Data Protection Impact Assessment

Version: 1.01

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:	Draft
Version:	1.01
Classification:	Official
Create Date:	14.06.2021
Approval Body:	BCC Information Governance Service
Date Approved:	
Document Review Period:	Annually.
Disposal Period:	Permanent

Version	Date	Details
1.01	14.06.2022	Updated content

Contents

1. Purpose of this Policy

This policy sets out BCC's obligations to undertake a Data Protection Impact Assessment where any processing of personal data is 'likely to result in a high risk to the rights and freedoms of individuals', as set out in Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018.

1.1. 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 carryout a DPIA to the organisation.

1.2. . The combined UK data protection Laws (UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (DPA 2018)) regulate the processing of 'personal data'. Data protection legislation contains data protection principles which must be complied with when processing personal data, including the incorporation of safeguards to ensure that the rights and freedoms of data subjects are protected.

1.3. Employees of BCC are obliged to comply with the combined UK data protection Laws (UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (DPA 2018)) when processing personal data on our behalf. A breach of the combined UK data protection Laws may result in criminal proceedings and may result in disciplinary action which could result in dismissal.

1.4. Data Processors acting on the instructions of BCC are obliged to comply with this policy when processing personal data on our behalf, as detailed in the contract between BCC and the processor.

2. R.A.C.I. Model

2.1. The RACI model is used for clarifying and defining roles and responsibilities in cross-functional or departmental projects and processes as detailed below:

- **Responsible**: All staff, third-party providers of services or support who process personal data for or on behalf of Bristol City Council.

- **Accountable:** Head of Information Assurance.
- **Consult:** Information Governance Board.
- **Inform**: All staff

3. Introduction

3.1. Conducting a DPIA is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals.

3.2. Bristol City Council (BCC) is committed to using people's personal data properly and legally, to ensure it is used only in ways people would reasonably expect and that it stays safe. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we collect, store and process personal data about our citizens, service users, employees, suppliers and other third parties. We recognise that the correct and lawful treatment of this data maintains trust and confidence in the organisation and provides for successful service delivery.

3.3. This policy should be read and complied with in conjunction with the following policies and guidance:

3.3 BCC's data protection policy gives further information about BCC's obligations and how it complies with them when processing personal data.

4. Definitions

The Data Protection Policies Glossary contains definitions of the key data protection terms

4.1. 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.

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

4.3. **BAU Change** – a business as usual change not governed by the Project Management Office (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 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.

4.4. **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

4.5. **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.

4.6. **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.

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

4.8. **CLB** – Corporate Leadership Board

4.9. **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.

5. Responsibilities

5.1 Data controller – BCC is the data controller.

5.2 Data Protection Officer (DPO) – is responsible for assisting BCC to monitor internal compliance with data protection legislation and this policy. The DPO must be consulted in relation to any DPIAs undertaken making their recommendations clear before a DPIA is signed off. The DPO can be contacted at data.protection@bristol.gov.uk

5.3 Information Governance service – is responsible for providing advice, support, and co-ordination in relation to data protection to the Information Asset Owners, the Lead Custodians and the DPO.

5.4 Information Asset Owners (IAO) – are responsible for the lawful processing of personal data within their service area, including ensuring that the need for a DPIA is recognised and that required DPIAs are undertaken. They are accountable for the risks identified within a DPIA and sign off approval of these risks and the DPIAs relating to the Information Assets they own.

5.5 Lead Custodian(s) – in relation to DPIAs, they are responsible for supporting the IAO to ensure that all relevant employees understand the circumstances in which a DPIA should be undertaken and that the employee or team leading a project, initiative or system undertakes a DPIA.

5.6 Project Management Office (PMO) - in relation to DPIAs, they provide project resource to support the completion of a project DPIA.

5.7 Project Managers / Business as Usual (BAU) Change Leads - are responsible for carrying out the DPIA process.

5.8 All employees involved in the development of projects, initiatives and

systems are responsible for ensuring they are aware of this policy and understand the circumstances in which a DPIA should be undertaken.

6. DPIA – What is it, how is it identified and undertaken

6.1 DPIAs are not just a compliance exercise. An effective DPIA allows us to identify and fix problems at an early stage, bringing broader benefits for both individuals and our organisation.

6.2 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.

6.3 A DPIA is required to be undertaken where proposed processing activity is likely to result in a high risk to the rights and freedoms of data subjects or to where processing is of a large scale, involves automatic decision-making including profiling or monitoring which decides on access to services and opportunities or involves sensitive data or vulnerable individuals or where data matching across various datasets is carried out. The UK GDPR and ICO require a DPIA to be undertaken in the circumstances outlined in the ICO guidance.

6.4 Responsibility for carrying out the DPIA process is formally recorded and assigned to a Project Manager / BAU Change Lead. It is the responsibility of

the Lead Custodian to ensure the need for a DPIA is assessed and DPIA is completed if required.

6.5 At the 'outline business case' stage of a project or triggered by a new BAU change, the Project Manager / BAU Change Lead completes the DPIA screening section of the DPIA, saves the entry and submits it for review by Data Protection team to decide if a full DPIA is required.

6.6 Where a DPIA is not required, the reasons for this are clearly documented and kept as a record of the decision made for future reference and review.

6.7 If required by the Information Governance service, the Project Manager / BAU Change Lead complete a full DPIA following the guidance on data protection impact assessments.

6.8 It may be necessary to consult with internal and external stakeholders. Contracts with third parties, including data processors, should include an obligation on them to assist DPIA consultations. Where these are professional advisers and other experts, the scope and cost of their involvement should be approved by the DPO.

6.9 The approved DPIA forms part of the project risk assessment and official project documentation where applicable.

7. Summary

- DPIAs are a fundamental part of BCC identifying risks that are associated with the processing of personal data.
- They are the responsibility of the IAO, Lead Custodian, PMO 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.

- Where external data processors are to be used, BCC consult with them whilst creating the DPIA
- Any new systems are referred to Information Security to ensure that they have suitable Operational and Technical measures in place before they are bought/implemented.

8. Standards

UK General Data Protection Regulation 2018

Data Protection Act 2018