Appendix 3. Satsafe Privacy Impact Assessment Tool

Privacy Impact Assessment

PIAs are a tool that you can use to identify and reduce the privacy risks of your projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help us to design more efficient and effective processes for handling personal data.

What do we mean by privacy?

Privacy, in its broadest sense, is about the right of an individual to be let 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, bodily 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 themselves 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.

Projects which might require a PIA include:

- A new IT system for storing and accessing personal data is being proposed
- 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 surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system, for example adding automatic number plate recognition (ANPR) capabilities to existing CCTV
- A new database which consolidates information held by separate parts of an organisation
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring
- A move of office, building or location
- The creation of a policy or procedure which centres on the collection or use of personal identifiable data
- Any other project or activity where through careful consideration a risk could be identified which needs mitigation

Who is responsible for conducting a PIA?

The completion of a PIA should be done through collaboration of the Project Sponsor, Project Manager and the HIG.

Guidance Notes:

(1) Does the project involve new or inherently privacy-invasive technologies?

Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic. Technologies that are inherently intrusive and technologies that are new and sound threatening, excite considerable public concern, and hence represent project risk.

In order to answer this question, considerations include:

- whether all of the information technologies that are to be applied in the project are already well-understood by the public;
- whether their privacy impacts are all well-understood by the organisation, and by the public;
- whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected; and
- whether all of those measures are being applied in the design of the project.

(2) Is the justification for the new data-handling unclear or unpublished?

Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed 'for security reasons', or 'to prevent fraud', are much less likely to calm public disquiet.

(3) Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?

The public understands that an identifier enables an organisation to collate data about an individual, and that identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly onerous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the Project Manager, these are warning signs of potential privacy risks.

(4) Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?

The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (e.g. to support so-called ‘front-end verification'), and the matching of personal data from multiple sources.

Section one:

This section helps the Information Governance Team assess whether further action is required.

Information System or Project Name	
Person completing PIA	
Date:	
Department:	
Is this a new process or a change to an existing process?	
What is the project/system? *Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.*	
Will the project involve the collection of new information about individuals? *This is where the project is increasing information we may already be collecting.*	
Is there a clear justification for the new data handling, is this clear and is it made known to the data subjects?	
Will the project compel individuals to provide information about themselves?	
Are we making additional uses for identifiers already collected?	
Are we creating new identifiers, if so why and with whom are they shared?	

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? *Are we creating new uses?*	
Does the project involve you using new technology which might be perceived as being privacy intrusive? *For example, the use of biometrics or facial recognition.*	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	
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.*	
Will the project require you to contact individuals in ways which they may find intrusive? *Have we obtained consent for making contact?*	
Describe Information Flows – to prevent function creep. *e.g. Obtained, used, retained.*	
Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?	

Will the project result in the handling of a significant amount of new data about data subjects, or change in existing data holding?	
Will the project involve collecting information about a significantly larger group of people?	
Will the data be linked to other systems? *For example will there be new interfaces that link this data to other previously unconnected systems?*	
Will there be new or changed data collection policies or practices that may be unclear or intrusive?	
Does the project involve new or changed data quality assurance processes or standards that may be unclear or intrusive?	
Does the project involve new or changed data security arrangements that may be unclear or intrusive?	
Does the project involve new or changed data access or disclosure arrangements that may be unclear?	
Does the project involve new or changed data retention arrangements that may be unclear?	
Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?	
Will the project give rise to new or changed data handling that is in any way exempt from legislative privacy protections?	

Section 2:

What type of information is involved? Please indicate all likely data types

Personal Information	Please Tick	Sensitive Information	Please Tick
Name		Health/Clinical Related Information	
Initials Only		Religion	
Address		Racial Category	
Postcode		Disabilities	
Part of Postcode		Sexual Orientation	
NI or works/ID Number		Safeguarding Adult or Children	
Local Identifier		Personal Banking/Financial Info	
Date of Birth		Criminal Convictions	
Staff Admin No.		Trade Union Affiliations	
Staff Designation			

Any other types of information not mentioned above please outline in box below:

Data Flows

Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information.

Risk

Risk to Individuals	Corporate and Compliance Risk
Inadequate disclosure controls increase the likelihood of information being shared inappropriately.	Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.	Problems which are only identified after the project has launched are more likely to require expensive fixes.
New surveillance methods may be an unjustified intrusion on their privacy.	The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
Measures taken against individuals as a result of collecting information about them might be seen as intrusive.	Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.	Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
Identifiers might be collected and linked which prevent people from using a service anonymously.	Data losses which damage individuals could lead to claims for compensation.
Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.	Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.	Non-compliance with sector specific legislation or standards.
Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.	Non-compliance with human rights legislation.
If a retention period is not established information might be used for longer than necessary.	

Identify the key privacy risks and the associated compliance and corporate risks. (Larger-scale PIAs might record this information on a more formal risk register).

Privacy Issue	Risk to Individual	Compliance Risk	Associated Organisation/ Corporate Risk

Identify privacy solutions

Describe the actions you 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).

Risk	Solutions	Result - Result: is the risk eliminated, reduced, or accepted	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Signed: …… Date: ……...
Project Lead

Signed: ……. Date: ……
Head of Information Governance