CONTROLLED DOCUMENT

N.B. Employees should be discouraged from printing this document. This is to avoid the risk of out of date printed versions of the document. The Intranet should be referred to for the current version of the document.

DPIA PROCEDURE

CATEGORY:	Procedure
CLASSIFICATION:	Information Governance
PURPOSE:	To lay out the requirements around carrying out Data Protection Impact Assessments.
CONTROLLED DOCUMENT NUMBER:	BG/IG/013
VERSION NUMBER:	003
CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:	Director of Corporate Services
CONTROLLED DOCUMENT AUTHOR:	GDPR Advisor
APPROVED BY:	Director of Corporate Services
APPROVED ON:	July 2024 (V002)
IMPLEMENTED ON:	July 2024 (V002)
REVIEW PERIOD:	Every 3 years - unless changes to legislation, best practice or internal roles and responsibilities
REVIEW DATE:	Latest Review Date: August 2025 – to reflect new Executive Team Structure Next full review date July 2027
ASSOCIATED DOCUMENTS:	DPIA Policy
Essential Reading for: **Information for:**	Trustees and all employees Trustees and all employees

Document Consultation and Review Process

Groups/Individuals who have overseen the development of this Procedure:	**Corporate Governance Team, Senior Leadership Team**
Groups/Individuals Consulted:	**Corporate Governance Team, Senior Leadership Team, PQ&E Committee, Board**

Document version control:

Date	version	Amendments made	Amendments Approved by
2018	V001	Procedures put in place by the then DPO to comply with the GDPR	
October 2024	V002	Procedures reviewed by Consultants – CYBATA and Updated	**Director of Corporate Governance and Company Secretary**
August 2025	V003	Updated to reflect new Executive Team structure and adoption of the term colleague for employee	**Director of Corporate Services**

For the Use of the Corporate Services Team only:

Date added to Register:	2020 – when register introduced
Date Published onHub:	September 2025 – V003)
Does it need to be published on website:	No

CONTENTS

1. DEFINITIONS

In this procedure, we use definitions from the GDPR unless otherwise stated.

'CCOPD' means personal data relating to criminal convictions and offences.

'DPIA' means the assessment that must be carried out in certain situations, contain certain information, and over which there are other obligations, as set out in the GDPR.

'EU GDPR' means the EU General Data Protection Regulation, 2016/679.

'GDPR' means either or both of the EU GDPR and UK GDPR. We will use this when there is little or no difference in the wording of the relevant law for the context.

'Personal data' has the meaning from the GDPR, meaning any information relating to an identified or identifiable natural person ('data subject'), which in turn means a person who can be identified, directly or indirectly from the information.

'Processing' means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

'Special Categories of Personal Data' or 'SCPD' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, an the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

'UK GDPR' means the UK-adopted version of the EU GDPR, which took effect from 1 January 2021 as a result of Brexit.

2. KEY REQUIREMENTS

2.1 Whenever processing of personal data – in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing - is likely to result in a high risk to the rights and freedoms of data subjects, or applicable law otherwise requires it, a DPIA shall be carried out in accordance with the GDPR, with the advice of the Data Protection Officer and the results recorded. DPIAs shall be reviewed at least when there is a change in the risk represented by the processing operation.

2.2 DPIAs must be carried out early in the planning stage of any project or new way of working that involves the processing of personal data, to ensure that risks are identified and controlled as appropriate.

2.3 As above, a DPIA is only required when there is a likely high risk to the rights and freedoms of data subjects, and when otherwise specifically required by law. Changes that do not affect personal data in that project or business activity – such as moving a button on a website or app or adding a screen

with no personal data impact - do not need the DPIA to be revisited. However, this must be carefully considered as many changes can have impacts on personal data.

2.4 If no personal data is processed, no DPIA need be carried out on the project or policy/way of working.

When a DPIA must be carried out

2.5 A DPIA is not mandatory for every processing operation: it is required when there is a likely high risk to the rights and freedoms of natural persons. A single DPIA may address a set of similar processing operations that present similar high risks.

2.6 The depth and breadth of the DPIA will depend on the level of likely risk presented.

2.7 The GDPR sets out a non-exhaustive list of 4 cases when a DPIA is required:

i. a *systematic and extensive evaluation* of personal aspects relating to natural persons which is *based on automated processing, including profiling*, and on which decisions are based that produce *legal effects* concerning the natural person or *similarly significantly affect* the natural person;

ii. *processing on a large scale of SCPD or CCOPD*;

iii. a *systematic monitoring of a publicly accessible area on a large scale*; and

iv. any *processing included in a list published* by [the Information Commissioner's Office] or the European Data Protection Board ('**Board**', replacing the Article 29 Working Party) of the kind of processing operations which are subject to the requirement for a DPIA.

2.8 In practice for Brunelcare, numbers 1 and 4 above are the most likely.

When a DPIA need not be carried out

2.9 A DPIA need not be carried out if there is no likely high risk to data subjects and it is not otherwise required by applicable law.

2.10 No DPIA is required where the processing in question is on the basis of 'compliance with the controller's legal obligation'[1] or 'public interest / exercise of official authority'[2] and (1) has a legal basis – if the EU GDPR applies - in EU law or the law of the Member State to which the controller is subject or – if the UK GDPR applies – UK law to which the controller is subject, (2) that law regulates the specific processing operation or set of operations in question, and (3) a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, unless Member States (or the UK respectively) deem it to be necessary to carry out such an assessment prior to processing activities.

[1] Article 691)(c)

[2] Article 6(1)(e)

Contents of a DPIA

2.11 Under the GDPR, DPIAs must at least contain:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects in question; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

2.12 The GDPR leaves a great degree of flexibility in how to carry out the DPIA and the Article 29 Working Party notes that controllers have broad discretion in what exactly their DPIA looks like

DPIAs & consultations

2.13 Brunelcare shall consult with the ICO as required by the GDPR and take into account any advice from the ICO.

Approved Codes of Conduct

2.14 The GDPR allows for approval of codes of conduct (Article 40) and for adherence to an approved code to be used as an element by which to demonstrate compliance with various requirements in the GDPR including DPIAs. If necessary or appropriate, Brunelcare will review such codes for relevance and fit for our operations.

3. ENFORCEMENT

3.1 All Brunelcare colleagues are responsible for following this procedure. Failure to follow this procedure when required could be grounds for disciplinary proceedings against an employee, which may result in disciplinary action including termination of employment.

3.2 Failure to follow this procedure when required by any non-employee such as a temporary worker, contractor or supplier may be a breach of their contract with Brunelcare and grounds for damages or termination.

4. OWNERSHIP

4.1 The Director of Corporate Services is responsible for maintaining this procedure and related awareness programs.