Information Security Document

Data Protection Impact Assessment Guidance

Version 6.0

Version	Date	Detail	Author
1.0	15/06/2017	First Draft for consideration by working group	Simon Hobbs
1.1	29/06/2017	Revised version for consideration by working group	Simon Hobbs
1.2	30/06/2017	Post working group version	Simon Hobbs
1.3	11/07/2017	Post IGG version	Simon Hobbs
1.4	26/11/2017	Post workshops and ICO Audit consultation version	Simon Hobbs
2.0	08/01/2018	Approved by Information Governance Group.	Simon Hobbs
3.0	07/02/2018	EDRM links added and Compliance Risk column deleted.	Simon Hobbs
4.0	25/03/2018	Amended to take account of GDPR requirements (ICO GDPR DPIA Guidance Consultation version 22nd March 2018) as well as further feedback from workshops	Simon Hobbs
5.0	14/05/2018	Minor amendments following workshops and GDPR changes.	Simon Hobbs
6.0	08/12/2020	Privacy Impact Assessment replaced by Data Protection Impact Assessment. Approved by IGG	Kathryn Baguley

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control	Description
A.18.1.1	Identification of applicable legislation and contractual requirements
A.18.1.3	Protection of records
A.18.1.4	Privacy and Protection of personally identifiable information

CONTENTS

1. Introduction

A Data Protection impact assessment (DPIA), previously called a Privacy Impact Assessment (PIA), is a tool which can help the Council identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective DPIA allows the Council to identify and fix problems at an early project stage, reducing the associated costs and damage to reputation which might otherwise occur; and in certain circumstances, a DPIA is mandatory.

This document is designed to guide you through the DPIA process to ensure that, where necessary, personal and special category data requirements are complied with, risks are identified and then either eliminated or mitigated. It is fully expected that the DPIA will change and evolve throughout the project/business change, and as such should be treated as a living document and updated throughout.

A DPIA should be carried out whenever there is a change that is likely to involve a new use or significantly change the way in which personal data is handled, for example a redesign of an existing process or service, or a new process or information asset is being introduced or when changes are being made to a data sharing agreement.

In the event of any doubt as to the implications of a project for the Council's compliance with data protection principles, then advice should be sought from Legal Services in the normal way. Advice may also be sought from the Council's Data Protection Officer (DPO).

2. What is a DPIA?

A DPIA is a process which helps an organisation to identify and eliminate/reduce the data protection risks.

The DPIA process is not new to the Council. Privacy implications are already considered as part of the project planning process. However, the aim of this procedure is to ensure that this is done on a systematic and consistent basis. The Council initially commenced formal PIAs in July 2017, and now the DPIAs are embedded into procurement processes and reviewed in line with the Council's processes.

To be effective, a DPIA should be used throughout the development and implementation of a project, using existing project management processes. The DPIA is a document which should be updated as the project/business change evolves.

A DPIA will enable the Council to systematically and thoroughly analyse the data protection risks a particular project or system may bring.

3. Who is responsible for conducting the DPIA?

Any department manager who is introducing a new or revised service or changes to a new system, process or information asset is responsible for ensuring the completion of a DPIA. If appointed, the Project Manager will assist the department with this process.

At the start of the design phase of any new service, process, purchase of, implementation of an information asset etc. consideration should be given to the need and procedures for completing the DPIA. The DPIA outcomes should be routinely reported back to the organisation and issues raised through the project/programme board and included in the Departmental Risk Register as appropriate. The department should ensure that the Information Governance Group (IGG) are provided with the DPIA and kept updated on progress.

Where significant risks are identified these should be aired, in the first instance, with the DPO who should discuss with the Caldicott Guardian (CG) and/or Senior Information Risk Owner (SIRO) as necessary.

4. Where will a DPIA be appropriate?

DPIAs will be applied to new projects and data sharing arrangements, because this allows greater scope for influencing how the project will be implemented.

A DPIA can also be useful when planning changes to an existing system.

A DPIA can also be used to review an existing system, but the organisation needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system. However, upon the introduction of GDPR the Council made a decision not to review existing systems, except unless required under GDPR.

Under GDPR is there a requirement to carry out a DPIA where there is a high risk to individuals The areas of high risk are discovered by the questions in Section 1 a, b and c (see DPIA template pages 3-6).

The main purpose of the DPIA is to ensure that data protection risks are minimised while allowing the aims of the project to be met.

Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice.

This analysis can be tested by consulting with people who will be working on, or affected by, the project including the project team itself. Exceptionally, where for example the data protection risks are considered to be high, consultation

with the wider public may be appropriate. In the case of new data sharing agreements consultation with the partners involved would be good practice.

Conducting a DPIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the data protection risks arising.

A DPIA should be completed **before** a project is undertaken.

5. The relevance of privacy to DPIAs

As mentioned above in the introduction, privacy was at the centre of the PIA, which is the predecessor to the DPIA. The relevance of considering the impact of privacy remains, but the DPIA broadens the scope of the assessment by looking at the wider impact of data protection risks.

So, privacy, in its broadest sense, is about the right of an individual to be left alone.

It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, body searches or other interference, acts of surveillance and the taking of biometric information.
- Informational privacy – the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

Some of the ways risks can arise to personal information are:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept for too long;
- Disclosed to someone where the person who it is about does not want them to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about; or
- Not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be

less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information.

Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a DPIA should be a minimisation of data protection risk.

6. The legal duty to carry out a DPIA and the benefits of a DPIA

The Information Commissioner (ICO) (for more information about the ICO please see page 14) promotes DPIAs as a tool which will help organisations to comply with their data protection obligations, as well as bringing further benefits.

Conducting a DPIA is a legal requirement of the GDPR and Data Protection Act 2018 in certain limited circumstances where there is a high risk to data protection, but carrying out an effective DPIA should also benefit the people affected by a project and also the organisation carrying out the project. Additionally it is a requirement of the Information Governance Toolkit Assessment to show that DPIAs are undertaken.

A DPIA will be legally required where the Council plans to;

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- Process special category data or criminal offence data on a large scale;
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies;
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- Carry out profiling on a large scale;
- Process biometric or genetic data;
- Combine, compare or match data from multiple sources;
- Process personal data without providing a privacy notice directly to the individual;
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour;
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them, and or

- Process personal data which could result in a risk of physical harm in the event of a security breach.

Conducting and publicising a DPIA will help the Council to build trust with the people using their services.

There can be financial benefits to conducting a DPIA. Identifying a problem early will generally require a simpler and less costly solution. A DPIA can also reduce the ongoing costs of a project by minimising the amount of information being collected or used where this is possible, and devising more straightforward processes for staff.

More generally, consistent use of DPIAs will increase the awareness of privacy and data protection issues within an organisation, and ensure that all relevant staff involved in designing projects think about data protection at its' earliest stages.

Examples of where a DPIA would be appropriate:

- A new IT system for storing and accessing personal data;
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data;
- A proposal to identify people in a particular group or demographic and initiate a course of action;
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of an organisation;
- Legislation, policy or strategies which will impact on data protection through the collection or use of information, or through surveillance or other monitoring;
- Cloud hosted applications, and/or
- The collection of new data on an existing system.

Some of the above refer to 'large scale' and while there is currently no definition in law some indications of things to consider are:

- the number of individuals concerned;
- the volume of data;
- the variety of data;
- the duration of the processing; and
- the geographical extent of the processing.

A DPIA should be used on specific projects and to be effective it should be applied at a time when it is possible to have an impact on the project. This means that DPIAs are more likely to be of use when applied to new projects or revisions of existing projects. Procurement practices and procedures are key to the success of this procedure and will be adapted accordingly.

The Council must identify the need for a DPIA at an early stage and build this into project management or other business processes.

The Department Manager commissioning the new process/system will be responsible for carrying out the DPIA and for completing the necessary templates.

Monitoring

The screening questionnaire responses (Section 1 a, b and c) and/or completed DPIA should be saved to EDRM and submitted to IGG for monitoring purposes by emailing a link to the Information Security Manager.

The presumption is that completed DPIAs will be published via the Council's website unless there are issues e.g. commercial confidentially that make this inappropriate.

The IGG will also monitor implementation of actions identified in DPIAs and scrutinise implementation of DPIA mitigation on a twelve monthly basis by receiving exception reports.

7. ICO role

The ICO is the UK regulator and independent body set up to uphold information rights. For more information please see https://ico.org.uk.

As indicated above, if the assessment process suggests that the risk to data protection is very high after any mitigation is applied (because there is no mitigation available or there is a reason the Council does not wish to pursue the mitigation) then it may be necessary to refer the completed DPIA to the ICO and consult with them. The ICO have indicated it will take between 8 and 14 weeks for a written response.

The DPO should be consulted **before** any DPIA is referred to the ICO under this provision.