Data Protection Impact Assessment

Version: 1.02

Contents

1. Policy Summary

- A DPIA is a written assessment which helps BCC identify, evaluate, and mitigate risks and privacy impacts to data subjects arising as a result of processing their personal data. A DPIA must be undertaken **before** the processing of any personal data which is 'likely to result in a high risk to the rights and freedoms' of data subjects. It ensures compliance with data protection legislation and other legal and regulatory requirements. It helps BCC to:
    - identify privacy risks to individuals.
    - anticipate and address the likely impacts.
    - foresee problems and find solutions.
    - Protect our reputation and offer assurance to stakeholders.

- DPIAs (Data Protection Impact Assessments) are a fundamental part of BCC identifying risks that are associated with the processing of personal data.

- They are the responsibility of the IAO (Information Asset Owner), Lead Custodian, PMO (Project Manager Officer) or BAU Change Leads to ensure that at the stage of any new or changed practices that a DPIA is completed, where the data being processed could cause high risks to the rights and freedoms of individuals.

- If External data processors are to be used, consult with them whilst creating the DPIA. It is also a requirement to complete the Information Security External Organisation Questionnaire which can be obtained from Information Security and also if AI is the tool being considered then the Data Ethics Impact Assessment needs to be completed.

- DPIA's must be completed by BCC and not 3rd parties

- The first stage is to complete DPIA Screening Questionnaire.

- Do not use acronyms without showing the full description when creating a DPIA Screening questionnaire/full DPIA.

- DPIA Screening questionnaire and full DPIAs will be reviewed and assessed by the Data Protection Team
- Any new systems, data migrations, testing where the data is not anonymised, or dummy data must be referred to Information Security to ensure that they have suitable Operational and Technical measures in place before they are bought/implemented.

- Failure to conduct a DPIA could result in a fine and/or disciplinary action and place service users data at risk. The full details of the Policy are contained in the following pages. It provides the details on when a DPIA is required, the responsibility of completing a DPIA and also the implications regarding the failure to carry out a DPIA to the organization

A copy of the full Data Impact Assessment policy is available on request.

2. Definitions

The Data Protection Policies Glossary contains definitions of the key data protection terms and can be found here.

2.1 DPIA – Data Protection Impact Assessments is a written assessment which helps BCC identify, evaluate, and mitigate risks and privacy impacts to data subjects arising as a result of processing their personal data.

2.2 Project Change – a new project or programme identified by Corporate Leadership Board (CLB) and managed through the PMO project portfolio.

2.3 BAU Change – a business as usual change not governed by the PMO but which still impacts upon the personal data processing of an individual e.g. a business process change, a cross skilling of a team, a new Software Request, a retrospective service review, a request for an SPO External site, new data processing arrangement with a supplier, a new contracts with a supplier, a waiver with an existing supplier or a data sharing initiatives involving personal data.

2.4 PMO – Project Management Office – is a department within our organisation that looks to standardize and document the best project management techniques. The PMO sets the scope for projects, creates Project teams to ensure effective implementation.

2.5 SIRO – Senior Information Risk Officer - Fosters a culture that values, protects and uses information for the public good. Leads the organisation's response on information risk. Responsible for ensuring the organisation's information is managed securely. Is a champion at board level.

2.6 IAO – Information Asset Owner - who are responsible and accountable for the specific, defined information assets within their remit. Information Assets are identifiable collections of information or data which have value to the Council for its business. They are responsible for managing the risks to personal information and business critical information held within a department.

2.7 IGB – Information Governance Board - is our strategic body that provides leadership across the organisation for the management of information assets & information risk management.

2.8 CLB – Corporate Leadership Board

2.9 DPO – Data Protection Officer – provides advice to the organisation on the continued compliance with the combined data protection laws, assists in ensuring the documentation required under the combined data protection boards is maintained, provides training and guidance to the organisation.

2.10 Artificial Intelligence (AI)- is an umbrella term used to describe 'Any computer system that can perform tasks usually requiring human intelligence. This could include visual perception, text generation, speech recognition or translation between languages.'

2.11 Data Ethics Impact Assessment – This assessment should be carried out before deploying a new algorithm, predictive model or other profiling technique. The term "algorithm" should be read to include any data analytics techniques that collect, combine and process data used to determine outputs that may have legal effect upon an individual or group of individuals.

3. Applicable Standards/Legislations

UK General Data Protection Regulation
DPA (Data Protection Act) 2018

4. Version Awareness

Please note that documents printed or downloaded are uncontrolled documents and therefore may not be the latest version.

Title:	Data Protection Impact Assessment (DPIA) Policy
Description:	Policy setting out Bristol City Council's approach to identifying the need for, undertaking and implementing data protection impact assessments and who in BCC is responsible for ensuring a DPIA is completed
Author:	Data protection
Scope:	All employees
Document Status:	Published
Version:	1.02
Classification:	Official

Create Date:	14.06.2021
Approval Body:	BCC Information Governance Service
Date Approved:	28.11.2023
Document Review Period:	Annually.
Next Review Date	November 2025
Disposal Period:	Permanent

Version	Date	Details
1.01	31/10/2023	Updated content, included AI requirements and format for ease of reading
1.02	11/11/2024	Annual Review, updates made to summary page to include reference to AI, Data Impact Ethics Assessment and Information Security questionnaire. Definitions added.