

## Data Protection Impact Assessment (DPIA) Screening Questions

Use this form to record the outcome of your DPIA screening exercise. Completed forms should be returned via e-mail to dataprotection@uwe.ac.uk . Where one or more questions in Section A are answered **YES**, a full Data Protection Impact Assessment will be required. For more guidance please see the explanatory notes on the following web page: [dataprotectionimpact.aspx](https://www1.uwe.ac.uk/about/corporateinformation/datamanagement/dataprotectionimpact.aspx)

When should this form be completed?
DPIA screening questions **must** be completed for any new system, project, activity or process collecting, storing, using or disposing of personal data (any information relating to an identified or identifiable living individual). They must also be completed for any change in process that for example may collect new personal data or process it for different purposes.

What happens next?

Once you have your completed the screening questions and you have answered “yes” to any of the mandatory questions, you must proceed to step 1 of the Data Protection Impact Agreement (DPIA) and complete. If you have answered “No” to the mandatory questions, but “Yes” to the advisory questions, it is strongly recommended that you conduct a DPIA. If you have answered “No to all questions” you are not required to complete a DPIA.

If you have any questions or are unsure if you should be completing a DPIA, please contact the Data Protection Office who advise whether you are required to conduct a full Data Protection Impact Assessment.

|  |
| --- |
| Data Protection Impact Assessment (DPIA) |
| Title of Project |  | Date |  |
| Owner (Dept) |  | DPIA conducted by (your name) |  |

|  |  |  |
| --- | --- | --- |
| Mandatory grounds to conduct a DPIA - SECTION A | Yes | No |
| 1. Will the project be using systematic and extensive profiling to make significant decisions about people? Examples include knowledge transfer partnerships using assistive technology
 | [ ]  | [ ]  |
| 1. Will the project process special category (sensitive) or criminal offence data on a large scale? Examples include health clinics.
 | [ ]  | [ ]  |
| 1. Will the project systematically monitor publicly accessible places on a large scale (e.g. CCTV)?
 | [ ]  | [ ]  |
| 1. Are you using new technologies e.g. biometrics, genetic, facial recognition or a major new piece of software? Examples include use of learner analytics and new student records systems
 | [ ]  | [ ]  |
| 1. Will the project use profiling of special category (sensitive) data or criminal offence data to decide on access to services, opportunity or benefit? Examples include asking all applicants to declare criminal convictions
 | [ ]  | [ ]  |
| 1. Will the project combine, compare or match data from multiple sources? Examples include wealth screening of alumni as potential donors
 | [ ]  | [ ]  |
| 1. Will the project process personal data without providing a privacy notice directly to the individual (‘invisible processing’)? Examples include scraping or mining personal data from external sources for research
 | [ ]  | [ ]  |
| 1. Will the project process personal data in a way which involves tracking individuals’ online or offline location or behaviour and meets one or more of the other criteria in Section A? Examples include using cookies for targeted advertising and CCTV
 | [ ]  | [ ]  |
| 1. Will the project process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them? Examples include offering an online chat service to under 16s
 | [ ]  | [ ]  |
| 1. Will the project process data that might endanger the individual’s health or safety in the event of a security breach? Examples include Wellbeing Records
 | [ ]  | [ ]  |
| If you’ve answered YES to any of the questions 1 – 10 then it is a legal requirement that you conduct a DPIA – move to Step 1 on page 4 |
| Advisory grounds to conduct a DPIA – SECTION B | Yes | No |
| 1. Will the project involve **large scale processing** of personal data?
 | [ ]  | [ ]  |
| 1. Will the project involve **profiling** or **monitoring or automatic decision making**?
 | [ ]  | [ ]  |
| 1. Does the project involve **Special category (sensitive data) or criminal offence data** or the use of the personal data of **vulnerable individuals (including children)**?
 | [ ]  | [ ]  |
| If you’ve answered YES to any of the questions 11 – 13 then it is strongly recommended that you conduct a DPIA – move to Step 1 on page 4. If you decide not to complete a DPIA even though you’ve answered Yes in section B, then email this form with an explanation as why to dataprotection@uwe.ac.uk |
| If you’ve answered ‘No’ to ALL the above question to do not need to conduct a DPIA.  |
|  |
| Full DPIA required? (Data Protection Office use only) | [ ]  | [ ]  |



## Data Protection Impact Assessment (DPIA)

## <Insert name of project/processing activity>

This template must be used to record your DPIA process and outcome. It follows the process set out in our [DPIA guidance](https://intranet.uwe.ac.uk/tasks-guides/Guide/data-protection), and should be read alongside [ICO guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/) and the [Criteria for an acceptable DPIA](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711) set out in European guidelines on DPIAs.

Queries regarding DPIAs should be directed to dataprotection@uwe.ac.uk

DPIA process

1. DPIA screening process **must** be considered and documented for any activity involving the processing of personal data
2. If applicable (i.e. the screening questions identify the necessity for a mandatory DPIA), this template **must** be completed:
3. Complete Steps 1 – 6
4. Send draft via e-mail to dataprotection@uwe.ac.uk for DPO advice on step 7
5. Complete step 7, sign and send a copy via e-mail to dataprotection@uwe.ac.uk . Keep the original for reference. The DPO will maintain a copy centrally. Please note that UWE may need to submit this document as evidence to the regulator.

# Step 1: Identify the need for a DPIA

|  |
| --- |
| 1. Summarise why you identified the need for a DPIA. (This can draw on your answers to the screening questions.)
 |
|  |
| 1. Explain broadly what the project aims to achieve and what type of processing it involves.
 |
|  |
| 1. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. (Identify other documents here).
 |

# Step 2: Describe the processing

|  |
| --- |
| **Describe the nature of the processing:** |
| 1. How will you collect, use, store and delete data?
 |
|  |
| 1. What is the source of the data?
 |
|  |
| 1. 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.
 |
|  |
| 1. What types of processing identified as likely high risk are involved?
 |
|  |

|  |
| --- |
| **Describe the scope of the processing:**  |
| 1. What is the nature of the data, and does it include special category or criminal offence data?
 |
|  |
| 1. How much data will you be collecting and using? How often?
 |
|  |
| 1. How long will you keep it?
 |
|  |
| 1. How many individuals are affected?
 |
|  |
| 1. What geographical area does it cover?
 |
|  |

|  |
| --- |
| **Describe the context of the processing:**  |
| 1. What is the nature of your relationship with the individuals?
 |
|  |
| 1. How much control will they have?
 |
|  |
| 1. Would they expect you to use their data in this way?
 |
|  |
| 1. Do they include children or other vulnerable groups?
 |
|  |
| 1. Are there prior concerns over this type of processing or security flaws?
 |
|  |
| 1. Is it novel in any way?
 |
|  |
| 1. What is the current state of technology in this area?
 |
|  |
| 1. Are there any current issues of public concern that you should factor in?
 |
|  |
| 1. Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
 |
|  |

|  |
| --- |
| **Describe the purposes of the processing:**  |
| 1. What do you want to achieve?
 |
|  |
| 1. What is the intended effect on individuals?
 |
|  |
| 1. What are the benefits of the processing – for you, and more broadly?
 |
|  |

# Step 3: Consultation process

|  |
| --- |
| **Consider how to consult with relevant stakeholders:** |
| 1. Describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so.
 |
|  |
| 1. Who else do you need to involve within your organisation?
 |
|  |
| 1. Do you need to ask your processors to assist?
 |
|  |
| 1. 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:**  |
| 1. What is your lawful basis (or bases) for processing?
 |
|  |
| 1. Does the processing actually achieve your purpose??
 |
|  |
| 1. Is there another way to achieve the same outcome?
 |
|  |
| 1. How will you prevent function creep?
 |
|  |
| 1. How will you ensure data quality and data minimisation?
 |
|  |
| 1. What information will you give individuals?
 |
|  |
| 1. How will you help to support their rights?
 |
|  |
| 1. What measures do you take to ensure processors comply?
 |
|  |
| 1. How do you safeguard any international transfers?
 |
|  |

# Step 5: Identify, assess and reduce risks

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary (see [Appendix 1](#RAG) for risk assessment guidance) | **Likelihood of harm**Remote/ Possible/ Probable | **Severity of harm**Minimal/ Significant/ Severe | **Overall risk** Low, medium or high | **Options to reduce or eliminate risk** | **Effect on risk**Eliminated/ Reduced/ Accepted | **Residual risk**Low/ Medium/ High | **Measure approved**Yes/no |
| Lawfulness, fairness and transparency*Example: Inadequate privacy information provided to data subjects* | Remote | Significant | High | *Example: Privacy notice information provided to data subjects and where appropriate GDPR compliant consent obtained and recorded.* | Choose an item. | Medium | No |
| Purpose limitation*Example: Data is processed for a purpose unrelated to and incompatible with why it was collected* | Choose an item. | Choose an item. |  | *Example: Appropriate policy document and training for relevant staff.* |  |  |  |
| Data minimisation*Example: More data is collected than is necessary to meet defined purpose, for example individuals may submit details of irrelevant offences* | Choose an item. | Choose an item. |  | *Example: Policy document to prescribe what data can be collected and processed. Process to remove irrelevant information submitted by data subjects*. |  |  |  |
| Accuracy*Example: Inaccurate data is collected and processed which may be used to make decisions about individuals* | Choose an item. | Choose an item. |  | *Example: Verification process where data is to be used to make admissions decision. Guidance for data subjects but difficult to mitigate where false information is deliberately provided by data subjects.* |  |  |  |
| Storage limitation*Example: Data kept for longer than is necessary* | Choose an item. | Choose an item. | Choose an item. | *Example: Approved Retention Schedule and process to securely delete records in a timely fashion according to this schedule.* | Choose an item. | Choose an item. | Choose an item. |
| Security*Example: Breach resulting from insecure storage of data* | Choose an item. | Choose an item. | Choose an item. | *Example: Records to be stored only in UWE secure storage*. | Choose an item. | Choose an item. | Choose an item. |
| Accountability*Example: Accountability principle not met: no record of processing or appropriate policies in place* | Choose an item. | Choose an item. | Choose an item. | *Example: Updated Record of Processing, approved DPIA and relevant policies in place.* | Choose an item. | Choose an item. | Choose an item. |

# Step 6: 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 |

**Glossary**

*Automated decision making and profiling* – Automated decision-making is the process of making a decision by automated means about a person without any human involvement. Profiling is automated processing of personal data to evaluate certain things about an individual e.g. to categorise individuals by traits or behaviours.

*Data Protection principles* - principles are rules about what you can and can’t do with personal data. Generally speaking if you follow these rules you will be able to comply with GDPR:

*Fair, lawful and transparent* – Personal data is handled in line with individuals’ reasonable expectations, under an appropriate [legal basis](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/) and in a transparent manner which does not mislead or deceive. An example of breaching this principle would be failing to provide individuals with a Privacy Notice then selling their details to a direct marketing company without their knowledge.

*Purpose limitation* – Personal data is only processed for specified purposes and not subsequently used for other incompatible purposes. An example of purpose creep breaching this principle would be if a researcher on a project exploring physical injuries disclosed his participant database list to his wife, who runs a travel agency, so that she can offer special holiday deals to research subjects needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

*Data minimization* – means only collecting data you need for the cited purpose(s). An example breaching this principle would be collecting an excessive amount of information from delegates when administering an event.

*Accuracy* – means you should take reasonable steps to ensure data and up to date. An example of breaching this principle would be failing to update a change of address when notified by a member of staff or student.

*Storage limitation* – means keeping personal data for only as long as is necessary. In reality this means you need to have a data retention policy or rationale for keeping data such as a legal requirement or business need. An example of breaching this principle would be keeping details of unsuccessful applicants for an indeterminate period just in case they decide to apply again in future.

*Security* – means making sure appropriate security measures are in place including technical controls such as encryption of data and non-technical measures such staff training. Examples of breaching this principle include failing to have access restrictions in place on student records systems and failing to provide training for staff.

*Data Processor* - A person, public authority, agency or other body which processes personal data on behalf of UWE, Bristol.

*ICO* – Information Commissioner’s Office, which is the regulator of data protection in the UK.

[*International transfers*](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/) – Transfer of personal data overseas (most commonly from cloud storage). In particular there are restrictions in place where personal data is transferred outside the European Economic Area (EEA) to a country deemed not to have adequate data protection in place.

*Personal data* - Personal data means any information that can be attributed to an identifiable living individual.

*Processing* - In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

*Scraping/ mining personal data* – using software to harvest personal data from pre-existing databases.

*Security flaws* – See security principle

*Special categories* - Special category data is personal data which the GDPR and/or other legislation states is more sensitive than simply personal data. It has more restrictions upon processing and needs more protection than personal data. The following types of personal information are defined as special categories: data relating to health (physical and mental), ethnicity, sexual orientation, sex life, trade union membership, biometric or genetic data, and political, philosophical and religious opinions/beliefs. Details of criminal offences and convictions and related security measures must also be afforded similar treatment.

**Appendix 1- DPIA risk definitions and Risk Assessment Guidance**

The following definitions and risk matrix should be used to assess the risks you have defined in step 5.

**Likelihood of harm**

*Remote* – Very low or low likelihood that will occur (less than 10% chance)

*Possible* – Reasonable possibility that will occur (between 10% and 50%)

*Probable* – More likely to occur than not (greater than 50% chance)

**Severity of harm**

*Minimal* – Little or no impact on rights and freedoms of affected data subjects, little or no impact to UWE’s reputation, little or no financial implication (e.g. would not lead to a regulatory fine or successful claim from affected data subjects), little or no operational impact.

*Significant* – Risk to rights and freedoms of affected data subjects, may impact on UWE’s reputation, financial risk is medium (may lead to a regulatory enforcement fine and/or successful claim from affected data subjects), may have an operational impact.

*Severe* - High risk to rights and freedoms of affected data subjects, will have a significant impact on UWE’s reputation, high financial risk (likely to lead to substantial regulatory enforcement fine and successful claim from affected data subjects), would be likely to have a significant operational impact.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | *SEVERE* | **LOW RISK** | **HIGH RISK** | **HIGH RISK** |
|  | *SIGNIFICANT* | **LOW RISK** | **MEDIUM RISK** | **HIGH RISK** |
|  | *MINIMAL* | **LOW RISK** | **LOW RISK** | **LOW RISK** |
| **SEVERITY OF HARM** |  | *REMOTE* | *POSSIBLE* | *PROBABLE* |
|  |  | **LIKELIHOOD OF HARM** |  |  |