

Data Protection Impact Assessment

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.

Not only is it a legal requirement in some cases, 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 Step 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 Step 1. If a requirement has been identified, you should complete all the remaining sections in order.

After Step 5, the Information Lawyer (Data Protection Officer) will review the DPIA within 14 days of receipt, and complete the rest of the assessment within 28 days. The DPO will identify any privacy risks, and proposed measures to address them.

These measures must then be agreed by the project lead, Information Asset Owner or Administrator, and, in some cases, the Senior Information Risk Owner.

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.

Data Protection Impact Assessment Template			
Version	3.1	Approved by	Data Protection Officer
Date last amended	2 nd November 2018	Approval date	2 nd November 2018
Lead officer	Chris Thornton, Information Lawyer (Data Protection Officer)	Review date	2 nd November 2019
Contact	information@southampton.gov.uk	Effective date	2 nd November 2019

Project Details

Name of Project
HRA Capital Digital Improvements
Brief Summary of Project
This is the second phase of the Housing Service IT & Digital plan which is designed to support improvements for tenants, housing staff and the council. This investment is to support the rationalisation and subsequent development of IT systems and equipment within housing enabling streamlined and digital business processes. Improvements, efficiencies and consistent ways of working can then be designed and delivered. The plan includes migrating the existing 125 users from the old systems and equipment onto the new platform and ways of working while also extending this to include a further 125 users, resulting in one place for the co-ordination of all Housing Operations staff, a single modern system that is very nearly “always-on”. Alongside these improvements the new system will enable improved communications with tenants via text message and email.
Estimated Completion Date
December 2019
Name of Project Lead
Jonathan Higginbottom & Sharon Whitaker

Details of Person Conducting DPIA

Name
Deborah Smart
Position
Service Lead – Digital and Strategic IT
Contact Email Address
Deborah.smart@southampton.gov.uk

Step 1: Identify the need for a DPIA

Does your project involve... (tick all that apply)

- The collection of new information about individuals
- Compelling individuals to provide information about themselves
- The disclosure of information about individuals to organisations or people who have not previously had routine access to the information
- The use of existing information about individuals for a purpose it is not currently used for, or in a way it is not currently used
- Contacting individuals in ways which they may find intrusive
- Making changes to the way personal information is obtained, recorded, transmitted, deleted, or held
- The use of profiling, automated decision-making, or special category data¹ to make significant decisions about people (e.g. their access to a service, opportunity, or benefit).
- The processing of special category data¹ or criminal offence data on a large scale.
- Systematically monitoring a publicly accessible place on a large scale.
- The use of new technologies.
- Carrying out profiling on a large scale.
- Processing biometric or genetic data.
- Combining, comparing, or matching data from multiple sources.
- Processing personal data without providing a privacy notice directly to the individual.
- Processing personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Processing personal data which could result in a risk of physical harm in the event of a security breach.

¹ personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

If you answered “yes” to any of these, please proceed to Step 2.

If none of these apply, please tick the below box, and return the form to the Information Lawyer (Data Protection Officer) at information@southampton.gov.uk

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

Step 2: Describe the processing

The nature of the processing

How will you collect data?

Personal data is submitted by subjects when requesting council housing services. This includes online-forms, in person and telephone.

Personal data is submitted by Staff when requesting employment in housing services. This includes online-forms, in person and telephone.

How will you use the data?

The data is processed by the Housing Service to deliver council housing services.

The data is processed by front-line staff to complete specific transactions and is coordinated and scheduled by office staff.

The data is only shared with relevant third parties where necessary and is processed according to data sharing agreements enforced by contracts.

Staff data will be used to coordinate and schedule work and manage the performance of the housing service.

How will you store the data?

Data is processed using Council managed infrastructure and applications. This includes electronic storage of data in file systems including: application databases, communication systems and content management systems.

Currently data is also processed using paper file systems that are office based. The proposed change will provide the tools to reduce this and potentially remove the need for paper completely following further change.

Staff data will be processed in electronic file systems and specifically the corporate HR system including training and attendance data. Data about staff abilities and capabilities will be processed and stored in operational applications.

How will you delete the data?

Electronic file systems in scope of this change will have data classification and data retention policies applied to periodically delete subject data when it is no longer required.

Paper file systems in scope of this change will have data classification and data retention policies applied to periodically delete subject data when it is no longer required.

What is the source of the data?

The source of the data is the data subject.

Will you be sharing data with anyone?

INFO: If yes, please provide details

Describe the scope of the processing

What is the nature of the data?

INFO: Detail the type of personal data being processed. List any fields that will be processed (e.g. name, address, data of birth, NHS number, video images)

For both Tenant and Staff:

Personally Identifiable Data including:

- Name
- Address
- Date of Birth

Financial Data including:

- Payment Details
- Bank Account Details

For Tenant:

Sensitive Personal Data including:

- Children’s Data

Does it include special category or criminal offence data? Please provide details.

INFO: “Special category” data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

Yes.

Staff and Tenants:

Criminal Offence Data is assumed to be stored and processed to prevent fraud and protect staff.

How much data will you be collecting and using?

Approximately 100,000 subjects.

Data for 91,080 tenants(estimated) of 18,000(estimated) properties

Data for prospective 5,000(estimated) tenants applying for properties

Data for 250 staff employed by the Housing Service.

How often will the data be collected and used?

The data will be collected and used continually to deliver housing services

How long will you keep it?

According to the Council retention policy Financial Data will be held for up to 7 years and this will require sufficient personally identifiable data to be able link transactions to the financial data.

How many individuals are affected?

Potentially the whole 250,000 (estimated) population of Southampton may engage with Housing Services.

Typically across 18,000 properties the typical rate of tenancy change is 20% per year (3600 new tenants per year) which means that if data is held maximum of 7 years and in the worst case new tenants arrive and tenants do not move properties then 7 years will require 39,600 properties tenancy data. If the typical household composition is 2.3 people per property then this is worst case personal data for 91,080 current and historic tenant subjects.

It is assumed that people applying for properties who are not successful will not need to be kept.

What geographical area does it cover?

All data processing is within the European Economic Area (EEA) which is controlled by the EU GDPR law in UK the national law that implements EU GDPR is the Data Protection Act 2018.

Describe the context of the processing

What is the nature of your relationship with the individuals?

INFO: Detail who the data subjects will be (e.g. residents, carers, pupils, staff, professionals)

Applicants.

Tenants.

Tenants children.

Employees/Staff.

Third party contract staff.

How much control will they have over their data?
They will have the full rights of the DPA2018 to control the data processing of their data by the Council Housing Service.
Would they reasonably expect the Council to use their data in this way?
INFO: Please provide details to support your answer
Yes and the lawful purpose is to fulfil a contract which reasonably limits some of the rights to restrict processing that are essential to fulfil the contract and provide taxpayer value for money.
Do they include children or other vulnerable groups?
INFO: If yes, please provide details
Yes. Children, people with disabilities and vulnerable Adults are typical in the population and will be present in Council Housing services. This needs to be captured and processed to ensure that the required support is provided to prevent discrimination and to safeguard the subjects and protect staff.
Are you aware of any prior concerns over this type of processing or security flaws?
INFO: If yes, please provide details
There have been no notifiable data breaches in the Housing Service scope that the proposed changes to systems that would warrant extra organizational or technical controls.
Is the processing novel in any way?
INFO: If yes, please provide details
No.
What is the current state of technology in this area?
Mature.
Are there any current issues of public concern that should be considered?
INFO: If yes, please provide details
Public and Staff would have a concern over systemic monitoring. This is not the case with the proposed system changes. The proposed systems will track and trace business events to time and location and member of staff for performance management and service improvement reasons and to better inform tenants and customers of planned visits/appointments.

Describe the purposes of the processing

What do you want to achieve?

Providing contracted and universal Housing Services to prospective and current tenants.

What is the intended effect on individuals?

To provide decent homes for the population of Southampton.

What are the benefits of the processing – for the Council, and more broadly?

To provide the contracted and universal Housing Services to provide accommodation for the tenant and their families and for the Council to efficiently and effectively provide the service within the constraints of available funding and ensuring value for money.

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

The technical and business changes will engage with stakeholders including tenants as new "user journey" processes are designed to ensure that the new features and functions provided by the technical changes are exploited by business change.

Tenants, Staff, Managers, Unions and partner organisations will be consulted.

Who else do you need to involve, or have you already involved within the Council?

INFO: e.g. IT services, records management

This will involve all required functions including:

- Housing Services
- IT Services
- Cyber/Information Security
- Records Management
- Information Governance/Data Protection [DPO and IAOs/IAAs]

Do you need to ask your processors to assist?

INFO: Processors are third parties who will process the personal data on our behalf

All required third party data processors will be included.

Do you plan to consult information security experts, or any other experts?

INFO: Please provide details to support your answer

Yes currently assumed all internal to the Council.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures

What is your lawful basis for processing? Please choose one of the following...

INFO: There should generally only be one legal basis for processing.

- The data subject has given consent
- 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
- The processing is necessary for the purposes of the legitimate interests pursued by the Council or by a third party

Does the processing actually achieve your purpose?

INFO: Please provide details to support your answer

Yes

Is there another way to achieve the same outcome?

INFO: Please details to support your answer

No

How will you prevent function creep?

INFO: Function creep is where data collected for one purpose is used for another purpose over time.

Design of the new systems will establish the minimum viable data processing required to deliver the Housing Services and will provide data to enable further development and optimization. If this further development and service optimization requires a significant change to data processing that could be called “function creep” then a further DPIA would be completed. The delivery approach proposed is more agile and aligned with a continuous service improvement/technical development that may include refining the data processing.

How will you ensure data quality and data minimisation?
INFO: We should only use the minimum amount of personal data possible to achieve the purpose of the processing.
Data quality and minimization will be designed in at the analysis and redesign stage being mindful of the 6 principles of “data minimization” within GDPR/DPA that collectively provide one of the 8 principles of DPA “Data Quality”.
What information will you give individuals about the processing?
It will be made clear to subjects accessing Council Housing Services why the data is being processed and what choice they have about its processing (aware of the reduced ability for a subject to limit processing of a contracted service) and how an individual can comply to the Council or complain about the Council to the ICO.
How will you help to support their rights?
INFO: Data subject’s rights include the right to access, rectify, erase, port, and restrict their data.
The Council DPO and Data Protection Officers will ensure that all applicable rights are implemented. The Housing Service will work with IT service and vendors to ensure that these are enabled and implemented in the systems changes.
What measures do you take to ensure processors comply with the GDPR, and assist the Council in supporting individuals in exercising their rights?
INFO: E.g. will there be a contract in place with the processor that contains data protection obligations?
All data processors will have contracts and associated data processing agreements that are GDPR/DPA compliant. This will assumed to be the case and will be checked during the assessment and design phase of the proposed system changes.
How do you safeguard any international transfers of personal data?
INFO: If there are no international transfers involved, please state this
The Housing Service today does not include international transfers of data. If this was required it would require taking advice from DPO and specialists to understand what organizational and technical controls would be required and this would trigger the need for a DPIA.

Step 5: Send DPIA Form to the Data Protection Officer

After completing this part of the form, please send the document to the Information Lawyer (Data Protection Officer) at information@southampton.gov.uk

The DPO will review the information provided, and identify and assess the privacy risks.

Step 6: Identify and assess risks (DPO to complete)

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
1.	Remote Possible Probable	Minimal Significant Severe	Low Medium High
2.	Remote Possible Probable	Minimal Significant Severe	Low Medium High
3.	Remote Possible Probable	Minimal Significant Severe	Low Medium High
4.	Remote Possible Probable	Minimal Significant Severe	Low Medium High
5.	Remote Possible Probable	Minimal Significant Severe	Low Medium High
6.	Remote Possible Probable	Minimal Significant Severe	Low Medium High

Step 7: Identify measures to reduce risk (DPO to complete)

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk
1.		Eliminated Reduced Accepted	Low Medium High
2.		Eliminated Reduced Accepted	Low Medium High
3.		Eliminated Reduced Accepted	Low Medium High
4.		Eliminated Reduced Accepted	Low Medium High
5.		Eliminated Reduced Accepted	Low Medium High
6.		Eliminated Reduced Accepted	Low Medium High
Comments from the Data Protection Officer			
Comments from the Senior Records Officer			

Step 8: Sign off

Item	Date	Notes
DPO reviewed DPIA and provided advice on:		DPO should advise on compliance, step 7 measures and whether processing can proceed
Senior Records Officer reviewed DPIA on:		SRO should advise on records management matters
Measures approved by Project Manager on:		Integrate actions back into project plan, with date and responsibility for completion
Comments from Project Manager:		
Residual risks approved by Information Asset Owner / Administrator on:		
Comments from IAO / IAA:		
Residual high risks approved by the Senior Information Risk Owner on:		If accepting any residual high risk, consult the ICO before going ahead
Comments from SIRO:		