



Data Protection Impact Assessments

The DPIA Template should be completed in accordance with the Data Protection and Confidentiality Policy. The Information Governance and Data Protection Officer should be consulted when completing a Data Protection Impact Assessment.

Data Protection by design and by default

Article 25(1) GDPR 2016: Taking into account the state of the art, the cost of implementation and the nature, scope, context and purpose of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

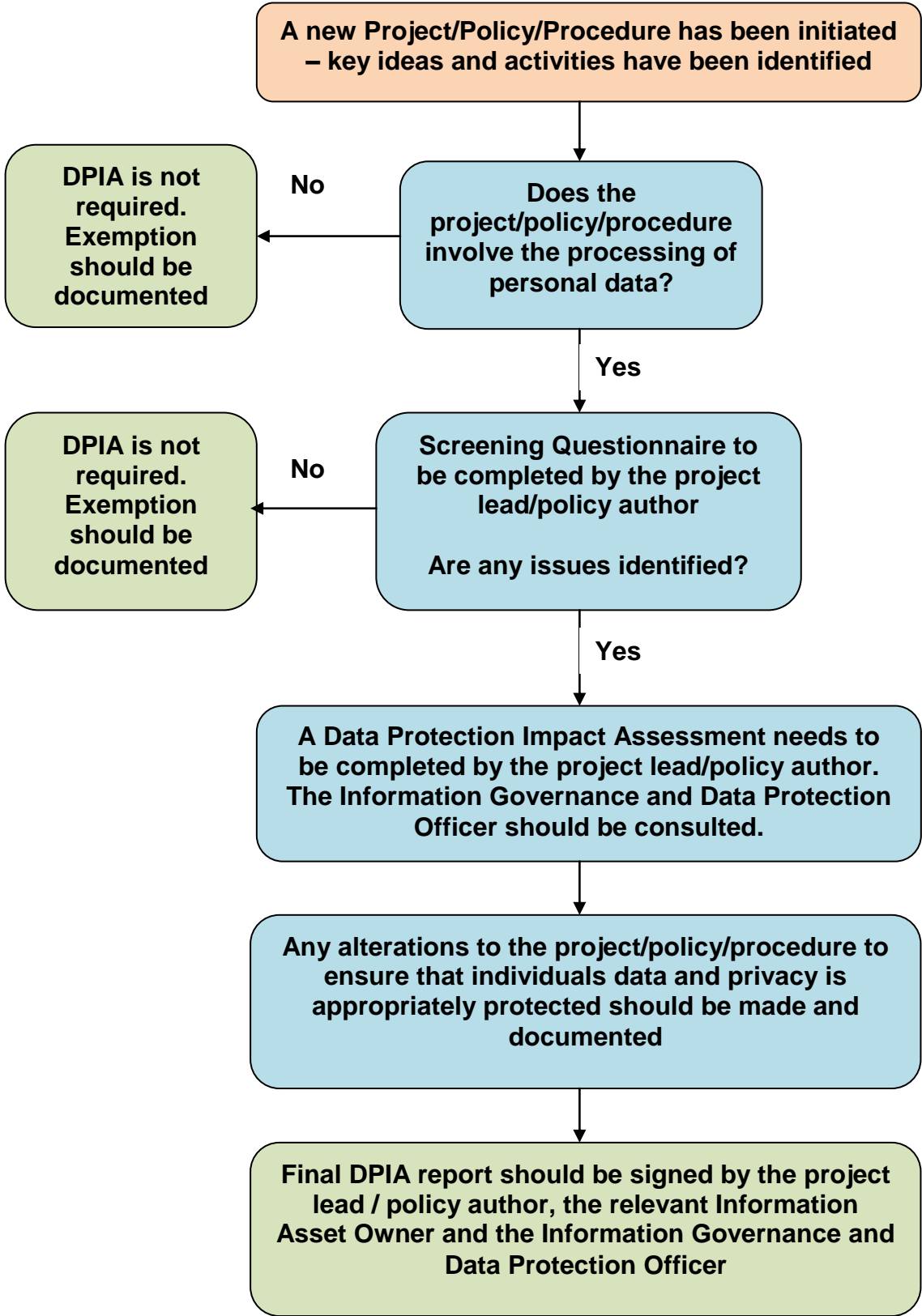
Article 25(2) GDPR 2016: The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Article 35(1) GDPR 2016: Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purpose of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to processing carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Article 35(3) GDPR 2016: A data protection impact assessment referred to in Article 35(1) shall in particular be required in the case of:

- (a) A systematic and extensive evaluation of personal aspects relating to living persons which is based on automated processing, including profiling, and on which decisions are based that significantly affect the person
- (b) Processing on a large scale of special categories (sensitive) data or personal data relating to criminal convictions and offences listed in Article 10
- (c) A systematic monitoring of a publicly accessible area on a large scale

Flowchart for the use of Data Protection Impact Assessments





Data Protection Impact Assessment (DPIA) Screening Questionnaire

Project/Policy/Procedure Title:

Project Lead:

Date:

| Question | Yes | No | Unsure | Comments |
|---|-----|----|--------|----------|
| 1 Are privacy-intrusive ¹ technologies being used? | | | | |
| 2 Are new and untested technologies being used? | | | | |
| 3 Are the purposes of data processing unclear? | | | | |
| 4 What is the lawful basis for processing data? | | | | |
| 5 Are new or substantially different identification authentication requirements needed? | | | | |
| 6 Will there be a significant amount of new data about each person, or a significant change in the current data-holdings? | | | | |
| 7 Will there be new data about a significant number of people? | | | | |
| 8 Will there be a new link of personal data with another data-holding? | | | | |
| 9 Are the data collection procedures new, changed, unclear or intrusive? | | | | |
| 10 Will there be a new or changed data quality process? | | | | |
| 11 Will there be new or changed data security arrangements? | | | | |
| 12 Are there new or changed data access or disclosure arrangements? | | | | |
| 13 Are there new or changed data retention arrangements? | | | | |
| 14 Has any external data sharing been identified on | | | | |

¹ 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 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.

| | | | | | |
|----|--|--|--|--|--|
| | the departments data flow map? | | | | |
| 15 | Is the personal data likely to raise privacy concerns with the individuals? e.g. health records, criminal records | | | | |
| 16 | Is there any use of highly sensitive or biometric data? e.g. protected characteristics or finger print recognition | | | | |
| 17 | Will personal data be disclosed to organisations or people who have not previously had access to the data? | | | | |
| 18 | Will data collection and processing result in automated decision making which will have a significant impact on the individuals concerned? | | | | |
| 19 | Will individuals be compelled to provide information about themselves? | | | | |
| 20 | Is there a contract or data sharing agreement in place with all third parties? | | | | |

If you have answered 'Yes' or 'Unsure' to any of the above, please consult with the Information Governance and Data Protection Officer. You may need to complete the full DPIA.

If all answers are 'No' or the Information Governance and Data Protection Officer has been consulted and approves, this Screening Questionnaire can be signed off by the Project Lead and responsible Information Asset Owner.

| Name | Job Title | Date |
|------|-----------|------|
| | | |
| | | |



Data Protection Impact Assessment Template

Project Lead/Policy Author:

Project Outline:

Set out a short summary of the intended project, policy or procedure.

What information is already available?

Are there any prior PIAs in this area? Are there any fact sheets, white papers, research or reports available? Have there been any consultations with professional associations? Have there been any consultations with regulators? Are there any other published views available?

Stakeholder Analysis – Who might be affected?

For example; patients, staff, trade unions, visitors

Name of Project/Policy:

Date:

| PRIVACY ISSUES | | | | | | |
|--|---------------------------------|---------------------------------|--|--|--|---|
| Questions | Answers: YES/NO/ COMMENTS | What are the privacy issues? | Has the project team discussed & identified other ways of dealing with these if they are impacting on privacy? If so, what? | Are there any privacy risks associated with the option chosen and what are they? | Has the SIRO been informed and has the risk been logged? Who is responsible for the risk and have they been consulted? What was the outcome? | Note how the project has been amended as a result of the privacy impact assessment |
| Technology | | | | | | |
| Does the project /policy use or suggest new or extra technologies that will have greater impact on privacy? Does the project/policy involve new or inherently privacy invasive technologies? Have you got established guidelines already? | | | | | | |
| Identity | | | | | | |
| Does the project/policy set up a new way to identify someone or reusing an existing way? Is it intrusive? Is it including a way to authenticate someone's identity or introducing an identity management process? | | | | | | |

| | | | | | | |
|--|--|--|--|--|--|--|
| Can someone's activities and actions now be identified as theirs, where as prior to the project/policy they would have been anonymous? | | | | | | |
| Multiple Organisations | | | | | | |
| Does the project/policy involve more than one organisation (including contractors)? | | | | | | |
| Data | | | | | | |
| Does the project/policy suggest using personal data in a new or significantly changed way? Is this the sort of data individuals would have concerns about? | | | | | | |
| Does the project/policy suggest using a lot of information about each person in a new or different way? | | | | | | |
| Does it involve using information about many people in a new or different way? | | | | | | |
| Does the project/policy involve pulling together information about individuals from different places, linking it or cross referencing? | | | | | | |

| | | | | | | |
|--|--|--|--|--|--|--|
| <p>Is the data handling new or introducing changes in relation to:</p> <ul style="list-style-type: none"> - Data Collection - Data Quality Assurance & Standards - Data Security Arrangements - Data Access/Disclosure Arrangements - Data Retention Arrangements <p>Does it make the data more readily accessible?</p> | | | | | | |
| Exemptions and Exceptions | | | | | | |
| <p>Could the project/policy be exempt from needing to consider privacy?</p> | | | | | | |
| <p>Is the key reason for the project/policy a major contribution to public security?</p> | | | | | | |
| <p>Does the project/policy mean that personal information will be seen or shared by other people, organisations or other countries that do not have the same legal needs to consider privacy?</p> | | | | | | |

Data Protection Impact Assessment Consultation Plan

Project/Policy/Procedure Name:

Date:

| | Guidance | Project Team Comments |
|---|---|------------------------------|
| Project/Policy/Procedure Summary | <i>Include brief outline of the project/policy/procedure and who will be affected by it (including numbers of people and whereabouts in the organisation}</i> | |
| Who will be consulted on the privacy issues? | <i>List all stakeholders/those who will be affected and why they have been chosen</i> | |
| What are you going to consult on? | <i>List the relevant issues which have been highlighted</i> | |
| Set out the groups/individuals and the dates that they are to be consulted on. Also means by which you are going to consult (letter/email/meeting) | <i>Set out a timetable</i> | |
| Is the SIRO or relevant IAO aware of any issues? | <i>What information risks have been identified?</i> | |

Data Protection Impact Assessment Consultation Outcome Record

One record should be completed for each stakeholder group/individual who is consulted

| | |
|---|---|
| Date of Consultation | |
| Who was consulted | <i>Name of Group or Individual</i> |
| List questions and concerns raised with the group or individual: | <i>Note responses to questions asked/any other comments or if any additional questions raised</i> |

Data Protection Impact Assessment Action Plan

| Action | Timescale | Responsible individual | Date Completed | Outcome/Comments |
|--------|-----------|------------------------|----------------|------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Summary of outcomes and changes made to process/project/policy to protect privacy

Once your DPIA is complete ensure that the Information Governance and Data Protection Officer have a copy of your Assessment to be reviewed by the Information Governance Group.