Guidance on Data Protection Impact Assessments

1. Introduction
   1. The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA) require the University as a data controller to consider and apply appropriate measures designed to implement their key principles effectively. Necessary safeguards must be incorporated into all activities involving the processing of personal data in order to ensure that the rights and freedoms of individuals are protected.
   2. A key element of the UK GDPR’s focus on accountability is the requirement to undertake a Data Protection Impact Assessment (DPIA) where any processing of personal data is “likely to result in a high risk” to the rights and freedoms of individuals.
   3. A DPIA therefore serves as a tool to help the University to identify, evaluate and mitigate risks to individuals arising as a result of the processing of their personal data. At the same time, a DPIA should ensure compliance with data protection law and other legal and regulatory requirements (for example, the Equality Act 2010).
   4. A failure to undertake a DPIA when required under the UK GDPR may result in a fine of up to £17.5 million or 4% of total global annual turnover, whichever is higher.
2. About this Guidance
   1. This Guidance sets out the University’s approach towards identifying the need for, undertaking, and implementing DPIAs.
3. Scope of this Guidance
   1. This Guidance is to be used in all cases where new processing of personal data is planned. This could include a new administrative system, novel uses of data (particularly where this could not reasonably be expected by data subjects), a new external supplier (or new processing for an existing supplier), or application or portal used by participants or attendees at an event. This guidance is also to be used where there is a contract renewal where the University are using an existing supplier.
   2. This process is suitable for Research projects. Where a Data Management Plan (DMP) has not been completed. . Research using personal data cannot take place without approval under the University Research Ethics process. Failure to gain this approval may well result in the destruction of all personal data and any research results or products.
4. Roles and responsibilities
   1. All members of staff involved in the development of projects, initiatives, studies, processes and systems (collectively referred to in this Guidance as Initiatives) are responsible for ensuring that they are aware of this Guidance and understand the circumstances in which a DPIA should be undertaken.
   2. The University Secretary’s Office is responsible for overseeing and reviewing the implementation of this guidance and must be consulted in relation to any DPIAs undertaken in accordance with its requirements.
   3. In practice, it is the responsibility of the staff member or team (i.e. the project manager, system owner, principal investigator etc.) leading an Initiative to undertake the screening questions and produce the first draft of a DPIA if necessary (see Appendix 1). This can then be further worked up in collaboration with the Head of Data Protection and Legal Services, who is the Data Protection Officer, and other relevant stakeholders.
   4. Draft DPIAs should be sent to the Data Protection Officer: dataprotection@sheffield.ac.uk.

1. Identifying the need for a DPIA
   1. The process to be followed when ascertaining whether to undertake a DPIA is attached at Appendix 1.
   2. A DPIA must be undertaken before the processing of any personal data which is “likely to result in a high risk to the rights and freedoms” of individuals. As such, it is necessary to identify whether there are any factors that warrant the need for a DPIA to be undertaken.
   3. In the case of any Initiatives involving the processing of personal data that were commenced before 25th May 2018 (when the UK GDPR came into force) and which are ongoing, such Initiatives should be reviewed and the need to undertake a DPIA considered.
   4. The UK GDPR requires a DPIA to be undertaken where any Initiative will involve:
2. the systematic and extensive evaluation of personal data by automated means, including profiling, resulting in decisions that would have significant effects for those individuals;
3. the processing of special categories of personal data or personal data relating to criminal convictions and offences on a large scale; or
4. the systematic monitoring of a publicly accessible area on a large scale.
   1. Where any new Initiative will involve the processing of personal data, the DPIA Screening Questionnaire in Appendix 1 should be completed. It is expected that the questionnaire will be completed by those leading the development of the Initiative.
   2. Before completing the questionnaire, it is important to:
5. identify the key stakeholders in the Initiative so that they can provide their input into the questionnaire; and
6. have a clear understanding of the scope and objectives of the Initiative so that the questionnaire can be completed as fully and accurately as possible.
   1. Where the outcome of the questionnaire suggests that the processing is unlikely to result in a high risk to individuals, there may be circumstances where it is advisable to undertake a DPIA anyway due to:
7. the nature, scope, context and purposes of processing personal data;
8. the groups of individuals affected by the processing (e.g. children or vulnerable adults);
9. the level of investment in the Initiative in terms of time, financial and other resources; or
10. the visibility of the Initiative internally and externally.
    1. Where it has been concluded that a DPIA is unnecessary and will not be undertaken, the reasons for this should be clearly documented. The Screening Questionnaire should be sent to the Data Protection Officer in addition to being retained. This will evidence the decision made. It may need to be revisited and reviewed at a later date. The Data Protection Officer will keep a register of completed DPIAs.
11. Undertaking a DPIA
    1. Having concluded that a DPIA is necessary or desirable for a particular Initiative, the DPIA Template in Appendix 1 should be completed. The DPIA Template explains the objectives and requirements of each section. Where any section is not completed because it is not applicable or not considered necessary, this should be explained.
    2. Part of the DPIA may involve consultation with relevant internal and external stakeholders. In the case of consultation with third party data processors, the contract with such third parties should include an obligation on them to provide assistance with undertaking DPIAs. However, this may have cost implications which should be considered and discussed with the third parties beforehand. In the case of consultation with professional advisers and other experts, the scope and cost of their involvement will need to be considered and approved by the University’s Data Protection Officer.
    3. Where the DPIA identifies Legitimate Interests as a lawful basis, Appendix 2 should be completed and approval granted from the Data Protection Officer.
12. Consultation with the ICO
    1. Where the outcome of a DPIA is that the processing of personal data in the context of an Initiative would result in a high risk and it is not possible to take any measures to eliminate or mitigate that risk, the UK GDPR requires that the processing cannot commence before the Information Commissioner’s Office (ICO) has been consulted.
    2. The ICO should not be consulted without the approval of the University’s Data Protection Officer, who will initiate contact with the ICO. Consultation with the ICO should only be necessary in very exceptional instances as it is expected that the University will be able to apply measures to appropriately mitigate or eliminate risk on most occasions.
13. Review of DPIAs
    1. A DPIA should be undertaken at the earliest opportunity in the development of an Initiative and re-assessed prior to commencement of the relevant processing activities to identify whether any changes to the Initiative impact upon the outcomes of the DPIA and whether the controls and measures identified in the DPIA have been integrated into the Initiative.
    2. Once the processing of personal data has commenced in respect of an Initiative, the DPIA should be reviewed regularly having regard to the nature and risks associated with the processing, and taking into account any changes to the processing activities or scope of the Initiative. A review should be undertaken at least annually by the staff member or team leading or owning the Initiative.
14. Disclosure and publication of DPIAs
    1. There is no legal requirement to proactively disclose or publish a DPIA, although it could be subject to a request made under the Freedom of Information Act 2000 and so may need to be released, subject to any exemptions contained in the legislation. However, it may be necessary to disclose a DPIA to another institution to provide assurance that due and proper consideration has been given to the data protection implications of an Initiative.
    2. A decision may also be taken to publish a DPIA in order to further build trust and confidence in the processing of personal data in relation to an Initiative and to demonstrate accountability and transparency. However, such a decision may only be taken in consultation with the University’s Data Protection Officer, and any DPIA that is being published should be redacted to remove any confidential or commercially sensitive information.
15. Policy review
    1. This Policy will be reviewed as required and at least every two years by the University Secretary and the Head of Data Protection and Legal Services.

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Editor** | **Description of Change** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Appendix 1**

**Data Protection Impact Assessment**

|  |  |  |
| --- | --- | --- |
| **Step 1: Identifying the need for a DPIA** | | |
| **Part A: Project overview** | | |
| Please provide an overview of the project. What does it involve and what will it aim to achieve? | | |
|  | | |
| What personal data will be processed? Please list the categories of personal data e.g. name, email address, date of birth etc. | | |
|  | | |
| **Part B: DPIA Screening Questions** | | |
| **Question** | **Yes** | **No** |
| 1. Will the project involve the processing of new (or additional) types of information about individuals? |  |  |
| 1. Is the project already processing personal data about individuals without a DPIA having been carried out? |  |  |
| 1. Will the project compel individuals to provide information about themselves before they can make use of the service provided? |  |  |
| 1. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information, including third party processors? |  |  |
| 1. Are you using information about individuals for a purpose for which it is not currently used, or in a way it is not currently used? |  |  |
| 1. Does the project involve processing sensitive (“[Special Category](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/)”) personal data? |  |  |
| 1. Does the project involve the personal data of vulnerable people? |  |  |
| 1. Does the project involve processing personal data on a large scale? |  |  |
| 1. Does the project involve systematic monitoring? |  |  |
| 1. Does the project involve the use or application of innovative technological or organisational solutions? |  |  |
| 1. Does the project involve automated decision-making that may have a significant effect on an individual? |  |  |
| 1. Does the project involve evaluating or scoring individuals (including profiling and predicting)? |  |  |
| 1. Does the project involve datasets that have been matched or combined? |  |  |
| 1. Is the data transferred internationally? |  |  |
| **If you have answered “Yes” to any of these questions, then a full Data Protection Impact Assessment is required; please proceed to step 2 below to complete this.** | | |

|  |
| --- |
| **Step 2: Describe the processing** |
| **Part A: Describe the nature of the processing** |
| What is the data flow? Where is the data being transferred? Which IT systems will be used? Who will have access to those systems?  Please provide a diagram if necessary |
|  |
| How will you collect, use, store and delete data?  Please provide as much detail as possible: the more detail you provide, the easier it is for the Data Protection Team to understand the project and assess the risks. |
|  |
| What is the source of the data? |
|  |
| Will you be sharing data with anyone? |
|  |
| What types of processing identified as likely high risk are involved? |
|  |
| **Part B: Describe the scope of the processing** |
| 1. What is the nature of the data, and does it include [Special Category](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/) or criminal offence data? |
|  |
| 1. How much data will you be collecting and using? |
|  |
| 1. How often will the collection and use occur? |
|  |
| 1. How long will you retain the data, taking into account the University’s [Retention Schedule](https://docs.google.com/spreadsheets/d/1qwtsZbVf8w07wmLMUlArh-J4ZRthID6_shUVv0iHVBI/edit#gid=360049762)? |
|  |
| 1. How many individuals are affected? |
|  |
| 1. Is there an international data transfer? If so, to which country/countries is the data being transferred? |
|  |
| **Part C: 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 are there any 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)? |
|  |

|  |
| --- |
| **Step 3: Consultation process** |
| 1. How will you seek individuals’ views? If you are not going to ask individuals for their views, then please justify why it is not appropriate to do so. |
|  |
| 1. Who else do you need to involve within your organisation? |
|  |
| 1. Are you using a data processor? If so, do you need to ask the processor to assist? |
|  |
| 1. Do you plan to consult information security experts, or any other experts? Have you consulted the University’s [Information Security Team](https://staff.sheffield.ac.uk/it-services/risk-assessments)? |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Step 4: Assessing necessity and proportionality** | | | |
| 1. What is your lawful basis for processing?   Data protection law requires us to have a lawful basis for processing personal data. Please select the appropriate lawful basis from the list of Article 6 UK GDPR lawful bases below.  If you are processing special category personal data, you need a lawful basis under Article 6 UK GDPR and a lawful basis under Article 9 UK GDPR. Please select the appropriate lawful bases from the list of Article 6 UK GDPR and Article 9 UK GDPR lawful bases below.  Please see the [ICO guidance on lawful bases](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/) if you need help deciding which lawful basis you should select. | | | |
| **Article 6 UK GDPR – Personal Data** | | **Article 9 UK GDPR – Special Category Data** | |
| Article 6(1)(a) – Consent |  | Article 9(2)(a) – Explicit consent |  |
| Article 6(1)(b) – Contract |  | Article 9(2)(b) – Employment, social security & social protection\*\* |  |
| Article 6(1)(c) – Legal obligation |  | Article 9(2)(c) – Vital interests |  |
| Article 6(1)(d) – Vital interests |  | Article 9(2)(d) – Not-for-profit body |  |
| Article 6(1)(e) – Public task |  | Article 9(2)(e) – Made public by the data subject |  |
| Article 6(1)(f) – Legitimate interests\* |  | Article 9(2)(f) – Legal claims |  |
| *\* If you have selected Article 6(1)(f) – Legitimate interests as your lawful basis, you must complete the Legitimate Interests Assessment at Appendix 2 of this document (please see below).* | | Article 9(2)(g) – Substantial public interest\*\* |  |
| Article 9(2)(h) – Medicine, Employee capacity, Medical Diagnosis, Health or Social Care\*\* |  |
| Article 9(2)(i) – Public health\*\* |  |
| Article 9(2)(j) - Archiving, Scientific and Historical Research or Statistical Purposes\*\* |  |
| *\*\* If you have selected (b), (g), (h), (i), or (j) as your lawful basis, you also need to select a condition under* [*Schedule 1 of the Data Protection Act 2018*](https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted)*. Please specify which condition you have selected:* | |
|  | | | |
| 1. What information will you give data subjects? Is there a Participant Information Sheet? Are you providing a Privacy Notice? If so, please can you provide a copy of this? | | | |
|  | | | |
| 1. How will you help to support data subjects’ rights e.g. will they have the right to make a Subject Access Request? Will you be able to delete their data if they make a request for erasure? | | | |
|  | | | |
| 1. If you are using a data processor, is there a data processing agreement in place with them? If so, please provide us with a copy of this so that we can review it alongside the DPIA. Please contact the Data Protection Team if you require a copy of our standard data processing agreement template. | | | |
|  | | | |
| 1. How do you safeguard any international transfers? Will you use the [International Data Transfer Agreement](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/)? | | | |
|  | | | |
| 1. Have you recorded the processing activity on your department’s Information Asset Register? | | | |
|  | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Steps 5 and 6: Identifying, assessing and mitigating risks** | | | | | | |
| **Risk** | **Likelihood** (Remote/ Possible/ Probable) | **Severity** (Minimal/Significant/Severe) | **Risk** (Low/Medium/High) | **Mitigation measure** | **Residual risk** | **Measure approved** (Yes/No) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **Step 7: Sign off and record outcomes** | |
| **Part A: DPIA Sign-off** | |
| DPIA Approved (Yes/No): |  |
| Name of Data Protection Team officer: |  |
| Date of approval/rejection: |  |
| Comments/summary of advice: |  |
| DPIA to be kept under review by (Name/Date of agreement to keep DPIA under review): |  |
| **Part B: Review of DPIA Sign-off** (for use where the processing activity described in the DPIA has not been approved) | |
| **DPO Review of DPIA** | |
| DPIA Approved (Yes/No): |  |
| Name: |  |
| Date of approval/rejection: |  |
| Comments/summary of advice: |  |
|  | |
| **SIRO Review of DPIA** | |
| DPIA Approved (Yes/No): |  |
| Name: |  |
| Date of approval/rejection: |  |
| Comments/summary of advice: |  |
|  | |
| **UEB Review of DPIA** | |
| DPIA Approved (Yes/No): |  |
| Date of approval/rejection: |  |
| Comments/summary of advice: |  |

**Appendix 2**

**Legitimate Interests Assessment**

**Please note: You only need to complete this Appendix if you have selected “Article 6(1)(f) – Legitimate interests” as your lawful basis in Step 4, Question 1 above.**

|  |
| --- |
| **Part A: Purpose Test – you need to assess whether there is a legitimate interest behind the processing** |
| Why do you want to process the data? |
|  |
| What benefit do you expect to get from the processing? |
|  |
| Do any third parties benefit from the processing? |
|  |
| Are there any wider public benefits to the processing? |
|  |
| How important are the benefits that you have identified? |
|  |
| What would the impact be if you couldn’t go ahead with the processing? |
|  |
| Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements, or e-privacy legislation)? |
|  |
| Are you complying with other relevant laws? |
|  |
| Are you complying with industry guidelines or codes of practice? |
|  |
| Are there any other ethical issues with the processing? |
|  |

|  |
| --- |
| **Part B: Necessity test – You need to assess whether the processing is necessary for the purpose you have identified** |
| Will this processing actually help you achieve your purpose? |
|  |
| Is the processing proportionate to that purpose? Please explain why. |
|  |
| Can you achieve the same purpose without the processing? |
|  |
| Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way? |
|  |

|  |
| --- |
| **Part C: Balancing Test – You need to consider the impact on individuals’ interests and rights and freedoms and assess whether this overrides your legitimate interests.** |
| **Nature of personal data** |
| Is it special category data or criminal offence data? |
|  |
| Is it data which people are likely to consider particularly ‘private’? |
|  |
| Are you processing children’s data or data relating to other vulnerable people? |
|  |
| Is the data about people in their personal or professional capacity? |
|  |
| **Reasonable expectations** |
| Do you have an existing relationship with the individual? |
|  |
| What is the nature of the relationship and how have you used data in the past? |
|  |
| Did you collect the data directly from the individual? What did you tell them at the time? |
|  |
| If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? |
|  |
| How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? |
|  |
| Is your intended purpose and method widely understood? |
|  |
| Are you intending to do anything new or innovative? |
|  |
| Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation? |
|  |
| Are there any other factors in the particular circumstances that mean they would or would not expect the processing? |
|  |
| **Likely Impact** |
| What are the possible impacts of the processing on people? |
|  |
| Will individuals lose any control over the use of their personal data? |
|  |
| What is the likelihood and severity of any potential impact? |
|  |
| Are some people likely to object to the processing or find it intrusive? |
|  |
| Would you be happy to explain the processing to individuals? |
|  |
| Can you adopt any safeguards to minimise the impact? |
|  |
| Can you offer the individuals an opt-out? (Yes/No) |
|  |

|  |  |
| --- | --- |
| **Making the decision: This is where you use your answers to Parts 1, 2 and 3 to ascertain whether or not you can apply the legitimate interests basis.** | |
| Can you rely on legitimate interests for this processing? (Yes/No) | |
|  | |
| Do you have any comments to justify your answer (Optional)? | |
|  | |
| LIA completed by: |  |
| Date: |  |
| LIA approved by: |  |
| Date: |  |