

## PDB Assessment Methodology

<b>Document name</b>	PDB assessment methodology
<b>Version number</b>	1.1
<b>Status</b>	Published
<b>Department/Team</b>	Cyber Security
<b>Relevant policies</b>	Security Incident Management Policy
<b>Distribution</b>	Internal
<b>Author/Owner</b>	Operational Security Manager
<b>Approved by</b>	Head of Cyber Security
<b>Date of sign off</b>	June 2023
<b>Review by</b>	June 2025
<b>Security classification</b>	OFFICIAL – ORG USE ONLY

### Key messages

The main objective of this document is to define a recommended methodology for assessing personal data breaches.

### Does this guide relate to me?

This document should be read and understood by all personnel with responsibility for managing our tactical response to personal data breaches.

## Table of contents

1.	Introduction .....	3
2.	Methodology .....	3
3.	Feedback on this document.....	5
4.	Version history.....	5

## 1. Introduction

- 1.1 This purpose of this document is to define a consistent and repeatable method for assessing and prioritising personal data breaches (PDB). The document supports the Security Incident Management Policy.
- 1.2 The scope of this document applies to PDBs that affect manually and electronically processed personal data within our organisation's care.
- 1.3 PDBs are a subset of information security incidents, and may be defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (GDPR Article 4(12) refers).

[Back to Top](#)

## 2. Methodology

### 2.1 Criteria

The main criteria to be assessed are summarised below.

- Data Processing Context (DPC): Addresses the type of data breached, together with a number of factors linked to the overall context of processing.
- Ease of Identification (EI): Determines how easily the identity of the individuals can be deduced from the data involved in the breach.
- Circumstances of breach (CB): Addresses the specific circumstances of the breach, which are related to the type of the breach, including any loss of confidentiality, integrity or availability, as well as any malicious intent.

### 2.2 Priority

To assess the priority of the PDB, and whether the PDB is likely to result in a risk to the rights and freedoms of data subjects, the incident responder should use the following method:

$$SE = DPC + EI + CB$$

Note, the method is advisory, and has been adapted from the ENISA recommendations for a methodology of the assessment of severity of personal data breaches ([www.enisa.europa.eu](http://www.enisa.europa.eu)), which contains a more

detailed description of the main criteria together with aggravating and mitigating factors that may be considered on a case-by-case basis.

### 2.3 Criteria scoring

<b>Data processing context</b>	
Basic score where breach involves simple data, and controller is not aware of any aggravating factors.	0
Basic score where breach involves behavioural or financial data, and controller is not aware of any aggravating or mitigating factors.	1
Basic score where breach involves sensitive data, and controller is not aware of any mitigating factors.	2

<b>Ease of identification</b>	
Personal data protected using strong encryption or otherwise cannot be matched to a subject.	0
Personal data in clear text but cannot be easily matched to a subject without additional information.	1
Personal data in clear text and can be easily matched to a subject.	2

<b>Circumstances of breach</b>	
Personal data: disclosed to known recipients; modified, or not available, but can be restored; and, there is no evidence of illegal processing	0
Personal data: disclosed to unknown recipients; modified, or not available, but cannot be restored; and, there is no evidence of illegal processing	1
Personal data: disclosed, modified, or not available, as a result of malicious behaviour.	2

### 2.4 Priority scoring

<b>Score</b>	<b>Risk</b>	<b>Consequences</b>	<b>Response</b>
0 to 2	Low	Subject may encounter minor inconvenience, which can be overcome without difficulty.	<ul style="list-style-type: none"> <li>May be handled in line with local business processes.</li> </ul>

3 to 4	Medium	Subject may encounter major inconvenience, which can be overcome with few difficulties.	<ul style="list-style-type: none"> <li>• Escalate to Incident Manager.</li> <li>• DPO shall be notified.</li> <li>• Subjects may be notified as appropriate.</li> </ul>
5 to 6	High	Subject may encounter severe consequences, which may prove difficult to overcome.	<ul style="list-style-type: none"> <li>• Escalate to Incident Manager.</li> <li>• DPO shall be notified.</li> <li>• ICO shall be notified.</li> <li>• Subjects shall be notified as appropriate.</li> </ul>

[Back to Top](#)

### 3. Feedback on this document

If you have any feedback on this document, please [click this link](#) to provide it.

[Back to Top](#)

### 4. Version history

Version	Changes made	Date	Made by
1.0	Initial release	June 2021	S Rook
1.1	Minor format changes on review	June 2023	S Rook

[Back to Top](#)