
What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (“DPIA”) is a process that assists organisations in identifying and minimising the privacy risks of new projects or policies.

Projects of all sizes could impact on personal data.

The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

Conducting a DPIA should benefit the Council by producing better policies and systems, and improving the relationship with individuals.

Why should I carry out a DPIA?

Carrying out an effective DPIA should benefit the people affected by a project and also the organisation carrying out the project.

Whilst not a legal requirement, it is often the most effective way to demonstrate to the Information Commissioner’s Officer how personal data processing complies with data protection legislation.

A project which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A DPIA should improve transparency and make it easier for individuals to understand how and why their information is being used.

When should I carry out a DPIA?

The core principles of DPIA can be applied to any project that involves the use of personal data, or to any other activity that could have an impact on the privacy of individuals.

Answering the screening questions in **Section 1** of this document should help you identify the need for a DPIA at an early stage of your project, which can then be built into your project management or other business process.

Who should carry out a DPIA?

Responsibility for conducting a DPIA should be placed at senior manager level. A DPIA has strategic significance and direct responsibility for the DPIA must, therefore, be assumed by a senior manager.

The senior manager should ensure effective management of the privacy impacts arising from the project, and avoid expensive re-work and retro-fitting of features by discovering issues early.

A senior manager can delegate responsibilities for conducting a DPIA to three alternatives:

- a) An appointment within the overall project team;
- b) Someone who is outside the project; or
- c) An external consultant.

Each of these alternatives has its own advantages and disadvantages, and careful consideration should be given on each project as to who would be best-placed for carrying out the DPIA.

How do I carry out a DPIA?

Working through each section of this document will guide you through the DPIA process.

The requirement for a DPIA will be identified by answering the questions in **Section 1**. If a requirement has been identified, you should complete all the remaining sections in order.

The Data Protection Impact Assessment Statement in **Section 7** should be completed in all cases, and a copy of this document should be sent to the Information Lawyer (Data Protection Officer) to record and review.

The Information Lawyer (Data Protection Officer) will review the DPIA within 14 days of receipt, and a draft DPIA report will be issued within 28 days. The report will confirm whether the proposed measures to address the privacy risks identified are adequate, and make recommendations for additional measures needed.

These measures will be reviewed once in place to ensure that they are effective.

Advice can be found at the beginning of each section, but if further information or assistance is required, please contact the Information Lawyer (Data Protection Officer) on 023 8083 2676 or at information@southampton.gov.uk.

Section 1 - Screening Statements

The following statements will help you decide whether a DPIA is necessary for your project.

Please tick all that apply.

The project will involve the collection of new information about individuals.

The project will compel individuals to provide information about themselves.

Information about individuals will be disclosed to organisations or people who have not previously had routine access to the information.

You are using information about individuals for a purpose it is not currently used for, or in a way it is not currently used.

The project involves you using new technology which might be perceived as being privacy intrusive. For example, the use of biometrics, facial recognition, or profiling.

The project will result in you making decisions or taking action against individuals in ways which can have a significant impact on them.

The information about individuals is of a kind particularly likely to raise privacy concerns or expectations. For example, health records, criminal records, or other information that people would consider to be particularly private.

The project will require you to contact individuals in ways which they may find intrusive.

The project involves making changes to the way personal information is obtained, recorded, transmitted, deleted, or held.

If any of these statements apply to your project, it is an indication that a DPIA would be a useful exercise, and you should complete the rest of the assessment, including the Data Protection Impact Assessment Statement in **Section 5**.

If none of these statements apply, it is not necessary to carry out a DPIA for your project, but you will still need to complete the Data Protection Impact Assessment Statement in **Section 5**.

Section 2 - Identifying the Need for a DPIA

Briefly explain what the project aims to achieve, what the benefits will be to the Council, to individuals, and to other parties.

Section 3 - Describe the Information Flows

The collection, use, sharing, and deletion of personal data should be described here.

Section 4 - Identifying the Privacy Risks

Answering the questions below will help identify the key privacy risks, and the associated compliance and corporate risks.

The questions cover the key data protection principles, and whilst all may not be relevant to your project, they may prompt you to consider areas of risk which aren't initially apparent.

Principle 1

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

What personal data will be collected and/or shared?

With whom will the personal data be shared?

How will individuals be told about the use of their personal data?

Conditions for processing

For all data (tick all that apply):

The data subject has given consent to the processing.

The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

The processing is necessary for compliance with a legal obligation to which the Council is subject.

The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council.

Does your project involves the processing of the following?

Tick all that apply:

data revealing racial or ethnic origin

political opinions

religious or philosophical beliefs

trade-union membership

genetic data or biometric data for the purpose of uniquely identifying a natural person

data concerning health

data concerning a natural person's sex life or sexual orientation

If so, which of the following apply?

The data subject has given explicit consent to the processing.

The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Council or of the data subject in the field of employment and social security and social protection law.

The processing is necessary for the establishment, exercise, or defence of legal claims, or whenever courts are acting in their judicial capacity.

The processing is necessary for reasons of substantial public interest.

The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

If you are relying on consent to process personal data, how will this be collected and recorded?

What will you do if consent is withheld or withdrawn? How will this be recorded?

Can an alternative condition for processing (see page 7) be used instead of consent? If yes, please provide details. See conditions on page 6 for options.

How will individuals be informed at the point of collection about how their personal data will be used?

Will any personal data be published on the Internet or in other media? If yes, please provide details.

Will a third party contractor be processing the personal data on our behalf, or involved at any stage in the data processing process?

Principle 2

Personal data shall be collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.

Do you envisage using the personal data for any other purpose in the future? If so, please provide details.

Principle 3

Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Are you satisfied that the personal data processed is of good enough quality for the purposes proposed? If not, why not?

Is there any personal data that you could not use, without compromising the needs of the project? If yes, please provide details.

How will you ensure that only personal data that is adequate, relevant, and not excessive in relation to the purpose for which it is processed?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

Are you able to update and amend personal data when necessary, after it has been collected and recorded? Please provide details.

How will you ensure that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

What retention periods are suitable for the personal data you will be processing?

How will you ensure the personal data is deleted in line with your retention periods?

What processes will be put in place for the destruction of the personal data?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

If an individual requested a copy of the personal data held about them, detail how this would be provided to them.

If the project involves marketing, have you got a procedure for individuals to opt out of their personal data being used for that purpose?

Principle 7

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Where, and in what format, will the personal data be kept?

Will an IT system or application be used to process the personal data? Please provide details.

How will this system provide protection against security risks to the personal data?

What training and instructions are necessary to ensure that staff know how to operate the system securely?

Will staff ever process the personal data away from the office (e.g. via paper files, on laptops, tablets, or smart phones)? If so, please provide details.

How will access to the personal data be controlled?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer personal data outside of the EEA? If yes, please provide details.

If you will be making transfers, how will you ensure that the personal data is adequately protected?

If a contractor is being used to process the personal data, where are they (and their data stores) based?

Section 5 - Data Protection Impact Assessment Statement

This statement must be completed for all projects, regardless of whether a DPIA was deemed to be necessary on completion of the screening questions in Section 1.

Name:

Position:

Project Summary:

Estimated date of project completion:

Please choose one of the following options:

None of the screening statements in Section 1 of this document apply to the above project, and I have determined that it is not necessary to conduct a Data Protection Impact Assessment.

Some of the screening statements in Section 1 of this document apply to the above project, and a need to carry out a Data Protection Impact Assessment was identified. The assessment has been carried out, and the outcomes will be integrated into the project plan to be developed and implemented.

Date:

Once completed, please send a copy of this document to Corporate Legal.

Email: information@southampton.gov.uk

Internal post: Corporate Legal, Civic Centre, Municipal, Ground Floor West

Document Information

Title: Data Protection Impact Assessment

Author: Chris Thornton, Senior Legal Assistant (Information)

Version: v2.7

Owner: Information Governance Board on behalf of the Council's Management Team

Agreed by: Information Governance Board on behalf of the Council's Management Team

Effective from: 31st January 2017

Review Date: 31st January 2018

Revision History:

06/12/13 - Version 1.0 - Reviser: Vikas Gupta - Document Created

10/03/15 - Version 2.0 - Reviser: Chris Thornton - Updated to PDF form format

17/07/15 - Version 2.1 - Reviser: Chris Thornton - Added information re report in introduction

14/01/16 - Version 2.2 - Reviser: Chris Thornton - Added screening question

27/01/16 - Version 2.3 - Reviser: Chris Thornton - Added project completion date to S7

24/01/16 - Version 2.4 - Reviser: Chris Thornton - Added service level for issuing reports

29/04/16 - Version 2.5 - Reviser: Chris Thornton - Removed sections 5 and 6, and revised questions

22/02/17 - Version 2.6 - Reviser: Chris Thornton - Changed wording to reflect GDPR

26/05/17 - Version 2.7 - Reviser: Chris Thornton - Changes made to consent to reflect GDPR