|  |  |
| --- | --- |
| Data Protection Impact Assessment  |  |
|  |

This template can be used to record the DPIA process and outcome. It is based on the template designed by the Information Commissioner, and follows the process set out in the ICO [guidance](https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf).

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.
The ICO [guidance](https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf) sets out the mandatory circumstances that require a DPIA, and provides useful examples. The final outcomes should be integrated back into your project plan.

**You should involve the University Data Protection Officer at an early stage in your DPIA by contacting** dpa@abdn.ac.uk.

|  |  |
| --- | --- |
| Project name |  |
| Project lead |  |
| DPIA lead |  |
|  |
| Revision History |
| Version | Date | Notes |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| Step 1: Identify the need for a DPIA |
|  |
| Explain briefly what the project aims to achieve, what type of [personal data](https://www.abdn.ac.uk/staffnet/governance/data-protection-6958.php#panel11099) is involved and why this led you to carry out a DPIA, referring to any relevant [mandatory circumstances](https://www.abdn.ac.uk/staffnet/governance/data-protection-6958.php#panel8628). You may find it helpful to link to other documents, such as a PID or research protocol. |
| <text> |
|  |
| Step 2: Describe the processing |
|  |
| **Describe the nature of the processing:** * How will you collect personal data? How often? What is the source(s) of the personal data?
* What will you use the personal data for?
* Will you share personal data with anyone? Will they use the data for a different purpose?
* Where will you store the personal data?
* How long will you keep the personal data? How will you then destroy the personal data?

You may find it helpful to add a diagram showing the flow of personal data. Even if you do not have all the answers, please provide what you can. |
| Collection of personal data<text>Use of personal data<text>Sharing of personal data<text>Storage of personal data<text>Retention and destruction of personal data<text>What security is in place including any contractual arrangements?<text>Who will have access to the data and how will they get access and how will it be controlled?<text>What audit trail capability does the system have (both in terms of access to and amending of a person’s records)?<text>What data will be migrated and how?<text>Will data be shared or is external access permitted?<text>What are the arrangements for the return of data at the end of the contract and for prompt destruction of data thereafter?<text>Is the system able to suspend a person’s record (place it on hold); add a note to a person’s record (and to make that note visible to system users consulting those records); is the system able to gather and export the entirety of a person’s records (if required?) <text> |
|  |
| **Describe the scope of the processing:** * Who are the individuals whose personal data will be used (the data subjects)? How many individuals are affected? Do they share a common characteristic? Are they from one geographical area? What is the relationship between them and the University?
* What is the nature of the personal data? Does it include [special categories of personal data](https://www.abdn.ac.uk/staffnet/governance/data-protection-6958.php#panel11100) or criminal offence data? How much of their personal data will you collect and use?
 |
| Data subjects<text>Types of personal data<text> |
|  |
| **Describe the context of the processing:** * Would the data subjects expect you to use their personal data in this way? How will you provide them with [privacy information](https://www.abdn.ac.uk/staffnet/governance/data-protection-6958.php#panel8632) explaining how their personal data will be used?
* Do the data subjects include children (under 18 years) or other vulnerable groups? Will you take any additional steps to meet their needs?
* Will data subjects be able to request access to their data? Or correct it? Or destroy it?
* Are there concerns over this type of processing or security flaws?

Does the project involve novel use of personal data or new technology? |
| Expectations of data subjects<text>Provisions for children and vulnerable groups<text>Data subjects’ level of control over their personal data<text>Concerns or novelty of processing<text> |
|  |
| **Describe the purposes of the processing:** * What is the intended effect of the project on data subjects?
* What are the benefits of the processing – for you, and more broadly?
 |
| Effects on data subjects<text>Benefits<text> |
|  |
| Step 3: Consultation process |
|  |
| **Consider how to consult with individuals affected by the processing:** * Describe when and how you will seek data subjects’ views on the proposal – or why it’s not appropriate to do so.
* Will you consult anyone else in the University? Or external partners and stakeholders?
 |
| Plan to consult data subjects<text>Plan to consult other stakeholders and experts<text> |
|  |
| Step 4: Assess necessity and proportionality |
|  |
| **Describe compliance and proportionality measures:** * What is your lawful basis for processing personal data? Do you have a valid exemption for processing special categories of personal data?

(The University Data Protection Officer will assist with the lawful basis and any exemption.)* To achieve your purpose, is it strictly necessary to use this type of personal data, in the ways you have set out and to keep it for as long as you propose?

Are there other, less intrusive ways to achieve the same outcome?* How will you ensure data quality and data minimisation?

How will you help data subjects to exercise their rights? How will they contact you?What measures will you take to ensure [processors comply with their obligations](https://www.abdn.ac.uk/staffnet/governance/data-protection-6958.php#panel8785)?How will you [safeguard any transfers](https://www.abdn.ac.uk/staffnet/governance/data-protection-6958.php#panel8629) of personal data to countries outside the UK? |
| Lawful basis for processing personal data<text>Necessity of processing<text>Measures to support proportionality<text> |

|  |
| --- |
| Step 5: Identify and assess risks |
|  |
| **Describe source of risk and nature of potential impact on individuals.** Include compliance risks and corporate risksas necessary. Use the [DPIA risk assessment matrix](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how10) to determine the level of each identified risk. |
| **Risk****ref** | **Risk and impact description** *Use one row per risk. Add additional rows if necessary.* | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|  |  | Remote, Possible or Probable | Minimal, Some harm or Serious harm | Low, Medium or High |
|  | <text> |  |  |  |
|  | <text> |  |  |  |
|  | <text> |  |  |  |
|  | <text> |  |  |  |
|  | <text> |  |  |  |
|  |
| Step 6: Identify measures to reduce risk |
|  |
| **Identify additional measures**What action could be taken, or controls put in place, to reduce or eliminate those risks identified as Medium or High level in step 5? |
| **Risk****ref** | **Options to reduce or eliminate risk** | **Measure approved** | **Effect on risk** | **Residual risk** |
|  |  | Yes/No | Eliminated, Reduced or Accepted | Low, Medium or High |
|  | <text> |  |  |  |
|  | <text> |  |  |  |
|  | <text> |  |  |  |
|  | <text> |  |  |  |
|  | <text> |  |  |  |

|  |
| --- |
| Step 7: Sign off and record outcomes |
|  |  |  |
| **Consultation responses** |
| Summarise the responses of the affected individuals consulted in step 3. If the views of individuals have not been accepted or followed in the proposal, explain the reason. |
| <text> |
|  |
| **DPO advice** |
| Advice on whether appropriate safeguards have been applied, whether the DPIA has been carried out correctly and whether the outcome complies with data protection requirements. |
| <text> |
| DPO advice provided by: |  |
| Date: |  |
|  |
| **Risk acceptance** |
| * I will ensure any measures to control risk in the description of processing (step 2), and any additional measures to reduce risk that I have accepted (step 6), are implemented.
* I have considered the summary of consultation responses and the DPO advice.
* I accept the residual risks involved in this processing activity.
 |
| Decision on DPO advice | Accepted / Overturned (delete as appropriate) |
| Measures and risks accepted by: |  |
| Date: |  |
|  |
| The DPIA will kept under review by: |  |
| Date the DPIA will be reviewed: |  |