James Hutton Group

Privacy Impact Assessment Guide and Template

Prepared By: Information Governance Officer
Approved By: Data Protection Officer
Date: 19 April 2018

Summary of Changes Since Previous Version:
New Policy.

Contents

James Hutton Group Institute Privacy Impact Assessment

1.0 Overview and Scope

This document applies to the employees, staff, workers and/or other individuals working or undertaking a role under or on behalf of the James Hutton Group which consists of The James Hutton Institute ("Hutton") including Biomathematics & Statistics Scotland ("BioSS") and James Hutton Limited ("JHL"). Hutton is a data controller in respect of all personal data it processes and JHL is a data controller in respect of the personal data it processes. When the terms 'we', 'us' or 'our' are used it should be read as referring to the James Hutton Group, unless otherwise specified.

If you are conducting a project or introducing a new process that will use personal data (see definition at Annex 2), whether you're collecting this information or it has been given to you by a data provider, it may be necessary, or you may be asked by the research commissioner or data provider, to fill in a *Privacy Impact Assessment* (PIA).

This document provides guidance on the following matters:

- What is a PIA?
- When is a PIA needed?
- The role of the Data Protection Officer with regard to PIAs.
- Screening Questions – a helpful guide to help you identify whether a PIA is necessary.
- A template form for a PIA, based on guidance issued by the Information Commissioner's Office. This form walks you through all the issues you need to consider when conducting a PIA.

2.0 What is a PIA?

A PIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. The obligation for Hutton Group to conduct a PIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks presented by the processing of personal data.

PIAs are an important tools for accountability, as they help controllers (such as Hutton/JHL) not only to comply with the requirements of relevant data protection laws, but also to demonstrate that the appropriate measures have been taken to ensure compliance with the relevant data protection laws. A single PIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. They aim at systematically studying new situations that could lead to high risks on the rights and

freedoms of natural persons and there is no need to carry out a PIA in cases that have already been studied. This may be the case for example, where similar technology is used to collect the same sort of data for the same purposes.

A PIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified in the circumstances, taking into account the benefits of what you want to achieve.

3.0 When is a PIA necessary?

Under the General Data Protection Regulation (GDPR) a PIA must be carried out **before** implementation of the new process or project and then periodically thereafter (where appropriate) where the processing is likely to result in a **high risk** to the rights and freedoms of individuals. A further PIA may be necessary following implementation of the process or project if the process or project develops in a manner that may alter the risk from the position when the original PIA was undertaken. In cases where it is not entirely clear whether a PIA is required, it has been recommended that the PIA is carried out nonetheless as a PIA is a useful tool to help controllers comply with data protection law.
In particular, you should carry out a PIA when the processing or project involves:

- Use of new technologies;
- A systematic and extensive evaluation of personal data relating to individuals which is based on automated processing such as profiling and on which decisions are based that produce legal effects concerning the individuals or similarly significantly affecting the individual;
- Systematic monitoring – processing used to observe, monitor or control data subjects, including data collected through networks or a systematic monitoring of a publicly accessible area.
- Large scale processing of special category of data (see definition at Annex 2) or of personal data relating to criminal convictions;
- Matching or combining datasets. For example, originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the individual;
- Data concerning vulnerable data subjects – this involves a power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights;
- Innovative use or applying new technological or organisational solutions; Carrying out profiling on a large scale.
- Carrying out any processing on a large scale.
- Processing biometric or genetic data.
- When the processing in itself prevents data subjects from exercising a right or using a service or a contract. Processing personal data without providing a privacy notice directly to the individual.

- Processing personal data in a way which involves tracking individuals' online or offline location or behaviour.

- Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.

- Processing personal data which could result in a risk of physical harm in the event of a security breach.

- Processing genetic data;

- Processing data that might endanger the individual's physical health or safety in the event of a security breach;

- Where there is a change to the nature, scope, context or purposes of processing.

Some practical examples of when a PIA may be required are (without limitation):

- Introducing a new IT system that stores or processes personal data;
- Developing internal policy or strategies that have data privacy implications;
- Building behavioural or marketing profiles based on usage or navigation on the website;
- Sharing data with other offices or externally;
- Introducing new reasons to process data;
- Undertaking research with vulnerable persons;
- Upgrading existing/processes where personal data exists.

You should aim to process data fairly and transparently, taking into account the rights and legitimate interests of the individuals. You should always consult Hutton's Data Protection Officer when considering whether a PIA is necessary and at the earliest opportunity. Where appropriate, Hutton Group should also seek the views of the data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Failure to carry out a PIA where necessary could lead to the Information Commissioner's Office (ICO) taking enforcement action against Hutton Group.

A PIA is a "living" process to help manage and review the risks of processing and the measures that have been put in place on an ongoing basis. This needs to be kept under review and reassessed if anything changes.

In particular, if you make any significant changes to how or why you process personal data, or to the amount of data you collect, you need to show that your PIA assesses any new risks. An external change to the wider context of processing should also prompt a review of the PIA. For example, if a new security flaw is identified, new technology is made available, or

new public concern is raised over the type of processing you do or the vulnerability of a particular group of data subjects.

4.0 Role of Data Protection Officer with regard to PIAs

Please note that if a PIA is required or you are unsure whether a PIA is required you must contact Hutton's Data Protection Officer at the earliest opportunity and seek their advice. You can contact the DPO on DPO@hutton.ac.uk or 01382 346814. Thorntons Law LLP acts as Hutton's DPO and in the first instance you should ask to speak with Loretta Maxfield, failing which another member of the Intellectual Property and Privacy Team.

The DPO will advise you whether a PIA is required and also assist with the completion of the PIA. If the PIA indicates that the process or project will result in a high risk to individuals measures taken by Hutton Group are unlikely to mitigate the risk, the DPO may require to inform the ICO.

The DPO may also be required to monitor the relevant process and/or project to ensure it is being carried out in accordance with the PIA therefore it is important that you keep the DPO involved as much as possible.

5.0 Screening Questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be required. You can expand on your answers as the project develops if you need to.

NB – If you've been told by a research data provider that you must fill in a PIA, you can skip this section and go straight to the Privacy Impact Assessment form *on page 3.*

1. **Will the processing involve evaluating personal data using automated means including profiling? If so, will decisions be made from this evaluation that would have a legal or significant impact on an individual?**

2. **Will the processing involve large scale processing of special category of data (see definition at rear of this document) or of personal data relating to criminal convictions?**

3. **Will the processing involve systematic monitoring of a publicly accessible area on a large scale? For example, use of CCTV.**

4. **Will the project involve the collection of new information about data subjects?**
   Re-use of data collected for one purpose e.g. providing a service, but now being used for research, is covered by question 4.

5. **Will the project compel individuals to provide information about themselves?**
   This could occur if an organisation has commissioned a research project relating to staff or members of the public.

6. **Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**
   This could also cover situations where an organisation is providing you with information for a research project that they haven't supplied to a third party before.

7. **Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**
   If you are using personal data for any other purpose other than the purpose that it was originally collected for, you need to consider what steps ought to be taken to ensure such processing complies with GDPR.

8. **Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.**
   This would cover things like fingerprint technologies.

9. **Will the project/process result in your making decisions or taking action against individuals in ways that can have a significant impact on them?**
   If you are conducting research for an organisation that could affect their clients or staff, this may apply.

10. **Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records or other information that people would consider to be particularly private.**
    Or any of the special category of personal data, that is, ethnicity or racial origin, political beliefs, religious beliefs, trade union membership, sexual life.

11. **Will the project require you to contact individuals in ways that they may find intrusive?**
    This may vary from individual to individual e.g. some people are happy for their health records to be used for research; others only want them used for their health care.

12. **Has the research funder or data provider asked for the results of a Privacy Impact Assessment?**
    If you have not done a privacy impact assessment prior to this request, but are required to by a research funder or data provider, you will need to fill out this form.

6.0 Privacy Impact Assessment Form

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits or legitimate interests are to the organisation, the purposes of the processing, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a business proposal, project proposal or the research ethics form. Also summarise why the need for a PIA was identified, drawing on your answers to the screening questions.

Step two: Describe the information flows and the necessity of the processing

You should describe the collection, use, storage and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining the data flows i.e. where you are getting the data from, where it will be stored and where it could be transferred to. You should also say how many individuals are likely to be affected by the project/process.

e.g.
Data will be collected from third party organisation/collaborator via secure transfer
↓
Data will be stored encrypted on Hutton network S:Drive
↓
Pseudonymised data set will be provided to department/science group along with report

You should explain and assess why the processing is necessary and how this processing is proportionate in relation to the relevant purposes as well as your assessment of the risks to the rights and freedoms of the individuals.

What types of processing identified as likely high risk are involved?

Describe the scope of the processing: *What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?*
Describe the context of the processing: *What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved?)*
Describe the purposes of the processing: *What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?*

Step three: Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risk, ensuring the protection of personal data. Who should be consulted (e.g. the DPO or data subjects), internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Consultation should be carried out as early as possible and where required as the project progresses.

Step four: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:
What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step five: Identify and assess the privacy and related risks

Identify the key privacy risks to the rights and freedoms of the individual(s) concerned and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex 1 can be used to help you identify the GDPR related compliance risks.

Privacy Issue (Describe the source of risk. Include associated compliance and corporate risks as necessary)	**Risk to Individuals**	**GDPR Compliance Risk**	**Likelihood of harm -** Remote, possible or probable	**Severity of harm -** Minimal, significant or severe	**Overall risk -** Low, medium or high

Step six: Identify privacy solutions

Describe the actions you could take to mitigate the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution	Result – is the risk eliminated, reduced or accepted?	Residual risk – Low, medium or high?	Evaluation – is the final impact on data subjects after implementing each solution justified, compliant and a proportionate response to the aims of the project?

Step seven: Sign off and record the PIA outcomes

Who has approved the privacy risks and mitigating solutions involved in the project? What solutions need to be implemented?

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This PIA will be kept under review by:		The DPO should also review ongoing compliance with PIA

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

Who is responsible for integrating the PIA 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 that may arise in the future?

Action to be Taken	Date for Completion of Actions	Responsibility for Action

Prepared by:
Name and Title of Primary Investigator: Comments: Signed: Date:

Approved by Data Protection Officer:
Contact details: Thorntons Law LLP DPO@hutton.ac.uk 01382 346814 Request to speak with Loretta Maxfield or someone else in the Intellectual Property Team

Comments of DPO:

Signed:……

Date……..

7.0 Annex 1 – Principles of the General Data Protection Regulation (GDPR)

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Article 5 of the GDPR requires that personal data shall be:

a. **processed lawfully, fairly and in a transparent manner in relation to individuals;**
Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

Will the processing be in accordance with data subject rights?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

b. **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;**
Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

c. **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;**
Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

d. **accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;**

If you are procuring new software does it allow you to amend/delete data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

e. **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;**

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Are you procuring software which will adhere to the technical and organisational measures required by the GDPR?

f. **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.**

Will the systems you are implementing ensure that the personal data is secure and will guard against Personal Data Breaches (see Annex 2 for definition)?
Will the project require you to transfer data outside the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Article 5(2) requires that:

i. **the controller shall be responsible for, and be able to demonstrate, compliance with the principles**.

Will the systems/processes you implement clearly demonstrate compliance with the principles of the GDPR?

8.0 Annex 2: GDPR Definitions

Personal Data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category of Data: means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Title	Privacy Impact Assessment Form
Author/Creator	Data Protection Officer, Information Governance Officer
Owner	Information Governance Officer
Date Published/Approved	19 April 2018
Version	Final Draft
Date of Next Review	12 Months from published/approval date
Audience	All
Related Documents	General Data Protection Regulation (GDPR) Policy
Subject/Description	Policy and guide relating to the requirement under GDPR for all organisations to adopt a privacy by design approach when implementing new systems or processes by completing a Privacy Impact Assessment to assess data protection risks and requirements.
Group	Finance and Corporate Services
Department	Research Support