DATA PROTECTION IMPACT ASSESSMENT POLICY

Amendment history
This policy will be reviewed every two years.

Date	Version	Author/Contributor	Amendment details
22/03/2019	02	Medicus Health Partners – all sites	
14/07/2022	03	Afinity DPO	All sites

DATA PROTECTION IMPACT ASSESSMENT POLICY

This policy will be used by Medicus Health Partners whenever any new project is undertaken whether in relation to IT and Communications, Infrastructure, Human Resources or Marketing, or any other activity which might have an effect on the processing of personal data.

We will also consider our Data Protection and Design by Default Policy to ensure we implement appropriate technical and organisational measures to ensure data protection and safeguard an individual's rights.

The aim is to ensure that we review carefully the effect of any project on the privacy of individuals and limit the personal data we collect to only that which is necessary and consider how we use this personal information.

1. WHAT IS A DPIA?

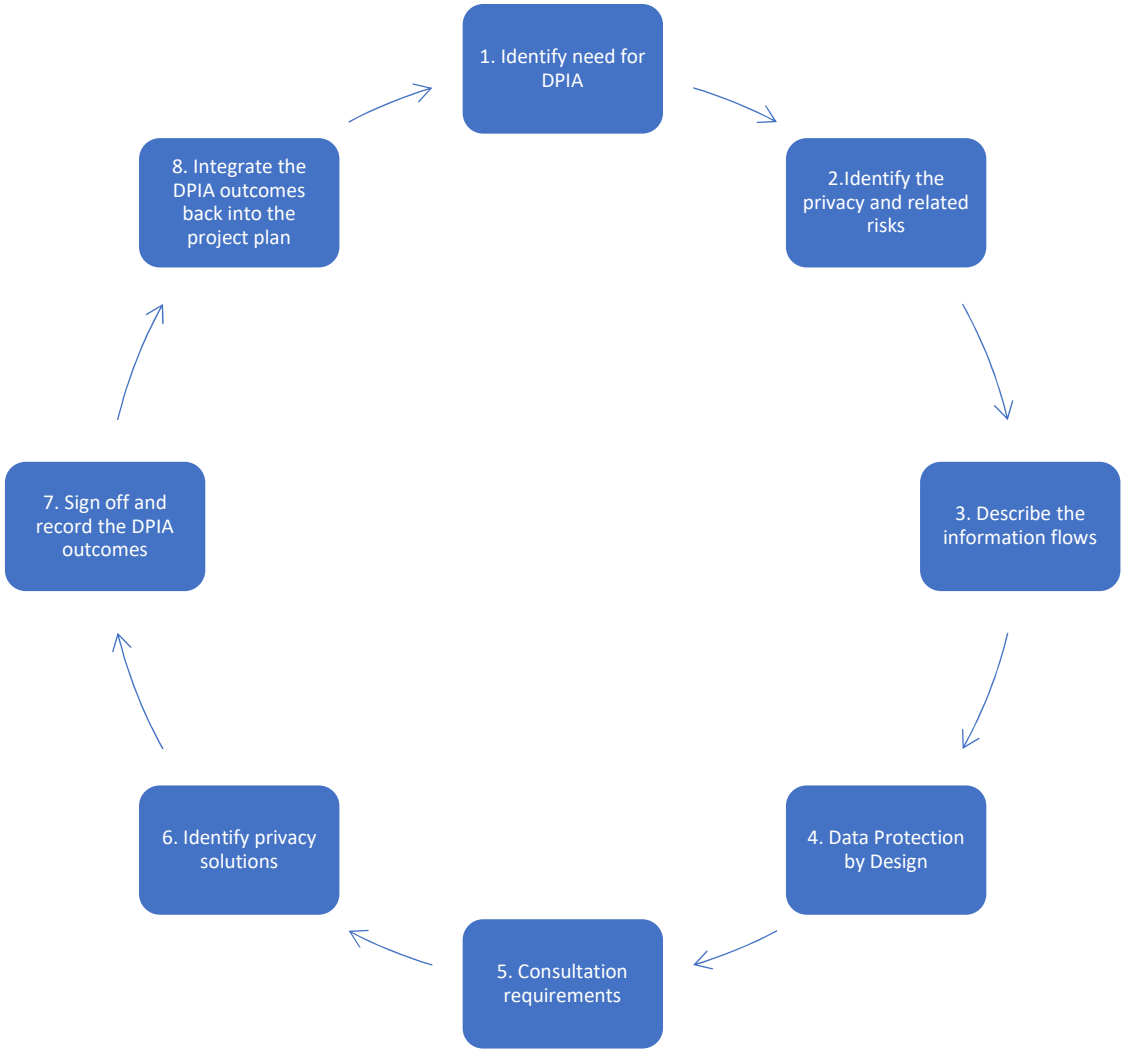
A DPIA is a procedure designed to describe the processing of information, assess its necessity and proportionality and help manage the risks to the rights and freedoms of individuals. This is done by assessing highlighted risks and determining measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of UK GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with Regulations. In other words, a DPIA is a process for building and demonstrating compliance.

2. IS A DPIA MANDATORY?

In line with the risk-based approach embodied by UK GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*". When a DPIA is deemed not necessary, the reasoning as to why must still be documented under the accountability principle.

3. HOW DO WE CARRY OUT A DPIA?

A DPIA should begin early in the life of a project, before we start our processing, and run alongside the planning and development process. We will use a template approach. It should include these steps:



Our DPIA must:

a) Describe the nature, scope, context and purposes of the processing;
b) Assess necessity, proportionality and compliance measures;
c) Identify and assess risks to individuals;
d) Identify any additional measures to mitigate those risks.
e) Include measures to ensure data protection by design and default.
f) Decide whether consultation is required
g) Determine the necessary training

The aim is to ensure that we review carefully the effect of any project on the privacy of individuals and limit the personal data we collect to only that which is necessary and consider how we use this personal information.

We must seek the advice of our data protection officer (if we have one). We should also consult with individuals and other stakeholders throughout this process.

We should start to fill out the template at the start of any major project involving the use of personal data, or if we are making a significant change to an existing process. The final outcomes should be integrated back into our project plan.

We will on every occasion ask ourselves screening questions to include the following:

1. Will the project involve the collection of new information about individuals?
2. Is the information necessary?
3. Will the project compel individuals to provide information about themselves?
4. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
5. Are we using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
6. Does the project involve us using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
7. Will the project result in us making decisions or taking action against individuals in ways that can have a significant impact on them?
8. Is the information about individuals 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.
9. Will the project require us to contact individuals in ways which they may find intrusive?
10. Are we able to limit the information (data) we request?
11. Are we able to limit who in our organisation has access to the information (data)?

These questions and the answers to them will assist us to decide whether a Privacy Data Impact Assessment (DPIA) is required.

4. PROCEDURE TO BE FOLLOWED

We will adopt a template approach to determine whether a DPIA is required and to organise the DPIA. This shall be as follows:

Step one: Identify the need for a DPIA

a) Consider what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

b) If helpful to link to other relevant documents related to the project, for example a project proposal.
c) Also consider why the need for a DPIA was identified.
d) Who will be responsible for the DPIA?

Step two: identify the privacy and related risks

a) Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.
b) Privacy issues.
c) Risk to individuals.
d) Compliance risk.
e) Associated organisation / corporate risk.
f) Identify the legal basis for processing.
g) The template will assist with this

Step three: Describe the information flows

a) The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. We will also say how many individuals are likely to be affected by the project.

Step four: Data protection by design

a) What organisational and technical measures can we use to improve data protection?
b) Do we need all the personal information or do we need the project at all or can it be in a different form?
c) Can we use pseudonymisation?
d) Can we limit the recipients?

Step five: Consultation requirements

a) Explain what practical steps we will take to ensure that we identify and address privacy risks. Who should be consulted, internally and externally? How will we carry out the consultation? We will link this to the relevant stages of our project management process.
b) Consultation can be used at any stage of the DPIA process.

Step six: Identify privacy solutions

a) Consider the actions we could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).
b) Consider Risk.

c) Consider Solution(s) and mitigation of risk.
d) Result: is the risk eliminated, reduced, or accepted?
e) Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step seven: Sign off and record the DPIA outcomes

a) Who has approved the privacy risks involved in the project? What solutions need to be implemented?
b) Risk
c) Approved solution
d) Approved by

Step eight: Integrate the DPIA outcomes back into the project plan

a) Who is responsible for integrating the DPIA outcomes back into 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 privacy concerns which may arise in the future?
b) Action to be taken
c) Date for completion of actions
d) Determine training required
e) Responsibility for action
f) Contact point for future privacy concerns

RISK ASSESSMENT – SCORING TABLES

Likelihood Score

Likelihood score	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Frequency How often might a breach occur	This will probably never happen	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it may not be a persisting issue	Will undoubtably happen/recur possibly frequently

Impact Scoring

Impact score (severity levels) and examples of descriptors	1	2	3	4	5
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on an individual's privacy and confidentiality	Minimal privacy impact requiring no/minimal intervention Other manual or electronic process in place to mitigate the risk	Minor impact on an individual's privacy Other manual or electronic process in place to mitigate the risk	Moderate privacy impact requiring professional intervention Aspects of reputational damage for the organisation if DPIA requirement not adopted Could result in an event	Major breach leading to possible larger scale privacy breaches Possible ICO reportable breach if data protection standard not adhered to Mismanagement of individual's privacy with long-term reputational issues	Serious breach and non-compliance with the law if requirement not adhered to Definite ICO report required if breach occurs An event which impacts on a large number

			which impacts on a moderate (less than 100) number of indivduals	Would impact on over 100 individuals - part system failure	of individuals – full system breach because of no adherence to standards. Is likely to be 1000 of individuals

Risk Type Scoring

	Likelihood				
	1	**2**	**3**	**4**	**5**
	Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
5. Catastrophic	5	10	15	20	25
4. Major	4	8	12	16	20
3. Moderate	3	6	9	12	15
2. Minor	2	4	6	8	10
1.Negligible	1	2	3	4	5

Status

1 - 3 Low risk 4 – 6 Moderate risk 8 – 12 High risk 15 – 25 Extreme risk