BRENTWOOD BOROUGH COUNCIL

Data Protection Impact Assessments Policy

Title:	Data Processing Impact Assessments Policy
Purpose:	To ensure we assess and manage risk appropriately around personal data when adopting new or amended systems, contracts and processes
Owner:	Data Protection Officer
Approved by:	Head of Legal Services
Date:	March 2018
Version No:	2.0
Status:	APPROVED BY PP&R COMMITTEE 12/3/18
Review Frequency:	Annually or when changes made to relevant Information Governance law
Next review date:	As above
Meta Compliance	IT to ensure policy subject to this

Introduction

This policy defines the Data Protection Impact Assessments Policy and is part of the Information Governance suite of policies. If you require advice on this or any information governance matter, please contact the council's Data Protection Officer (DPO). Further information and resources including training and other online support are available on the council's intranet.

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

Data protection impact assessments (DPIAs) help us identify, assess and mitigate or minimise privacy risks with data processing activities. They are particularly relevant when a new data processing process, system or technology is being introduced.

DPIAs also support the accountability principle, as they help the council to comply with the requirements of the General Data Protection Regulation (GDPR) and demonstrate that appropriate measures have been taken to ensure compliance.

The Legal Requirement

Article 35 of the GDPR states:

"Where a type of processing 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 natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

When should I do it?

A DPIA should be conducted as early as possible in any new project, so that its findings and recommendations can be incorporated into the design of the processing operation.

What must I do?

1. If you are managing any initiative to create a new process or contract or amend an existing process or contract which involves the use of personal data or business sensitive data, you must contact the Data Protection Officer (DPO) to begin the Data Processing Impact Assessment (DPIA) process.

2. If you are managing an initiative which requires a DPIA, you must begin the DPIA process in the planning phase of any project cycle or new contract.

3. DPIA's must be approved* before any activity being considered under the DPIA is implemented.

4. The owner of the process being considered under a DPIA is responsible for drafting the DPIA.

5. *DPIA's must be reviewed and approved by the service manager and Data Protection Officer in every case.

6. The Data Protection Officer must keep a central record of DPIA's carried out by Services; the DPIA's will identify risks and mitigations and approvals.

7. The Data Protection Officer will monitor performance against this policy and report to the Senior Information Risk Officer on areas for improvement.

8. The Data Protection Officer will review DPIA's to ensure that the requirements identified have been fully implemented.

Why must I do it?

1. Known as ***privacy by design***, the embedding of data privacy assessment into the design of projects can have the following benefits:

   - Potential problems are identified at an early stage.
   - Addressing problems early will often be simpler and less costly.
   - Increased awareness of privacy and data protection across the organisation.
   - Organisations will be less likely to breach the GDPR.
   - Actions are less likely to be privacy intrusive and have a negative impact on individuals.

2. To comply with the Information Commissioner's Code of Practice supporting compliance with the Data Protection Act, which may be viewed at:

   https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

3. A DPIA may arrive at an outcome that the proposals in an initiative are not appropriate due to the degree of risk to the Council of breaching the Data Protection Act. In such instances, the Data Protection Officer will suggest possible alternatives, but may refuse to approve the proposal. If work has already begun on implementing the proposal and contractual arrangements have been entered into before being approved under a DPIA, this would represent a breach of this policy. This may result in the discontinuance of work already commenced and present BBC with legal, contractual and financial consequences.

4. The approval of a DPIA is the authorisation that BBC is satisfied that ht risks of the proposal are acceptable. This policy is breached by implementing a proposal involving personal data without prior DPIA approval, rather than only in the event of something going wrong.

5. The Data Protection Officer can provide advice on what the DPIA needs to include but cannot complete the form on your behalf. The review of the DPIA needs to be objective.

6. To review and audit the quality of the process. To ensure recommendations in the DPIA have been implemented. To assist with future reviews on the same processes.

7. To ensure the process is working and refinements are made to improve performance.

8. To ensure recommendations have been adopted.

How must I do it?

1. If your initiative requires technical IT support, contact the IT manager in the first instance.

2. Once you have identified that personal data will be involved in your proposed project/contract, you should contact the Data Protection Officer for an initial discussion around your proposals and to run through the DPIA form.

3. If in doubt about the progress or status of your DPIA, contact the Data Protection Officer.

4. Use the Data Processing Impact Assessment Form within the Code of Practice document contained in the above-mentioned link.

5. Each DPIA will be reviewed by the DPO and proposals reviewed to assess with the process owner risks and consider suggestions for risk mitigation and approval of the DPIA once sufficient mitigation has been demonstrated.

6. The DPO will maintain a central record of all DPIA's for audit and reference/precedent purposes.

7. Reporting on statistics re: DPIA's received, implemented and breaches of policy.

8. DPO to ascertain from the relevant Service Manager that adequate controls are in place.

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you. The Council as well as those individuals affected is also at risk of financial and reputational harm. Fines of up to €20,000,000 may be imposed on Councils for serious data breaches. Please report any actual or potential data breaches or other concerns relating to information governance to the Data Protection Officer as soon as possible.

This document includes a DPIA template for you to use.

References:

GDPR 2016

Data Protection Act 2018

Conducting Privacy Impact Assessments Code of Practice (ICO)

Human Rights Act 1998