Data Protection Impact Assessment Guidance

Author: Rachel Everitt

Date: October 2024

Version: v0.2

Title	Data Protection Impact Assessment Guidance
Author	**Rachel Everitt**
Owner	**Data Protection Officer**
Created	**March 2022**
Approved by	**Audit Committee**
Date of Approval	**February 2025**
Review Date	**February 2027**

Document Version Control

Document Version Control	
Issue Number	Date
0.01	March 2022
0.02	October 2024

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Introduction

Data Protection Impact Assessments (DPIA's) help to identify and minimise the data protection risks of a project. This should be used when introducing new or amending existing systems or processes which involve personal data. To support with identifying when a DPIA needs to be completed the DPIA Screening Questionnaire can help indicate when it is needed.

This guidance sets out how Bury Council will carry out DPIA's and is supported by a template DPIA. It is part of Bury Council's Information Governance Framework and should be read in conjunction with the other policies and procedures within the framework.

2. DPIA process

The following steps must be taken when completing a DPIA.

Step 1: Identify the need for a DPIA

A DPIA must be completed for any processing that is likely to result in high risk to individuals.

In particular, the UK GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires you to do a DPIA if you plan to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);

- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice (‘invisible processing’) (in combination with any of the criteria from the European guidelines);
- track individuals’ location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual’s physical health or safety in the event of a security breach.

A DPIA may also be required for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Use the Data Protection Impact Assessment screening tool to help you determine if a DPIA is required. If the answer is ‘Yes’ to any of the questions on the screening tool, a DPIA should be completed.

Step 2: Describe the processing

We need to understand how and why you are using the data, make sure you answer each of the following questions:

What is the nature of the processing? This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether you use any processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

What is the scope of the processing? This should include, for example:

- the nature of the personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

Personal data is defined as data relating to a living individual (a data subject) who can be identified, directly or indirectly, from that data.

Special Category personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Biometrics (where used for identification)

What is the context of the processing? This is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:

- the source of the data;
- the nature of your relationship with the individuals;
- how far individuals have control over their data;
- how far individuals are likely to expect the processing;
- whether these individuals include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern;

- whether you have considered and complied with relevant codes of practice.

What is the purpose of the processing? is the reason why you want to process the personal data. This should include:

- your legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for you or for society as a whole.

Step 3: Consider consultation

You need to document how you will seek the view of anyone who will have an interest in the project. Does anyone else from within the Council need to be involved – IT, legal, procurement, HR? Are there any external partners involved?

ICO guidance states that if the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public-consultation process, or targeted research. This could take the form of market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

If for any reason, your DPIA decision differs from the views of individuals, you need to document your reasons for disregarding their views.

Step 4: Assess necessity and proportionality

In this section you need to describe how your plans help achieve your purpose. Is there another way to achieve your purpose? Is there any legislation that supports you collecting this data?

GDPR legislation states that you should include how you ensure data protection compliance, which are a good measure of necessity and proportionality. In particular, you should include relevant details of:

- your lawful basis for the processing;
- how you will prevent function creep;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation;
- how you intend to provide privacy information to individuals;
- how you implement and support individuals' rights;
- measures to ensure your processors comply; and
- safeguards for international transfers.

Step 5: Identify measures to mitigate risk

You need to consider whether there could be any impact on individuals including any harm or damage your processing could cause. This could be physical, emotional or material.

Consider whether the processing could contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

List any risks on the DPIA and assess the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk.

You must make an objective assessment of the risks. The ICO has produced a helpful structured matrix to think about likelihood and severity of risks:

Severity of impact	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

If you need help identifying risks, please contact the Risk Management team for advice; riskmanagement@bury.gov.uk

Step 6: Identify measures to reduce risk

For any risks that were identified as being medium or high risk at Stage 5, you should consider options for reducing the risk, for example:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;

- using a different technology;
- putting clear data-sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

  This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks.

For each measure you should document

- whether this will eliminate or reduce the risk
- weather the risk has been accepted if all measures to reduce or eliminate the risk are in place
- any residual risk after taking these measures

Step 7: Sign off and record outcomes

Once you have completed the DPIA you should send it to the Policy and Compliance Team for the Data Protection Officer to review. The DPO may request further information or ask you to review sections before approving the DPIA.

Once the DPO has approved the DPIA, it should be sent to the Policy and Compliance Team; IG@bury.gov.uk, for filing.

Consulting the ICO

You do not have to consult the ICO on every DPIA. However, if there is still a high risk which you have accepted cannot be reduced or eliminated, you will need to consult the ICO before you can go ahead with the processing. The DPO will provide advice on whether this is required.

Step 8: Keep under review

You are responsible for keeping the DPIA under review. If there is a substantial change to the nature, scope, context or purposes of your processing you will need to repeat this process in full.

3. Processing likely to result in high risk

The ICO has provided examples which a DPIA is required for. If your project relates to any of these processes, please contact the DPO for advice:

Type of processing operation(s) requiring a DPIA	**Description**	**Non-exhaustive examples of existing areas of application**
Innovative technology	Processing involving the use of new technologies, or the novel application of existing technologies (including AI). A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions) when combined with any other criterion from WP248rev01.	• Artificial intelligence, machine learning and deep learning • Connected and autonomous vehicles • Intelligent transport systems • Smart technologies (including wearables) • Market research involving neuro-measurement (i.e. emotional response analysis and brain activity) • Some IoT applications, depending on the specific circumstances of the processing
Denial of service	Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special-category data.	• Credit checks • Mortgage or insurance applications • Other pre-check processes related to contracts (i.e. smartphones)
Large-scale profiling	Any profiling of individuals on a large scale	• Data processed by Smart Meters or IoT applications • Hardware/software offering fitness/lifestyle monitoring • Social-media networks • Application of AI to existing process

Type of processing operation(s) requiring a DPIA	Description	Non-exhaustive examples of existing areas of application
Biometric data	Any processing of biometric data for the purpose of uniquely identifying an individual. A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion from WP248rev01	• Facial recognition systems • Workplace access systems/identity verification • Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition)
Genetic data	Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject. A DPIA is required for any intended processing operation(s) involving genetic data when combined with any other criterion from WP248rev01	• Medical diagnosis • DNA testing • Medical research
Data matching	Combining, comparing or matching personal data obtained from multiple sources	• Fraud prevention • Direct marketing • Monitoring personal use/uptake of statutory services or benefits • Federated identity assurance services
Invisible processing	Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate	• List brokering • Direct marketing • Online tracking by third parties • Online advertising • Data aggregation/data aggregation platforms

Type of processing operation(s) requiring a DPIA	Description	Non-exhaustive examples of existing areas of application
	effort (as provided by Article 14.5(b). A DPIA is required for any intended processing operation(s) involving where the controller is relying on Article 14.5(b) when combined with any other criterion from WP248rev01	• Re-use of publicly available data
Tracking	Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment. A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from WP248rev01	• Social networks, software applications • Hardware/software offering fitness/lifestyle/health monitoring • IoT devices, applications and platforms • Online advertising • Web and cross-device tracking • Data aggregation / data aggregation platforms • Eye tracking • Data processing at the workplace • Data processing in the context of home and remote working • Processing location data of employees • Loyalty schemes • Tracing services (tele-matching, tele-appending) • Wealth profiling – identification of high net-worth individuals for the purposes of direct marketing
Targeting of children/other	The use of the personal data of children or other	• Connected toys • Social networks

Type of processing operation(s) requiring a DPIA	**Description**	**Non-exhaustive examples of existing areas of application**
vulnerable individuals for marketing, profiling for auto decision making or the offer of online services	vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.	
Risk of physical harm	Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.	• Whistleblowing/complaint procedures • Social care records

Appendix 1: Data Protection Impact Assessment (DPIA) – Screening Tool

Project/Process Title			
Directorate / Service Area			
Overview of Project/Process			
Screening Questions	**Yes**	**No**	**Justification for Answer**
Will your project/app/system involve processing of information about individuals which includes special category or criminal conviction data? **Please note this includes 'anonymous' data within these categories if unique identifiers such as initials or reference numbers are also processed.** *If you are processing any of the below types of personal data your answer should be YES:* • *Racial or ethnic origin* • *Political opinions* • *Religious or philosophical beliefs* • *Trade union membership* • *Genetic data* • *Biometric data* • *Data concerning health* • *Data concerning a person's sex life* • *Data concerning a person's sexual orientation* • *Criminal conviction data* *Please note this is not an exhaustive list*	□	□	

Will you be collecting new personal information about individuals, or information which, if breached could have a significant impact on an individual? *Examples where the answer would be YES:* - *This a new system/process processing personal data that has not been previously collected* - *This is an existing system/process processing personal data but additional data must be collected due to a change in scope of the system/process* - *Data which has routinely been collected is being collected in a new way, this data is very sensitive and would cause distress to the data subject if it was breached* *Please note this is not an exhaustive list*	☐	☐	
Will information about individuals be disclosed or shared with organisations or people who have not previously had routine access to the information? *Example of where the answer would be YES:* - *There is a requirement to share information with an external 3rd party who has not previously had access to the data.* - *This would also result in the need for a Data Sharing Agreement (DSA)* *Please note this is not an exhaustive list*	☐	☐	
Are you going to use information you already hold about individuals for a purpose it is not currently used for? *Example of where the answer would be YES:* - *Matching information from different systems/data sources, where purpose/lawful basis of original data collection may differ* - *Details of the Information Asset in question will be contained within NYCC's Information Asset Register (IAR) and the purpose for processing, along with the legal basis for processing will be recorded. The way information will be*	☐	☐	

used in this new system/process must match the existing purpose/legal basis, otherwise a DPIA is required • Does the project involve using technology which might be perceived as privacy intrusive or monitoring any publicly accessible areas? For example, CCTV, facial recognition, use of biometrics* such as thumb prints, • Vehicle number plate recognition or location tracking. *Please note this is not an exhaustive list*			
Does any phase of project/system/ app use automated decision making based on information provided by the individual or received from a 3rd party? *Automated individual decision-making is a decision made by automated means without any human involvement (e.g. online credit checks).* *Example of where the answer would be YES:* • *A new piece of software is being implemented which checks an applicant's geographical location, age and household income and automatically offers a free service to eligible applicants when certain conditions are met* *Please note this is not an exhaustive list*	☐	☐	
Will the project include marketing or contacting individuals which may be considered intrusive? *By phone, by email or by post, where they have not be informed/are not expecting that this contact will take place.* *Example of where the answer would be YES:* • *I have access to a list of email addresses which were collected for the purpose of setting people up as users of their local library. I'd like to send them a notice about a new transport services available that operate near the library.* *Please note this is not an exhaustive list*	☐	☐	

Will the project include data matching from different sources or profiling? *Combining, comparing or matching personal data obtained from multiple sources.* *Example of where the answer would be YES:* • *Matching data from two/three different children's systems to understand which children may be eligible to join a new learning programme* *Please note this is not an exhaustive list*	□	□	
Will you be conducting large scale processing, this includes numbers, duration and geographical spread? *Example of where the answer would be YES:* • *Processing data related to all/most children who reside in Bury* • *Tracking all/most individuals using public transport systems in Bury* *Please note this is not an exhaustive list*	□	□	

If you have answered YES to any of the questions above then a full DPIA must be carried out.

If you have answered NO to ALL of the above screening questions then a DPIA is not necessary. Please complete the declaration below and email a copy to the Policy and Compliance Team; IG@bury.gov.uk

Date of Assessment:	
Officer name:	
Signature	

Note:

If the scope of work changes, then the pre-assessment MUST be repeated.

If you have any doubts, please contact the Data Protection Officer; IG@bury.gov.uk, for advice

Appendix 2: Data Protection Impact Assessment

How to use this DPIA

Each section of the DPIA should be completed to provide a full overview of the proposal, the information being collected and/or processed and how the data protection principles have been considered and demonstrate that these can be upheld.

The supporting DPIA guidance document has been created to run alongside the DPIA and provide:

- Further guidance and clarification on the information that is required within the DPIA
- Additional information on what should be in place to meet the data protection principles

Title of project:	
Individual completing this form:	
Department:	
Service:	

Step 1: Identify the need for a DPIA
Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing
Describe the nature of the processing: • How will you collect, use, store and delete data? • What is the source of the data? • Will you be sharing data with anyone?

- You might find it useful to refer to a flow diagram or another way of describing data flows.
- What types of processing identified as likely high risk are involved?

Describe the scope of the processing:

- What is the nature of the data, and does it include special category or criminal offence data?
- How much data will you be collecting and using?
- How often?
- How long will you keep it?
- How many individuals are affected?
- What geographical area does it cover?

Describe the context of the processing:

- What is the nature of your relationship with the individuals?
- How much control will they have?
- Would they expect you to use their data in this way?
- Do they include children or other vulnerable groups?
- Are there prior concerns over this type of processing or security flaws?
- Is it novel in any way?
- What is the current state of technology in this area?
- Are there any current issues of public concern that you should factor in?
- Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing:

- What do you want to achieve?
- What is the intended effect on individuals?
- What are the benefits of the processing for you, and more broadly?

Step 3: Consultation Process

Consider how to consult with relevant stakeholders:

- Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.
- Who else do you need to involve within your organisation?
- Do you need to ask your processors to assist?
- Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

- What is your lawful basis for processing?
- Does the processing actually achieve your purpose? Is there another way to achieve the same outcome?
- How will you prevent function creep?
- How will you ensure data quality and data minimisation?
- What information will you give individuals?
- How will you help to support their rights?
- What measures do you take to ensure processors comply?
- How do you safeguard any international transfers?

Step 5: Identify and assess risks			
Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** (remote, possible or probable)	**Severity of harm** (minimal, significant or severe)	**Overall risk** (low, medium or high)

Step 6: Identify measures to reduce risk			
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5	**Effect on risk** (eliminated, reduced or accepted)	**Residual risk** (low, medium or high)	**Measure approved** (yes/no)

Step 7: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		
Residual risks approved by:		
DPO advice provided:		
Summary of DPO advice:		
DPO advice accepted or overrules by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals’ views, you must explain your reasons
Comments:		

This DPIA will be kept under review by:		The completed DPIA should be sent to the Policy and Compliance Team for filing