# **York St John University**

**Data Protection Impact Assessment Procedure**

# Introduction

The General Data Protection Regulation (GDPR) introduces a new requirement for organisations to carry out a data protection impact assessment (DPIA) prior to embarking on a project that involves the use of personal data.

A DPIA enables you to

* identify and plan how to deal with the associated privacy risks
* ensure data protection compliance is built into the design of the project, demonstrate openness and transparency; and
* evidence compliance with your legal obligations.

The York St John University’s DPIA procedure must be followed when:

* Planning to introduce a new IT system for storing and accessing personal data.
* Negotiating a new data sharing initiative where two or more organisations agree to share, pool, or link sets of personal data.
* Designing a proposal to identify people in a particular group or demographic and initiate a course of action e.g. analysis.
* Research involving the collection of individuals' personal data.
* Planning to use existing data for a new and unexpected or more intrusive purpose.
* Introducing new policy or strategies that will impact on an individual's/individuals’ privacy through the collection and use of personal data; or through surveillance or other monitoring.

The Information Commissioner's Office lists further examples of when a DPIA is required and provides detailed Data Protection Impact Assessment guidance - <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

The University Secretary is the Data Protection Officer and responsible for providing advice, ensuring the DPIA process is completed appropriately and monitoring its performance pursuant to GDPR Article 35.

# The DPIA Lifecycle

A DPIA helps an organisation to understand the potential impact a planned project or research study may have on an individuals’ privacy and the steps which may be required to identify and reduce those associated risks. This is a key element of the new GDPR focus on accountability and data protection by design, and a more risk-based approach to compliance.

The DPIA process needs to start early in the project - ideally before you start processing - so that action can be taken to address the identified data protection risks by building remedial action into the project plan. It runs alongside the initiative with regular review to ensure the planned actions are effective to reduce risks. It does not have to eradicate the risk, but should help to minimise high risks and consider whether or not the remedial risks are justifiable and manageable.

If your DPIA identifies a high risk which you cannot mitigate, you must consult the ICO before proceeding.



# DPIA Questionnaire

## Project details

Please answer all the questions. DPIA's are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of privacy. This will allow the University to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.
Please complete the **Project Details** in all cases.
Please read the flow chart in the **First Questions** section.

Document whether a **DPIA** is required.
Complete the **DPIA (**if required).

Send the completed workbook to gov.compliance@yorksj.ac.uk so that the Risks and Issues can be assessed.
**If a DPIA is not required, you must retain this workbook within the project documentation in case it is required later either in the project lifecycle or as evidence of compliance with GDPR.**

|  |  |
| --- | --- |
| Project Title: |  |
| Project Lead: |  |
| Project Lead Job Title/Designation |  |
| Email |  | Telephone |  |
| Project Overview |
|  |

## Do I need to complete a DPIA?

If a DPIA is not required, you must retain this workbook within the project documentation in case it is required later either in the project lifecycle or as evidence of compliance with GDPR.

**Read the information to the left. If your project involves any of the listed categories, you need to complete the Screening Questions. If no, a Data Protection Impact Assessment is not required.**

**When do we need to do a DPIA?**

You must do a DPIA before you begin 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 yet, you need to screen for factors which point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR says you must do a DPIA if you plan 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.

The ICO also requires you to do a DPIA if you plan 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 behaviour;
* profile children or target services at them; or
* process data that might endanger the individual’s physical health or safety in the event of a security breach.

## DPIA screening questions

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Screening question** | **Y** | **N** | **Comments** |
| **S1** | Will the project involve the collection of information about individuals? |  |  |  |
| **S2** | Will the project require individuals to provide information about themselves? |  |  |  |
| **S3** | Will you be using information about individuals for a purpose that is not currently used for, or in a way it is not currently used? |  |  |  |
| **S4** | Does the project introduce new or significantly change the way in which personal data about a large number of individuals is handled? |  |  |  |
| **S5** | Does the project introduce new or additional information technologies that can reveal an individual’s identity and has the potential to affect that person’s privacy? |  |  |  |
| **S6** | Does the project involve the use of systematic and extensive profiling or automated decision making to make significant decisions about people? |  |  |  |
| **S7** | Will you be processing special category data or criminal offence data on a large scale? |  |  |  |
| **S8** | Will you be systematically monitoring a publicly accessible place on a large scale? |  |  |  |
| **S9** | Does the project involve the use of new technologies? |  |  |  |
| **S10** | Does the project involve profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit? |  |  |  |
| **S11** | Do you intend to carry out profiling on a large scale? |  |  |  |
| **S12** | Will you be processing biometric or genetic data? |  |  |  |
| **S13** | Does the project involve combining, comparing or matching data from multiple sources? |  |  |  |
| **S14** | Do you plan to process personal data without providing a privacy notice directly to the individual? |  |  |  |
| **S15** | Do you plan to process personal data in a way which involves tracking individuals’ online or offline location or behaviour.  |  |  |  |
| **S16** | Do you plan to process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them |  |  |  |
| **S17** | Do you plan to process personal data which could result in a risk of physical harm in the event of a security breach.  |  |  |  |
| **S18** | Do you plant to carry out any other: * Evaluation or scoring;
* Automated decision-making with significant effects;
* Systematic monitoring;
* Processing of sensitive data or data of a highly personal nature; Processing on a large scale; Processing of data concerning vulnerable data subjects;
* Innovative technological or organisational solutions;
* Processing involving preventing data subjects from exercising a right or using a service or contract.
 |  |  |  |
| **S19** | Will the personal data be processed out of the EU? |  |  |  |

Answering “Yes” to any of the screening questions above represents a potential data protection risk factor. Please proceed and complete the DPIA Questionnaire.

## DPIA

Start to fill in the details from the beginning of the project, after the screening questions have identified the need for a DPIA. The template follows the process that is used in the ICO’s code of practice.

|  |
| --- |
| **Step one: Overview**Explain broadly what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example the project inception document.Also summarise why the need for a DPIA was identified (reference the screening questions).**Project Vision****Project Aims****Project Benefit****Project objectives****Why a PIA is needed** |
| **Step two: Describe the information flows**You should describe the nature of the processing, how you will store, collect, use and delete personal data? Will you be sharing the data with anyone? It may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project. What types of processing identified is likely to involve high risk?**The information flows****Data collection sources****Data use****Data deletion**  |

|  |
| --- |
| **Step three: Describe the categories of personal data** Describe the scope of the processing: what is the nature of the data (personal, pseudonymised); does it include special category data or criminal offences data. How much data will you be collecting and using? How often will you be using it? How long will you keep it? How might individuals are affected? What geographical area does it cover? At what stage do you intend to pesudonymise or anonymise the data? How will you pseudonymise/anonymise data?  |

|  |
| --- |
| **Step 4. Describe the context of the processing.**What is the nature of your relationship with the individuals? How much control over their personal data will they have? Would they expect you to use their data in this way? Does the project include children or other vulnerable groups? Are there any prior concerns over this type of processing or security flaws? Is it novel in any way? Are there any current issues of public concern that you should factor in?  |

|  |
| --- |
| **Step 5: Describe the purposes of the processing.**What do you want to achieve? What is the intended effect on individuals? What are the benefits of processing for you and more broadly? |

|  |
| --- |
| **Step 6: Consultation process**Step 3: Consultation process. Consider how to consult with relevant stakeholders. Describe when and how you will seek individuals’ views - or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? If outsourcing do you need to ask your processors to assist? Do you plan to consult information security experts, or any other expert opinion e.g. Data Protection Officer?  |

|  |
| --- |
| **Step 7: Assess necessity and proportionality.** Describe compliance and proportionality measures, in particular what is your lawful basis for processing? (A *GDPR Article 6 condition; and both an Article 6 and Article 9 condition if processing special categories of personal data or data concerning criminal offences*). Are you relying on consent and if “yes” does it meet the Article 7 conditions of consent requirements? Does your processing actually achieve your purpose? Is there another, less intrusive way to achieve the same outcome? How will you prevent function creep? How will you ensure data minimisation? What information will you give to individuals (privacy notices)? How will you support their individual rights? What measures will you take to ensure your processors comply with your instructions? If processing outside the EU how you will safeguard any international transfers?  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Step eight: Identify the privacy and related risks**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.Annex three can be used to help you identify the DPA related compliance risks.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Describe the source of the risk and nature of the potential impact in individuals. Include associated compliance and corporate risks | Risk to individuals | Likelihood of harm (remote, possible or probable) | Compliance risk | Associated organisation / corporate risk |
|  |  |  |  |  |

 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Step nine: Identify measures to reduce risks**Describe the actions you could take to reduce or eliminate the risks identified, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** |  **Solution(s)** | **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? |
|  |  |  |  |

  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Step ten: Sign off and record the PIA outcomes** Who has approved the privacy risks involved in the project? What solutions need to be implemented?

|  |  |  |
| --- | --- | --- |
| Risk | Approved solution | Approved by  |
|  |  |  |

 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Step eleven: Integrate the PIA outcomes back into the project plan** 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 that may arise in the future?

|  |  |  |
| --- | --- | --- |
| Action to be taken | Date for completion of actions | Responsibility for action |
|  |  |  |

|  |
| --- |
| Contact point for future privacy concerns  |
|  |

 |

# Linking the DPIA to the data protection principles

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

**GDPR Article 5 Principles relating to the processing for personal data**

**Principle 1: Personal data shall be:**

**(a) processed lawfully, fairly and in a transparent manner in relation to the data subject.**

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 Article 6 and Article 9 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?

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?

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

**(b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.**

Does your project plan cover any of the above purposes for processing personal data?

Have you identified a 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?

Is the amount of personal data you are using excessive? 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 regards for the purpose for which they are processed, are erased or rectified without delay.**

If you are procuring new software does it allow you to amend 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 the data subject 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 in accordance with Article 89(1) subject to the implementation of appropriate technical and organisational measures required by this Regulation in order to safeguard the right and freedom of the data subject.**

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?

**(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 and organisational measures.**

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Will the project require you to transfer data outside of the EEA?

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

**Article 5 Principle 2**

**The controller shall be responsible for and be able to demonstrate compliance with principle 1**

You must retain this workbook within the project documentation in case it is required later either in the project lifecycle or as evidence of compliance with GDPR.

**Appendix A**

**Article 89 Research checklist**

If your research project involves the use of “special categories” of personal data you need to satisfy one of the conditions set out in the GDPR Article 9 (as well as an Article 6 condition) and the most appropriate will be:

(2) (j) *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*.

This means if you are using Article 9(2) (j) for your lawful basis you must meet the requirements set out in Article 89.

Article 89 of the GDPR allows controllers to process data for scientific or historical research purposes or statistical purposes as long as appropriate safeguards are in place. Where possible, controllers are required to fulfil these purposes with data that does not permit, or no longer permits, the identification of data subjects using anonymisation or pseudonymisation techniques unless this would prejudice the purpose of the research or statistical process.

If you are processing personal data for these purposes, you must ensure the following:

* Technical and organisational measures are in place to protect the data against risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data;
* data is anonymised or pseudonymised so that it does not permit, or no longer permits, the identification of data subjects;
* A process is in place to justify and record any decision to retain identifiable data if anonymisation is not possible because this would prejudice the purpose of the research or statistical process.
* The minimum amount of personal data necessary for the purpose is used (data minimisation principle)
* The data is not used for the purposes of measures or decisions about an individual data subject,
* The processing of the data is not likely to cause substantial damage or substantial distress to an individual.
* The retention of special category data for research purposes has a public interest justification (UK Data Protection Act Schedule 1 Part 1(4)(c)).