

# Middlesex University Data Privacy Impact Assessment (DPIA) Policy

|  |  |
| --- | --- |
| Policy owner | Legal Team |
| Author if different from above | N/A |
| Version | Version 2 |
| Last Review Date | 01/09/2022 |
| Next Review Due | March 2024, unless circumstances require an earlier review |

Approvals

|  |  |
| --- | --- |
| **Committee / Individual** | **Date** |
| Information Governance Group (IGG) | Approved by the Information Governance Group on 28 Nov 2022 |

**Introduction**

Middlesex University is fully committed to protecting the personal data of data subjects in accordance with the General Data Protection Regulation (GDPR). We take the privacy of personal data very seriously and have initiated a variety of methods and controls to ensure we know what data we collect and hold and that we protect that data appropriately. When the University undertakes any processing activities it should consider this Data Privacy Impact Assessment (DPIA) policy to consider whether a DPIA needs to be done.

DPIAs ensure that relevant staff involved in designing projects think about privacy at the early stages and adopt a data protection by design approach, which referred to in the next section below (Privacy by Design and Default).

DPIA’s are also an effective way to demonstrate the University’s compliance with all data protection principles and obligations.

This DPIA policy also forms part of the University’s research registration process. Researchers should refer to the policy to enable them, in relation to each research project, to make judgements on whether or not a DPIA needs to be done.

**Privacy by Design and Default**

Having a DPIA Policy and following it enables us to comply with the legal requirement under data protection law to have in place appropriate technical and organizational measures to ensure that the data protection principles are followed in practice. This requirement is referred to as data protection *‘by design and default’*. This essentially means that the University must integrate or ‘bake in’ data protection into its processes, activities and business practices from the design stage of activities, and right through the life cycle of activities.

To ensure we deliver privacy by design, where appropriate, a Data Protection Impact Assessment (DPIA) should be done before we start on a project or activity. The DPIA process is designed to help us analyse, identify and minimize the data protection risks of a project or plan.

The purpose of a DPIA is to ensure that:

* our use of personal data is fully understood;
* that risks to the rights and freedoms of individuals resulting from the processing of personal data are carefully examined; and
* that all appropriate measures are put in place to protect these rights throughout the lifecycle of the processing.

A DPIA does not have to eradicate all risk, but it should help the University to minimize and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what we want to achieve.

An effective DPIA allows the staff involved in a project to identify and fix problems at an early stage which benefits the project and the University. There can also be financial benefits to doing a DPIA as it can enable the University to analyse the costs and benefits of an activity, and to consider risks and how to minimize them. Managing risk effectively should minimize the risk of the University facing financial loss or reputational damage as a result of no effective risk analysis having taken place through the DPIA process.

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

It is vital to do a DPIA for **new projects or systems** to ensure compliance with the principle of data protection by design.

A DPIA may also be required if changes are made to an existing project or system. DPIAs must be updated as the process develops, particularly if issues are identified which may affect the risk to the data protection rights of the affected individual.

A DPIA can cover a single processing operation, or a group of similar processing operations. It may be appropriate to rely on an existing DPIA if it covered a similar processing operation with similar risks.

**What types of risks should be assessed?**

Assessing risk is about considering any potential harm to individuals as a result of the processing.

The risks assessed could include actual damage or harm and also the possibility of harm. Harm can include social or economic harm.

There is a significant reputational and financial risk for the University if processing activities are not compliant with data protection law, or where poor decisions are taken which result in risks that cannot be effectively managed, and this results in personal data of individuals being affected.

**DPIA’s should be kept under review**

DPIAs should not be considered as a one- off exercise to file away. A DPIA is a ‘living’ process to help the University manage and review the risks of the processing and the measures put in place on an ongoing basis. DPIAs should be kept under review and should be reassessed if anything changes. In particular, if any significant change is to be made to how or why personal data is processed, or to the amount of data collected, you need to show that your DPIA assesses any new risks. An external change to the wider context of the processing should also prompt you to review your DPIA. For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing you do or the vulnerability of a particular group of data subjects.

**When is a DPIA not required?**

A DPIA would not be required where:

* The processing is not likely to result in a high risk to data subjects’ rights;
* The nature, scope, context and purposes of the processing are very similar to the processing for which a DPIA has already been carried out. Where a set of similar processing operations present similar high risks, a single DPIA may be undertaken to address all of those processing operations;
* or Personal data is not being processed.

**Who should carry out a DPIA?**

In the context of a research project, the Chief Investigator, Principal Investigator, or Supervisor is normally responsible for ensuring the completion of a DPIA, as part of the research registration form.

In relation to other projects/ activities, that the University intends to undertake, the staff responsible for the project/activity should consider whether or not a DPIA is required and should consult the University’s data protection officer for any guidance and advice that they may require for completing the DPIA. Directors and Heads of Service should ensure that the staff undertaking a DPIA are the appropriate staff to do so within their service areas.

Note that in all cases, input and support from relevant third-party data processors should be sought where applicable.

**DPIA Template**

**DPIA’s must be completed using the template form which can be found below and on the intranet at:** [**https://www.intra.mdx.ac.uk/about-us/services/student-and-legal-affairs/gdpr**](https://www.intra.mdx.ac.uk/about-us/services/student-and-legal-affairs/gdpr)

**Middlesex University** **Data Privacy Impact Assessment (DPIA) Template**

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process in accordance with the Data Protection Impact Assessment Policy. The final outcomes should be integrated back into your project plan.

**Screening Questions**

|  |  |
| --- | --- |
| If you state yes to any of these points you will need to complete the DPIA | Yes/No |
| Will the project collect or process any special category data? |  |
| * personal data revealing **racial or ethnic origin**; * personal data revealing **political opinions**; * personal data revealing **religious or philosophical beliefs**; * personal data revealing **trade union membership**; * **genetic data**; * **biometric data** (where used for identification purposes); * data concerning **health**; * data concerning a person’s **sex life**; and * data concerning a person’s **sexual orientation**. | Yes/No |
| Will the project collect or access any personal financial data or other confidential or private information? | Yes/No |
|  |  |
| Will the project access precise location information? | Yes/No |
|  |  |
| Will the project’s intended audience be children (under 13 years old) and/or teens (13-18 years old) OR will the project unintentionally collect children’s/teens’ personal information? | Yes/No |
|  |  |
| Will the project involve the profiling or evaluation of individuals' preferences? | Yes/No |
|  |  |
| Is it possible that personal information will be used for making entirely automated decisions on an individual in a way that significantly affects such individuals? | Yes/No |
|  |  |
| Is it possible that personal information will be used for making entirely automated decisions on an individual in a way that significantly affects such an individual? | Yes/No |
|  |  |
| Will the project involve observing, monitoring or controlling individuals, including data collected through networks or systematic monitoring of a publicly accessible area? | Yes/No |
|  |  |
| Will the project involve the processing of an individual's data by new or innovative technologies? | Yes/No |

**Step 1: Identify the need for a DPIA**

|  |
| --- |
| Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer to or link to other documents, such as a project proposal. Summaries of why you identified the need for a DPIA. |
|  |

**Step 2: Describe the processing**

|  |
| --- |
| **Describe the nature of the process:** |
| How will you collect, use, store and delete data?  What is the source of the data?  Will you be sharing data with anyone?  You might find it useful to refer to a flow diagram or other way of describing data flows.  What types of processing identified as likely high risk are involved? |

|  |
| --- |
| **Describe the scope of the process:** |
| What is the nature of the data, and does it include special category or criminal offence data?  If you are processing a special category, will you be processing (delete appropriate)?   * personal data revealing **racial or ethnic origin**; * personal data revealing **political opinions;** * personal data revealing **religious or philosophical beliefs**; * personal data revealing **trade union membership**; * **genetic data**; * **biometric data** (where used for identification purposes); * data concerning **health**; * data concerning a person’s **sex life**; and * data concerning a person’s **sexual orientation**.   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 process:** |
| What is the nature of your relationship with 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 process:** |
| What do you want to achieve?  What is the intended effect on individuals?  What are the benefits of the process – for you, and more broadly? |

**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?  Do you need to ask your processors to assist?    Do you plan to consult information security experts, or any other experts? |

**Step 4: Assess necessity and proportionality**

|  |
| --- |
| **Describe compliance and proportionality measures, in particular:** |
| What is your lawful basis for processing? Please select one:  **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.  **(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.  **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).  **(d) Vital interests:** the processing is necessary to protect someone’s life.  **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.  **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)  Does the process actually achieve your purpose?  What rights will the data subjects have? Please delete it if not appropriate.   1. The right to be informed 2. The right of access 3. The right to rectification 4. The right to erasure 5. The right to restrict processing 6. The right to data portability 7. The right to object 8. Rights in relation to automated decision making and profiling.   Is there another way to achieve the same outcome?  How will you prevent function creeping?  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 5: Identify and assess risks**

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| Example of risk: | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |

**Step 6: Identify measures to reduce risk**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
|  |  | Eliminated reduced accepted | Low medium high | Yes/no |

**Step 7: Sign off and record outcomes**

|  |  |  |
| --- | --- | --- |
| **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 DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |

**Sign off of DPIAs**

Staff must refer all DPIA’s to the University’s Data Protection Officer for sign off.

**Guidance for completing DPIA training**

The University’s Data Protection Officer should be contacted for any guidance and training required to complete a DPIA.

**Data Protection Officer Contact Details:**

Email: dpaofficer@mdx.ac.uk