should be made with the recipient to arrange recovery:

- If electronic, the recipient should be asked to confirm permanent deletion of the message (including from their Deleted Items email folder).
- If postal, arrangements should be made for the material to be returned to this office (PSOW to supply return envelope) or collected by a member of staff if local or via a courier [this exact method will depend on the nature of the incident and material involved].

5.3 Where the incident concerns PSOW's website, the Information Governance Manager and the Head of IT should consider whether it is necessary to inform website providers and the Policy and Communications Team. Information will need to be amended or removed immediately as required.

5.4 Where the incident concerns PSOW's internal systems or databases, the Information Governance Manager and the Head of IT should also consider whether it is necessary to notify IT support and systems providers.

6. **Assessment the risk** (step 2)

6.1 Following containment/recovery, the Information Governance Manager and the relevant member Manager should carry out an assessment of the risk associated with the incident using the Assessment and Response Form.

6.2 The Assessment and Response Form consider the potential adverse consequences for individuals based on severity and how likely they are to happen. The following factors are assessed:

- Type of breach (i.e. confidentiality, integrity, availability).
- The type, sensitivity and volume of the data.
- Number of individuals affected.
- Security of the data.

- Ease of identification.
- Severity of consequence / possible harm which may result, including:
  - Financial loss.
  - Distress
  - Reputation.
  - Identity theft.
  - Discrimination.
  - Loss of confidentiality.
  - Unauthorised reversal of pseudonymisation.
- Any special characteristics of the individual(s).
- Severity of consequences to PSOW.

6.3 The Article 29 Working Party says that:

> "This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached."[2]

6.4 Incidents need to be considered on a case-by-case basis, taking account of possible emotional distress, and physical and material damage. Some incidents or breaches will perhaps only likely result in possible inconvenience to PSOW staff. Others may have a significant impact on the individual whose data has been compromised.

6.5 Once an initial assessment is made the ongoing management of the incident should be discussed with the COODOI and CLADOI.

7. Notification of breach (step 3)

7.1 Discussions with the COODOI and CLADOI will determine the action to be taken at steps 3 and 4 (Notification and Evaluation).

7.2 Step 3 involves deciding who should be notified of the breach, based on the assessment of risk.

7.3 Article 33 GDPR requires mandatory breach notification to the ICO unless a breach is unlikely to result in a risk to the rights and freedoms of individuals. It is important to record the rationale for this decision.

7.4 If the Risk Assessment concludes that there is a high risk that the individuals will be put at risk the ICO should be notified without undue delay. Where feasible, within 72 hours of having become aware of the incident. The National Cyber Security Centre (NCSC) should be notified in the case of a cybersecurity incident and can be reported through Action Fraud.

7.5 Article 34 also requires the individuals to be notified of any breach likely to result in a high risk to their rights and freedoms without undue delay.

7.6 If the outcome of the risk assessment is that the level of risk is medium then advice should be sought from the ICO. In the case of a cybersecurity incident, it will be necessary to consider seeking advice from the NCSC and report the incident to Action Fraud.

7.7 Completion of the ICO's self-assessment form may help with the assessment of risk. A phone call to them to discuss the incident may also be helpful and as they can offer advice on managing the risk and mitigating its effect. If necessary, they will take details of the breach over the telephone.

7.8 In the event of a decision to notify the ICO, PSOW should use ICO's Breach Notification Form. The A29 Working Party Notification Flowchart is also available at the end of this document, along with the risk matrix.

8. Evaluation and response (step 4)

8.1 Section 4 of the incident Investigation Form details any actions to be taken in light of the incident – for example, changes to policies, processes or guidance or developments to IT systems. Where possible, these actions should also be assigned to a member of staff for completion.

8.2 It is for the line manager to consider any necessary steps (informal or formal) relating to the staff member who may have been involved in the incident. PSOW is committed to ensuring that there is a culture where staff feel able to report mistakes. Involving staff within the incident management process is important to ensure that lessons are learned, and future risks can be identified as soon as possible and mitigated. Further training may be arranged, or additional guidance may be provided.

The relevant HR policies will be followed where appropriate, though any actions relating to staff performance should not be included on the incident Investigation Form, which may be disclosed to the Information Commissioner's Office.

8.3 The IGM will update the Information Security Incident Register.

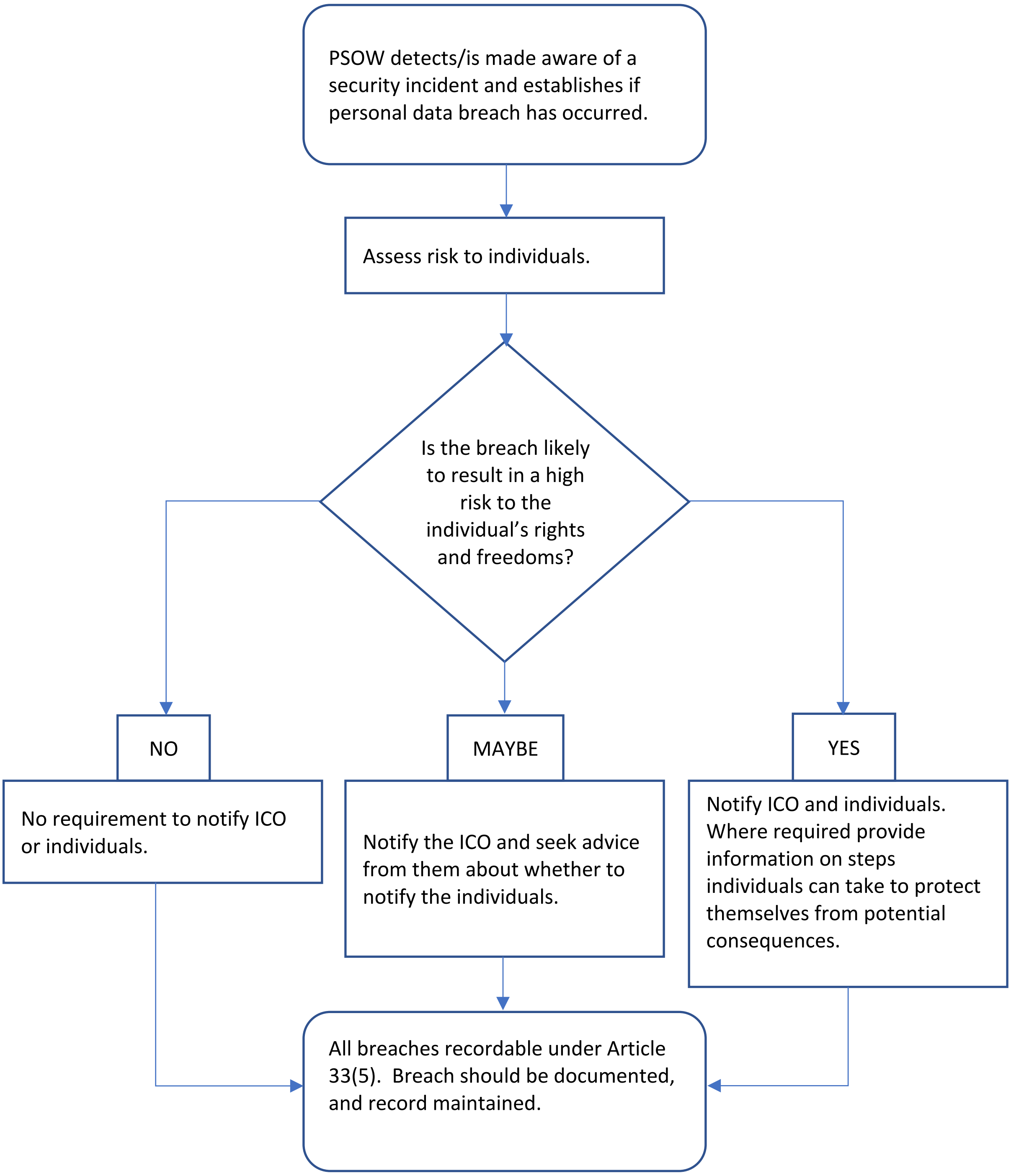
9. Monitoring and review

9.1 Quarterly Information Governance monitoring reports to Management Team provide a summary of incidents, data breaches and any mitigating actions required.

9.2 Incidents and breaches are also reported on a quarterly basis to ARAC.

9.3 This Policy and Procedure will be reviewed every two years.

10. Appendix one: Flowchart of notification requirements[3]



PSOW detects/is made aware of a security incident and establishes if personal data breach has occurred.

Assess risk to individuals.

Is the breach likely to result in a high risk to the individual's rights and freedoms?

NO

No requirement to notify ICO or individuals.

MAYBE

Notify the ICO and seek advice from them about whether to notify the individuals.

YES

Notify ICO and individuals. Where required provide information on steps individuals can take to protect themselves from potential consequences.

All breaches recordable under Article 33(5). Breach should be documented, and record maintained.

[3] Based on Article 29 Working Group flowchart in the A29WP Guidelines (see footnote 2).