Information Security Document

Data Protection Impact Assessment Procedure

Version 6.0

Version History

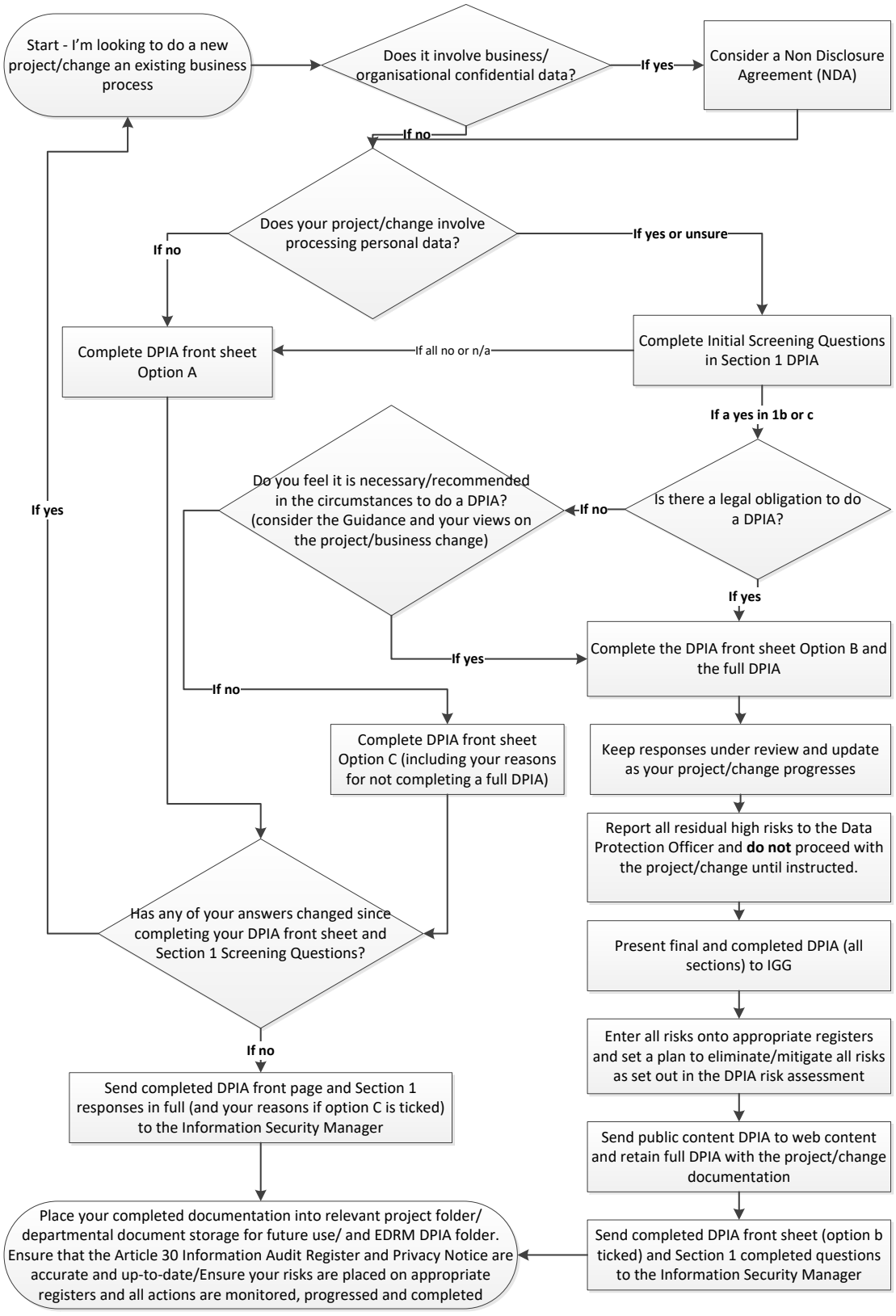
Version	Date	Detail	Author
1.0	15/06/2017	First Draft for consideration by working group	Simon Hobbs
1.1	29/06/2017	Revised version for consideration by working group	Simon Hobbs
1.2	30/06/2017	Post working group version	Simon Hobbs
1.3	11/07/2017	Post IGG version	Simon Hobbs
1.4	26/11/2017	Post workshops 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

DPIA flowchart



DPIA Procedure step by step

Section 1 a – (DPIA template page 3) - This is for you to record the data types you are going to use. You will see that the table uses the traffic light colouring system, so you can see personal data in green, data which people feel as more sensitive in amber and special category data in red. This exercise helps you to see how many data types you are collecting and an initial steer on the sensitivity of the data.

Section 1 b and c – (DPIA template pages 4, 5 and 6) - These are a list of questions which will give you an initial view on the project/business changes level of data protection impact. If a response to any of the questions is "yes" then a DPIA must be carried out if it is a legal requirement (see above list) or should be considered (see above list of recommended circumstances). The responses to Section 1 must be kept up-to-date throughout your project/business change. Your completed responses to Section 1 **must be** sent to the Information Security Manager.

In the event that a full DPIA is deemed appropriate/necessary, you must complete **Section 2 onwards.**

Sections 2 and 3 – (DPIA template pages 7 and 8) – These ask for more details about your project/business change. This information is likely to be contained within your project documentation, Project Initiation Document (PID) or Business Case.

Section 4 – (DPIA template page 9) – This asks you to record any consultations. It is important, especially in larger projects, to consult with external stakeholders (including where appropriate reviewing data sharing agreements) so that affected parties are involved in the process; which could include the general public or trade unions.

Section 5 - (DPIA template page 9) – This looks at certifications and assurance, and these are important in the understanding of the credentials of a third party and assist in analysing the data protection risk.

Section 6 – (DPIA template pages 10 and 11) - This records the contractual controls. The questions raised within this section should be considered at the outset of your project/business change and completed when you have more understanding of the agreement between the Council and third party. You may also find that this area changes as your negotiations progress, so it is important that this remains accurate.

Section 7 – (DPIA template page 11) - This looks at the rights and freedom of individuals. To read more about individual rights, please consult the Individual Rights Identification Guidance.

Section 8 – DPIA template pages 12, 13 and 14) - These link the project/business change with the data protection principles.

Principle 1 assistance - determining the lawful basis
Initial points to note:

- You **must** have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing (shown below). No single basis is '*better*' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it in the DPIA and your departments Article 30 Information Audit register. (For more information on the Article 30 Information Audit Register, please speak with your Department Liaison Officer or the Access to Information Solicitor).
- It is **really** important that it is right first time - you should not swap to a different lawful basis at a later date without good reason.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If you are processing special category data you must have a further condition for processing.

- There are 10 conditions for processing special category data in Article 9 of the GDPR, which are:

  (a) Explicit consent
  (b) Employment, social security and social protection (if authorised by law)*
  (c) Vital interests
  (d) Not-for-profit bodies
  (e) Made public by the data subject
  (f) Legal claims or judicial acts
  (g) Reasons of substantial public interest (with a basis in law)**
  (h) Health or social care (with a basis in law)*
  (i) Public health (with a basis in law)*
  (j) Archiving, research and statistics (with a basis in law)*

*Please note: If you are relying on conditions (b), (h), (i) or (j), you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the Data Protection Act 2018. Please speak with Legal Services for assistance if needed.

**Please note: If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the Data Protection Act 2018. Please speak with Legal Services for assistance if needed.

- You **must** determine your condition for processing special category data **before** you begin this processing under the GDPR, and you should document it.

If you are looking to process criminal convictions or offence data, you need the following:

•A lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.
•The Data Protection Act 2018 deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it. Please speak with Legal Services for assistance if you feel this applies.
•You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

DPIAs and risk assessment scoring

Remember: each and every part of the DPIA is designed to help you understand you project and help you to consider where your data protection risks may lie.

To identify the information risks and describe the mitigation that will need to be put in place to minimise the risk and impact on the Council.

Initial Score: Calculate the total score of the risk without any action plans to reduce the level of risk by multiplying the level of score from the Impact Assessment Criteria table with the score from the Likelihood Assessment Criteria table. This is to provide an indication of the worst case scenario.

Likelihood Assessment Criteria

Level	Description
5	Expected (monthly)
4	Likely (annually)
3	Possible (1 incident in 2 years)
2	Unlikely (1 incident in 5 years)
1	Rare (1 Incident in 10 years or above)

Impact Assessment Criteria

Level	Description
5	Catastrophic
4	Major
3	Moderate
2	Minor
1	Insignificant

IE if the impact is at level 5 and the likelihood is level 3: the score would be 5x3=15

Action Plan:
Detail the plans to reduce the risk or what controls are to be put in place.

Target Score
Using the scoring formula in the tables above, calculate the score once controls are in place.

Risk Control Plan: insert risk control definition as appropriate

Risk Control Definitions

Take the Opportunity	Accept the risk and turn it into a positive opportunity or benefit
Treat/Control	Actions required to mitigate the likelihood and/or impact
Tolerate/Accept	No action - risk within tolerance or accept - Understand and live with the risk.
Terminate	Cease or avoid the risk

Transfer	Transfer to potential third party via contract or bond or insurance etc

Evaluation:
Is the final impact on individuals justified, compliant and proportionate to the aims of the project?

Approved By:
If the Target score (i.e. after mitigation is applied) is over 16, this must be signed off by a Senior Manager at Service Director level or equivalent.

In certain circumstances (where there is a very high unmitigated risk) it may be necessary to consult with the ICO itself. Please take advice from the Council DPO if you think this may apply to your project. See below heading on 'Residual High Risk scoring DPIAs for more information.

Ensure that you integrate the DPIA outcomes back in to the Project Plan. You must be able to answer the following:

- Who is responsible for integrating the DPIA outcomes back in to the project plan and updating any project management paperwork?
- Who is responsible for implementing the solutions that have been approved?
- Who is the contact for any data protection concerns that may arise in the future?

Once the DPIA process has been completed consideration should be given as to how the mitigation of risks identified should be incorporated into any Project Plan and also as to whether risks should be included in Departmental Risk Registers.

The completed DPIA should be signed off by the senior responsible officer for the project or process in the relevant Department. It should also be logged in the relevant folder in EDRM. DPIAs. The completed DPIA **must** be sent for consideration to IGG **prior to** any implementation.

Residual high risk scoring DPIAs

If any risk is found to be high (16 or over) then this must be signed off by a Service director or equivalent.

In cases where high residual risk remains then this **must** be referred to the DPO. High residual risk means:

a. The risk mitigation has been carried out in full and the risk remains high,
b. risk mitigation is not available, so the risk remains high
c. There are reasons why mitigation is not considered appropriate, so the risk remains high,
d. and for our scoring purposes, is 20 or over

It is important all high residual risk assessments are considered by the DPO, as this may require a referral to the ICO before proceeding any further with the project or business change.

In cases of very high risk it may be necessary to consider referral to the ICO. The DPO **must** be consulted in relation to any proposed reference to the ICO.