**University of Cambridge**

**Data Protection Impact Assessment (DPIA) Template**

|  |
| --- |
| This template presupposes a basic knowledge of the core concepts of, and terms used within, the General Data Protection Regulation (GDPR) and wider data protection legislation. These are summarised at <https://www.information-compliance.admin.cam.ac.uk/data-protection> and <https://www.information-compliance.admin.cam.ac.uk/data-protection/guidance/provisions>  Contact: <https://www.information-compliance.admin.cam.ac.uk/contact-us>  Version 1, issued May 2018 |

**Introduction and guidance notes**

**What is a DPIA?**

A DPIA is a requirement of the GDPR. It is a documented assessment of the data protection considerations surrounding a proposed (or ongoing) procedure, system, project or initiative. It:

1. Describes the nature, scope, context and purposes of the (proposed) personal data processing.
2. Assesses the necessity and proportionality of the (proposed) personal data processing.
3. Identifies and assesses risks to individuals.
4. Identifies any additional measures to mitigate those risks.

**Who completes this DPIA template?**

Parts A to C of this DPIA template should be completed by those responsible for the procedure, system, project or initiative. It should then be sent to the Information Compliance Office ([data.protection@admin.cam.ac.uk](mailto:data.protection@admin.cam.ac.uk)), which will complete Part D and liaise with the independent Data Protection Officer as necessary.

**When is a DPIA needed?**

A DPIA is required where the proposed (or ongoing) procedure, system, project or initiative represents a high risk to the rights and freedoms of individuals. The below list of headings shows when a DPIA is either mandatory or recommended. It should be stressed, when reading some of the broadly-worded headings (especially those at headings 4 to 13), that a DPIA is triggered where proposed (or ongoing) personal data processing represents a high risk to individuals. Accordingly, whether or not there really could be a high risk to individuals should be considered alongside the headings below.

*Headings 1 to 3 below represent circumstances when a DPIA is* ***mandatory*** *because they are listed in the GDPR itself:*

1. Where there is systematic and extensive automated profiling with significant effects on individuals.
2. Where there is large-scale use of sensitive (special category) personal data or personal data about criminal convictions and offences.
3. Where there is systematic and large-scale public monitoring.

*Headings 4 to 13 below represent circumstances when a DPIA is* ***mandatory*** *because they are included in a formal list published by the Information Commissioner:*

1. Where innovative technologies (especially Artificial Intelligence) are being used in relation to the personal data processing.
2. Where an individual’s access to/refusal of services is being determined by automated profiling and/or involves their sensitive (special category) personal data.
3. Where there is systematic and extensive profiling (unlike heading 1 above, not necessarily automated and not necessarily producing significant effects on individuals).
4. Where biometric personal data are being used.
5. Where genetic personal data are being used for non-healthcare purposes.
6. Where personal data will be collected and matched from multiple sources, especially in an unusual way.
7. Where personal data that have not been collected from data subjects are used without those data subjects’ knowledge.
8. Where personal data are used for online or physical tracking.
9. Where children under 13 or other vulnerable individuals will be targeted with direct marketing, profiled, or offered online services involving personal data processing.
10. Where a personal data breach could jeopardise the health and safety of individuals.

*Headings 14 and 15 below represent additional circumstances when a DPIA is* ***recommended****, especially if both headings apply, because they are included in an advisory list published by European data protection regulators and are not otherwise covered by headings 1 to 13 above:*

1. Where personal data will be evaluated and scored.
2. Where personal data will be processed on a notably large scale (unlike heading 2 above, not necessarily using sensitive (special category) personal data).

If you are in doubt as to whether a DPIA is necessary, please contact the Information Compliance Office ([data.protection@admin.cam.ac.uk](mailto:data.protection@admin.cam.ac.uk)).

**What about research projects?**

This template is designed principally for DPIAs at the University in an administrative/IT context. Relevant University research projects undergo pre-existing processes, usually as part of ethical reviews, which encompass the core required elements of a DPIA. However, a consideration of the questions in this template may help researchers to formulate and refine the data protection aspects of their projects.

**What happens to a completed DPIA?**

A copy of the completed DPIA will be held on file in the Information Compliance Office as part of the University’s accountability obligations under the GDPR. A copy should also be retained with the documentation for the procedure, system, project or initiative. If a completed DPIA reveals an unmitigated high risk, the Data Protection Officer has to consult the ICO before proceeding.

**Part A – Description of the personal data processing**

|  |  |
| --- | --- |
| **1. Factual details about the procedure, system, project or initiative** | |
| 1.1 Title of procedure, system, project or initiative |  |
| 1.2 Lead contact (name and email address) |  |
| 1.3 Has a DPIA previously been carried out in relation to this procedure, system, project or initiative? If so, when? |  |
| 1.4 Briefly describe the procedure, system, project or initiative. |  |
| 1.5 What are its general purposes and benefits? |  |
| 1.6 Who are the main stakeholders? |  |
| 1.7 Will any of the main stakeholders be consulted during the development of the procedure, system, project or initiative? If so, how? If not, why not? |  |

|  |  |
| --- | --- |
| **2. Factual details about the personal data used by the procedure, system, project or initiative** | |
| 2.1 Who are the data subjects (students, staff, alumni, etc.)? Are any of them children (under 13) or vulnerable adults? |  |
| 2.2 Where does the personal data come from (the data subjects themselves, public sources, other University systems, etc.)? |  |
| 2.3 How many data subjects might personal data be collected from/held about? |  |
| 2.4 What types of personal data might you be collecting or using? Is there any sensitive (special category) data involved? |  |
| 2.5 What format(s) (hard copy, electronic database, online images, etc.) will the personal data be held in? |  |

**Part B – Necessity and proportionality assessment**

|  |  |
| --- | --- |
| **1. Lawfulness, transparency and purpose** | |
| 1.1 What legal basis/bases are you relying upon to process the personal data? |  |
| 1.2 If the legal basis is consent, how is the consent collected and evidenced? |  |
| 1.3 If the legal basis is the legitimate interests of the University, what are those interests and how are they balanced against the interests of the data subjects? |  |
| 1.4 Are the data subjects already told their data will be used in this way (e.g. in a privacy notice)? If so, how and by who? If not, how will they be told and by who? |  |
| 1.5 What are the specific purposes of the personal data use? If you are re-using personal data, are these the same purposes for which the personal data were originally collected? |  |

|  |  |
| --- | --- |
| **2. Data quality** | |
| 2.1 Are all of the personal data you propose to collect/use/store really necessary? |  |
| 2.2 How will the personal data be kept accurate and of high quality? What are the consequences of inaccuracy for the data subjects? |  |
| 2.3 How long will (different types of) personal data be kept for? Can anything be anonymised/pseudonymised at any stage? |  |

|  |  |
| --- | --- |
| **3. Data security** | |
| 3.1 How will access to the personal data be controlled? |  |
| 3.2 Will the personal data be backed up? |  |
| 3.3 Will the personal data be encrypted, in whole or in part? |  |
| 3.4 What other technical and/or policy controls will be implemented to secure the personal data? |  |
| 3.5 How will personal data breaches be recognised? |  |
| 3.6 How will those accessing and using the personal data be trained/advised on data protection matters? |  |

|  |  |
| --- | --- |
| **4. Rights** | |
| 4.1 Will the data subjects be able to:  a. access their personal data?  b. correct their personal data?  c. delete their personal data?  d. object to the use of their personal data?  e. restrict the distribution of their personal data?  If not, why not? |  |
| 4.2 Will any automated decisions be taken about the data subjects? If so, why? Will they know about the logic behind them? |  |

|  |  |
| --- | --- |
| **5. Data sharing** | |
| 5.1 Will the personal data be shared beyond the University? If so, who with and why? |  |
| 5.2 Will the personal data be stored or transferred outside the EEA? If so, who with and why? |  |
| 5.3 Will relevant agreements/contracts be put in place with these third parties to govern the sharing? If not, why not? |  |

**Part C – Risks and mitigations**

Complete the following table for each risk to the data subjects (or any other individuals) that arises from the procedure, system, project or initiative. (Examples of risks include: illegitimate access to personal data; undesired modification of personal data; loss of personal data; identity theft or financial loss; being misled or deceived about personal data uses; unnecessary intrusion into an individual’s private/family life; or being monitored unknowingly.)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk description** | **Risk likelihood**  1: Rare  2: Unlikely  3: Possible  4. Likely  5. Almost certain | **Risk severity**  1. Very low  2. Low  3. Medium  4. High  5. Very high | **How will the likelihood of this risk be mitigated?** | **Risk likelihood (after mitigation)**  1: Rare  2: Unlikely  3: Possible  4. Likely  5. Almost certain | **How will the severity of this risk be mitigated?** | **Risk severity (after mitigation)**  1. Very low  2. Low  3. Medium  4. High  5. Very high |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Now send your DPIA to the Information Compliance Office:** [**data.protection@admin.cam.ac.uk**](mailto:data.protection@admin.cam.ac.uk)

**Part D – Information Compliance Office review and Data Protection Officer advice**

This section should only be completed by the Information Compliance Office.

|  |  |  |
| --- | --- | --- |
| **DPIA Reference number:** |  | |
| **Date DPIA received:** |
|  | **Comments** | **Name and date** |
| 1. Is the form fully completed? |  |  |
| 2. Are the risk mitigation measures suitable? |  |  |
| 3. Are the residual risks acceptable? |  |  |
| 4. Consult the DPO. |  |  |
| 5. Summarise the DPO’s advice. |  |  |
| 6. Is the DPO’s advice accepted? If not, why not? |  |  |
| 7. Describe the implementation of the DPO’s advice (if applicable). |  |  |
| 8. Set a future DPIA review date (if necessary). |  |  |