DATA PROTECTION IMPACT ASSESSMENT (DPIA) FRAMEWORK

GUIDANCE FOR THE COMPLETION OF A DATA PROTECTION IMPACT ASSESSMENT

Approved by the:
Information Governance Steering Group
22.2.21

DATA PROTECTION IMPACT ASSESSMENT FRAMEWORK: GUIDANCE FOR THE COMPLETION OF A DATA PROTECTION IMPACT ASSESSMENT

Summary of Key Points to Note

The General Data Protection Regulation (GDPR) introduced a new obligation to complete a Data Protection Impact Assessment (DPIA) before carrying out types of processing likely to result in high risk to individuals' interests. This is a key element of the new focus on accountability and data protection by design. DPIAs are now mandatory in some cases, and there are specific legal requirements for content and process. Key to note:

- DPIAs should be completed by key project personnel - this could be the project lead, manager, or any other key project team member. It is likely that multiple staff from the project will need to be involved with carrying out the DPIA.
- It is essential that the person(s) undertaking the DPIA has clear knowledge of the project, the systems involved and the level of information required, therefore this document is for use by anyone who proposes or develops new systems/upgrades existing systems within the organisation.
- A DPIA should be done before any type of processing which is "likely to result in a high risk". This means that although the actual level of risk has not been assessed, a DPIA screens for factors that point to the potential for a widespread or serious impact on individuals.
- We should aim to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent where feasible allowing individuals to monitor what is being done with their data and restricting settings to ensure systems aren't accessible by default to an indefinite number of persons.
- The Information Governance (IG) Team can provide advice and guidance throughout the design phase of any new service, process or information asset.
- DPIAs should be approved by the Trust's Data Protection Officer prior to submission to the Information Governance Team.
- The IG Team will review and forward any DPIA's to the IG Steering Group which is chaired by a senior member of the IG Team, which will provide feedback and recommendations.
- A DPIA template is provided at Appendix 2.

DATA PROTECTION IMPACT ASSESSMENT FRAMEWORK: GUIDANCE FOR THE COMPLETION OF A DATA PROTECTION IMPACT ASSESSMENT

CONTENTS

DATA PROTECTION IMPACT ASSESSMENT FRAMEWORK: GUIDANCE FOR THE COMPLETION OF A DATA PROTECTION IMPACT ASSESSMENT

1. INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) introduced a new obligation to complete a DPIA before carrying out types of processing likely to result in high risk to individuals' interests. This is a key element of the focus on accountability and data protection by design. DPIAs are now mandatory in some cases, and there are specific legal requirements for content and process.

2. SCOPE

2.1 All key project personnel involved in the introduction of new processes or proposed changes to processes e.g. project lead, manager or any other key project team members should be aware of this guidance and associated templates.

3. ROLES AND RESPONSIBILITIES

3.1 Senior Information Risk Owner (SIRO)

The SIRO has ownership of the organisation's information risks and provides assurances to the Trust Board. They are responsible for assessing the risks associated with changes to existing systems or the development of new information systems and for providing a final approval to such activities.

3.2 Caldicott Guardian

The Caldicott Guardian can provide advice and guidance where the proposed activity involves the collecting, processing, storage and sharing of patient or other personal confidential data. They should be consulted as part of the DPIA process where necessary and can also provide final approval to proposed activities.

3.3 Data Protection Officer

The Data Protection Officer should be consulted as part of the DPIA process in order to provide specialist advice and guidance relating to the activity and the organisational objectives of its progress. They should also be consulted should any review of a completed DPIA indicate outstanding or unmitigated risks or recommendations that require consideration prior to their acceptance or rejection.

3.4 Information Governance Team

The IG team will forward any DPIA's to the IG Steering Group which is chaired by a senior member of the IG team. Feedback and recommendations will be provided to you.

3.5 Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are accountable for the information systems under their control and are responsible for managing any risks associated with data flows into and out of those systems and for the quality, security and confidentiality of any data held in them.

3.6 **Information Asset Administrators**

Information Asset Administrators will:

- ensure that guidance in this document is followed,
- recognise actual or potential risks when new processes are being introduced in their directorate/department,
- consult with their IAOs and where necessary the DPO to take steps to understand how to mitigate risks,
- encourage project/programme leads to complete the DPIA at the initial stage of a project/process

3.7 Managing information risk effectively requires a structured approach involving work areas where accountability sits with senior managers, rather than specialist staff. All staff need to work together to help identify and mitigate information risk.

4. KEY PRINCIPLES

4.1 What is a DPIA

4.1.1 A DPIA is a way to systematically and comprehensively analyse processing activities and help identify and minimise data protection risks. DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

4.1.2 To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

4.1.3 DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping demonstrate accountability and building trust and engagement with individuals.

4.1.4 A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

4.1.5 It's important to embed DPIAs into organisational processes and ensure the outcome can influence plans. A DPIA is not a one-off exercise and should be seen as an ongoing process, and regularly review it.

4.2 Do we need a DPIA?

4.2.1 A DPIA should be done before any type of processing which is "likely to result in a high risk". This means that although the actual level of risk has not been assessed, a DPIA screens for factors that point to the potential for a widespread or serious impact on individuals.

4.2.2 In particular, the GDPR says a DPIA must be done where there are plans to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale

4.2.3 The ICO also requires a DPIA if there are plans to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behavior;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

4.2.4 A DPIA should be considered for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals. For example, the NHS considers the following as specific situations worthy of a DPIA:

- the requirement for a change of the legal basis for processing data;
- replacement of an existing personal data system by new software;
- design and development of a system where the data held is on a consent basis;
- changes to an existing system where additional personal data will be collected;
- a proposal to collect personal data from a new source;
- creation or redesign of web-forms for collecting personal data;
- plans to outsource business processes involving storing and processing personal data;
- intended reuse of information which was originally collected for a limited purpose in a new and unexpected way;
- relocation of staff or equipment;
- stake holder Engagement e.g. surveys.

4.2.5 Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. It is important to note that the individuals referred to are patient/service users and staff.

4.3 Who should carry out a DPIA?

4.3.1 DPIAs should be completed by key project personnel - this could be the project lead, manager or any other key project team member. It is likely that multiple staff from the project will need to be involved with carrying out the DPIA.

4.3.2 It is essential that the person(s) undertaking the DPIA has clear knowledge of the project, the systems involved and the level of information required, therefore this document is for use by anyone who proposes or develops new systems/upgrades existing systems within the organisation.

4.4 When Should a DPIA Be Completed?

4.4.1 A DPIA can help evidence that data protection by design has been considered by accessing data protection and privacy issues upfront in every activity. It can help ensure compliance with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

4.4.2 The GDPR states that data protection by design should happen:

- 'at the time of the determination of the means of the processing' – in other words, when you are at the design phase of any processing activity; and
- 'at the time of the processing itself' – i.e. during the lifecycle of your processing activity

4.4.3 It should begin at the initial phase of any system, service, product, or process. It should start by considering the intended processing activities, the risks that these may pose to individuals, and the possible measures available to ensure compliance with the data protection principles and protect individual rights. These considerations must cover:

- the state of the art and costs of implementation of any measures;
- the nature, scope, context and purposes of your processing; and
- the risks that your processing poses to the rights and freedoms of individuals.

4.4.4 These considerations lead into the second step, where actual technical and organisational measures are put in place to implement the data protection principles and integrate safeguards into the processing.

4.5 What are the underlying concepts of data protection by design and by default?

- a proactive approach to data protection and anticipates privacy issues and risks before they happen, instead of waiting until after the fact;
- privacy as the default setting - design any system, service, product, and/or business practice to protect personal data automatically, with privacy built

into the system, the individual does not have to take any steps to protect their data – their privacy remains intact without them having to do anything;

- privacy embedded into design - embed data protection into the design of any systems, services, products and business practices, ensure data protection forms part of the core functions of any system or service – essentially, it becomes integral to these systems and services;
- put in place strong security measures from the beginning, and extend this security throughout the 'data lifecycle' – process the data securely and then destroy it securely;
- ensuring visibility and transparency to individuals, such as making sure they know what data is processed and for what purpose(s);
- Respect for user privacy – by offering strong privacy defaults, providing individuals with controls, and ensuring appropriate notice is given.
- We should aim to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent where feasible allowing individuals to monitor what is being done with their data and restricting settings to ensure systems aren't accessible by default to an indefinite number of persons.
- Pseudonymisation is defined within the GDPR as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable individual"

4.6 The objective of the DPIA is to avoid the following risks

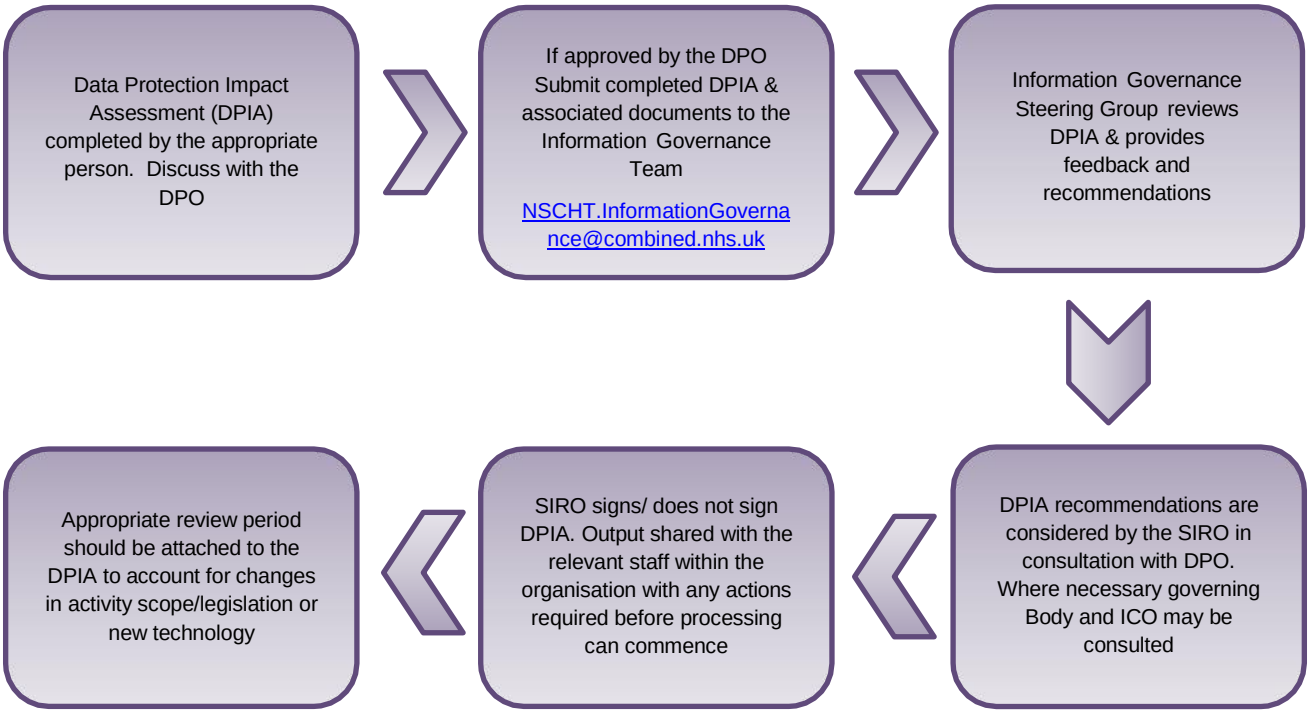
- **Loss of public credibility** as a result of perceived harm to privacy or a failure to meet expectations with regard to the protection of personal information;
- **Imposition of regulatory conditions** as a response to public concerns, with the inevitable cost that entails;
- **The need for system re-design** late in the development stage, and at considerable expense;
- **Collapse of the project, or even of the completed system,** as a result of adverse publicity and/or withdrawal of support by the organisation or one or more key participating organisations;
- **Compliance failure,** through breach of the requirements of the Data Protection Legislation and particularly the GDPR

4.7 Outcomes of an Effective DPIA

4.7.1 An effective DPIA will:

- identify the project's privacy impacts;
- consider those impacts from the perspectives of all stakeholders;
- provide an understanding of the acceptability of the project and its features by the organisations and people that will be affected by it;
- identify and assess less privacy-invasive alternatives;
- identify ways in which negative impacts on privacy can be avoided;
- identify ways to lessen negative impacts on privacy;
- clarify the business need that justifies where negative impacts on privacy are unavoidable;
- document the outcome.

5. DATA PROTECTION IMPACT ASSESSMENT REVIEW PROCESS



6. COMPLETING THE DATA PROTECTION IMPACT ASSESSMENT

6.1 Once the preparation has been completed and the information collated the DPIA template included as Appendix A should be completed along with the Data Protection compliance check Appendix B and the Risk register for Privacy Impact Assessment Appendix C.

7. TRAINING

7.1 There is no specific training in relation to this guidance, however guidance on how to complete the DPIA template can be found at Appendix 1 and the IG Team can provide advice and guidance.

8. REFERENCES AND ASSOCIATED DOCUMENTS

- Information Commissioners Office (Data Protection Act 2018 and General Data Protection Regulation) – www.ico.gov.uk/
- Data Security and Protection Toolkit – https://www.dsptoolkit.nhs.uk

Appendix A: Template

Data Protection Impact Assessment (DPIA)

Project name:

Click here to enter text.

Date DIPA started:

Click here to enter a date.

Stage 1 - preparation for screening

1.1 Project outline – what and why

Note: Explain the scope of the project to ensure you know its aims and its potential impact, explain what the project consists of and why it is undertaken. Map the data flows – where do you obtain the data, how are they processed, where are they stored.

Click here to enter text.

1.2 List of stakeholders

Note: This should cover all individuals involved in the project and those that may be affected by it – internal stakeholders and data subjects. At this stage you want to have as broad a list of groups as possible - this can be edited down at a later stage for more focused consultation.

Internal stakeholders:
Click here to enter text.
Data subjects affected by the project:
Click here to enter text.

1.3 External context

Note: This involves conducting a search for prior projects of a similar nature, from both inside and outside the organisation. This may reveal design features that have been created by other project teams in order to address much the same categories of problem confronted by your project. Note any lessons that can be learned.

Click here to enter text.

Stage 1 completed by:

Click here to enter text.

Date:

Click here to enter a date.

Stage 2 - Compliance with privacy laws

Note: Data Protection legislation is relevant to any DPIA, and a DP compliance check should always be carried out. The Data Protection Officer will be able to advise you on the relevance of other privacy laws.

2.1 General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA)

Note: The template you have to fill in for the data protection compliance check can be found in Appendix A of this document. Your local Data Protection Champion and the Data Protection Officer will be able to assist with the completion.

A Data Protection compliance check has been carried out as part of this DPIA, the details of which are in appendix A. From this we have concluded:

Click here to enter text.

2.2 Human Rights Act (HRA) (Article 8)

Note: In most cases HRA considerations will be covered by the other work on this DPIA, including the Data Protection compliance check. If that is the case, you can simply record here that there are no special considerations that are not covered by other aspects of the DPIA. If there are any outstanding issues, describe them here.

Click here to enter text.

2.3 Privacy and Electronic Communications Regulations 2003 (amended 2011) (PECRs)

If the project involves electronic marketing messages (by phone, fax, email or text), cookies, or providing electronic communication services to the public, you also need to make sure you comply with the PECRs.

The following guidance will help:

Information Commissioner's Office PECR guidance.

Describe any issues here, or confirm if not applicable.

Click here to enter text.

2.4 Common Law duty of confidence

Click here to enter text.

2.5 Others

Click here to enter text.

Stage 2 completed by:

Click here to enter text.

Date:

Click here to enter a date.

Stage 3 - Screening

Note: The information you have gathered in Stage 1 should assist you in addressing the screening questions.

3.1 Technology

3.1.1 Will there be new or additional information technologies that have substantial potential for privacy intrusion?

Yes: ☐

No: ☐

3.2 Data collection

3.2.1 Will the project involve the collection of new information about individuals?

Yes: ☐

No: ☐

3.2.2 Will the project compel individuals to provide information about themselves in the course of the project?

Yes: ☐

No: ☐

3.3 Identification methods

3.3.1 Will there be new or substantially changed identity authentication requirements that may be intrusive or onerous?

Yes: ☐

No: ☐

3.4 Involvement of multiple organisations

3.4.1 Will the initiative involve multiple organisations that will have access to the personal data?

Yes: ☐ No: ☐

3.5 Changes to the way data is handled – considering the actual processing

3.5.1 Will there be new or significant changes to the handling of special categories of personal data or data that would be considered sensitive by the data subjects? Examples are data about racial and ethnic origin, political opinions, health, sexual life, offences and court proceedings, finances and information that could enable identity theft.

Yes: ☐ No: ☐

3.5.2 Will the personal details about each individual in an existing database be processed in a new and different way?

Yes: ☐ No: ☐

3.5.3 If yes to the above, will this involve a large number of individuals?

Yes: ☐ No: ☐

3.5.4 Will there be new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

Yes: ☐

No: ☐

3.6 Changes to data handling procedures – considering policy documents and standards

3.6.1 Will there be new or changed data collection policies or practices that may be intrusive?

Yes: ☐

No: ☐

3.6.2 Will there be changes to data quality assurance or processes and standards that may be unclear or unsatisfactory?

Yes: ☐

No: ☐

3.6.3 Will there be new or changed data security arrangements that may be unclear or unsatisfactory?

Yes: ☐

No: ☐

3.6.4 Will there be new or changed data security access or disclosure arrangements which many be unclear or permissive?

Yes: ☐

No: ☐

3.6.5 Will there be new or changed data retention arrangements that may be unclear or extensive?

Yes: ☐

No: ☐

3.6.6 Will there be changes to the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

Yes: ☐ No: ☐

3.7 Decision on how to proceed

Note: From the work you have done above, you should now be in a position to determine whether you need to do a DPIA, or whether a privacy law compliance check is sufficient. Record your conclusion below:

Click here to enter text.

Stage 3 completed by:

Click here to enter text.

Date:

Click here to enter a date.

Stage 4 - Internal stakeholder consultation

Note: Consult all internal stakeholders identified under 1.2 to conduct a preliminary identification of risks.

4.1 Risk analysis

The table below lists the key privacy risks that have been identified by the internal stakeholders.

Note: You do not need to do a detailed assessment of the risks at this at this stage. It is, however, important to be reasonably clear about what the main risks are.

	Description of risk	Preliminary assessment of exposure Low/Medium/High
Risk 1	Click here to enter text.	L ☐ M ☐ H ☐
Risk 2	Click here to enter text.	L ☐ M ☐ H ☐
Risk 3	Click here to enter text.	L ☐ M ☐ H ☐
Risk 4	Click here to enter text.	L ☐ M ☐ H ☐
Risk 5	Click here to enter text.	L ☐ M ☐ H ☐
Risk 6	Click here to enter text.	L ☐ M ☐ H ☐
Risk 7	Click here to enter text.	L ☐ M ☐ H ☐
Risk 8	Click here to enter text.	L ☐ M ☐ H ☐

Note: From the risks identified by the internal stakeholders you should now be in a position to assess whether an external stakeholder consultation is appropriate. If there are only few low to medium risks, you might wish to continue straight to **Stage 6**.

Is an external stakeholder consultation needed? Note any rationale behind the decision.

Click here to enter text.

Stage 5 - External stakeholder consultation

Note: For Large DPIAs, where there has been extensive consultation, you may wish to produce a separate consultation report, which should then feed into the analysis. **Always** complete Stage 5 to ensure compliance with the Data Protection Act and other privacy laws.

5.1 External consultation

Note: Decide what type of external consultation will be most appropriate and will give you the best and most complete results – focus groups, mail shots, etc.

External stakeholders

Stakeholder name	**The privacy issues they raised**
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

Stage 6 - Risk analysis

Note: You should carry out the risk analysis using exactly the same methodology as you do for other project risks. The table in Appendix B is provided as a guide only and should be adapted to conform to your project risk register.
The Guide to DPIAs provides some useful pointers on the types of solutions to privacy risks that can be explored (see section 7).
The table in Appendix B shows the key risks that have been identified, and the options for avoiding or mitigating those risks.

Stage 7 - Approval

7.1 Recommendation

Note: Drawing on your analysis of the privacy risks and other project risks, explain which option presents the best way forward. If significant risk remains, you should explain what the problem is and why the stakeholder consultation failed to resolve this. Your recommendation may then be that the project needs to be re-thought.

Click here to enter text.

7.2 Approval

Note: For large projects, this stage should align with the Full Business Case and approval should be given by the relevant budget holder. All you need to record below is who has approved the recommendation at 7.1 and the terms of that approval.

Click here to enter text.

Stages 4-7 completed by:

Click here to enter text.

Date:

Click here to enter a date.

Stage 8 - Readiness for service

Note: Explain below what checks were carried out before the service went live to ensure that the privacy solutions approved as part of this DPIA are working, and that the system or process is still legally compliant, as well as whether updates were required to any relevant privacy notices:

Click here to enter text.

Stage 8 completed by:

Click here to enter text.

Date:

Click here to enter a date.

Stage 9 - Review

Note: Indicate below how and when the post-implementation review will be carried out:

Click here to enter text.

Stage 9 completed by:

Click here to enter text.

Date:

Click here to enter a date.

Appendix B

Data protection compliance check

Completion of this template requires knowledge of data protection legislation. Assistance can be obtained from the Trust's Data Protection Officer NSCHT.informationgovernance@combined.nhs.uk

Where you have already provided the information at Stage 1 of the main DPIA Template, simply cross-refer to the relevant answer.

	Question	Answer
1.	What type of personal data is going to be processed?	Click here to enter text.
2.	Which of the legal bases in Article 6 (1) of the GDPR will provide a legitimate basis for the processing? Consult the guidance	Click here to enter text.
3.	If special categories of personal data are going to be processed, which of the legal bases in GDPR Article 9 (in addition to the Article 6(1) legal bases) will provide a legitimate basis for that processing? Consult the document Note – special categories of personal data are personal data consisting of information as to (a) the racial or ethnic origin of the data subject, (b) political opinions, (c) religious beliefs,	Click here to enter text.

	(d) Trade Union membership, (e) physical or mental health, (f) sexual life, (g) genetic data and (h) biometric information.	
4.	Are there any special considerations relating to Article 8 of the Human Rights Act that will not be covered by the DPIA? Note – This Article provides that everyone has the right to respect for his private and family life, his home and correspondence. It is subject to qualifications relating to national security, crime etc.	Click here to enter text.
5.	Will any of the personal data be processed under a duty of confidentiality? If yes, how is that confidentiality being maintained?	Click here to enter text.
6.	How are individuals being made aware of how their personal data will be used?	Click here to enter text.
7.	Does the project involve the use of existing personal data for new purposes?	Click here to enter text.

8.	What procedures will be in place for checking that the data collection procedures are adequate, relevant and not excessive in relation to the purpose for which the data will be processed?	Click here to enter text.
9.	How will the personal data be checked for accuracy?	Click here to enter text.
10.	Has the personal data been evaluated to determine whether its processing could cause damage or distress to data subjects?	Click here to enter text.
11.	Will there be set retention periods in place in relation to the storage of the personal data?	Click here to enter text.
12.	What technical and organisational security measures will be in place to prevent any unauthorised or unlawful processing of the personal data?	Click here to enter text.
13.	Will you be transferring personal data to a country outside of the European Economic Area? If so where, and what arrangements will be in place to ensure that there are adequate safeguards over the data?	Click here to enter text.

Appendix C

Risk register for privacy impact assessment

Risk description	Inherent Privacy Risk			*Options for avoiding or mitigating this risk	Risk Owner	Residual Privacy Risk		
	Impact	Likelihood	Exposure			Impact	Likelihood	Exposure

* For each privacy risk, there could be a number of options for avoiding or mitigating that risk. You should list all the options then consider the residual risk for each one.