***Introduction***

As a Data Controller, the College must assess risks of harm associated with any project involving personal data. The *General Data Protection Regulation (GDPR)* and *Data Protection Act 2018 (DPA)* identify certain types of processing activities as likely to result in a **high risk** to individuals. A Data Protection Impact Assessment (DPIA) is a process to help data controllers identify and address the data processing risks in a specific context.

Your Data Protection Officer (DPO) has produced a Screening Questionnaire to assist Colleges in identifying whether a particular processing activity is **high risk**. The outcome of that has triggered the requirement to carry out a full DPIA for your specific project or processing.

Please complete this form in full, ensuring that you keep your College Data Protection Lead (CDPL) informed throughout the process. They are your first source of advice and guidance. Where necessary, as required under current data protection legislation, your CDPL may also contact the DPO at college.dpo@ois.cam.ac.uk for notification and guidance.

Your completed DPIA will be reviewed and signed off by the CDPL, who acts as *de facto* DPO in relation to these impact assessments.

**NOTE**: A DPIA **ONLY** addresses the processing of personal data in relation to data protection legislation. It does not address directly the requirements and considerations of other privacy laws (including, but not limited to, e-communications regulations, consumer laws, or equality and discrimination legislation). Compliance with other legal requirements should be evaluated separately.

***Section A: Project outline***

Please provide basic information about the project and the date that this form was completed (this should correspond with the information provided on the Screening Checklist):

|  |  |
| --- | --- |
| Responsible Department |  |
| Name and position of responsible person |  |
| Project title |  |

|  |  |
| --- | --- |
| Length of the project (providing dates if applicable)Is it a finite project? Is it a permanent change? |  |
| Date form completed |  |

***Section B: Description (end-to-end) of personal data processing*** *(Article 35(7)(a) GDPR)*

The following questions assist you in describing the nature, scope context and purpose of the personal data processing you intend to carry out as part of this project. If a business case, project plan or operational document already exists already, you may choose to append it.

|  |  |
| --- | --- |
| 1. Description of the personal data processing

What is it for? How will it benefit the College, individuals and/or other parties? *Provide as much detail as possible*. |  |
| 1. Why do you need to undertake this processing?
 |  |
| 1. Who is involved in the processing within the College?

List all individual roles (or teams) involved in processing personal data at any stage of this project.*You can edit the list as the project progresses.* |  |
| 1. Who is involved in the processing outside the College?

List all teams or companies involved in processing personal data at any stage of this project.*You can edit the list as the project progresses.* |  |
| 1. Will you be relying on any third parties to process the data?
 | Yes\* [ ]  No [ ] \* If ‘Yes’, you must be satisfied with, and have details of, their data processing procedures and security measures before allowing access to your personal data.  |
| 1. Types of personal data collected, created, stored or otherwise processed during the project
 | **Personal data**Name [ ] Date of birth/Age [ ] Gender [ ] Contact details [ ] Financial data (e.g. income, bank details) [ ] Unique identifier (e.g. CRSid, NI or NHS Number) [ ] Online identifier (e.g. IP address, Cookie identifier) [ ] Vehicle number plate [ ] Other *(please specify)*:……..…………………………………………………….**Special categories of personal data** Race [ ] Ethnic origin [ ] Political opinions [ ] Religious or philosophical beliefs [ ] Trade union membership [ ] Sex life [ ] Sexual orientation [ ] Health data (e.g. medical history, sick leave) [ ] Genetic data [ ] Biometric data, used to identify an individual [ ] **Other sensitive information** Criminal convictions and offences [ ] Other *(please specify)*:……..……………………………………………………. |
| 1. Whose personal data is it?
 | Students [ ] Staff (inc. Fellows) [ ] University [ ] Retired/Ex-College personnel [ ] Alumni [ ] Donors (inc. alumni) [ ] Visitors [ ] Other *(please specify)*:……..……………………………………………………. |
| 1. How many records will you process annually (approx.)?
 | Fewer than 100 [ ] 100-1,000 [ ] 1,000-10,000 [ ] More than 10,000 [ ] Does this represent **large scale** processing of the College’s personal data? Yes [ ]  No [ ]  |
| 1. What IT assets are you using in the personal data processing?

For example: hardware, software, systems, networks, etc. |  |
| Are any of the above new to the users? Yes [ ]  No [ ]  |
| 1. Does the data you create as part of the project still represent personal data?
 | Yes [ ]  No [ ]  |
| 1. Where are you storing and/or sending the outputs?
 |  |
| 1. How long will you retain this data?

Either give a timescale or criteria on how you will decide how long to retain it for.  |  |
| 1. How will you anonymise or destroy the data once the purpose has been achieved?
 |   |

***Section C: Establishing Necessity and Proportionality*** *(Article 35(7)(b) GDPR)*

The following questions assist you in determining how your project complies with each of the seven Data Protection Principles set out by GDPR. These principles are:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

|  |  |
| --- | --- |
| 1. Lawfulness of processing
 | 1. Necessary for the performance of a **contract** Yes [ ]  No [ ]

If ‘Yes’, what do you consider the contract to be? For example, student offer letter, staff contract of employment, Fellowship election letter, gift pledge, etc.……………………………………………………. |
| 1. Necessary to achieve the **legitimate interest(s)** of:

The College Yes [ ]  No [ ] If ‘Yes’ what do you consider the legitimate interest(s) to be? …………………………………………………….A third party Yes [ ]  No [ ] If ‘Yes’ what do you consider the legitimate interest(s) to be?……………………………………………………. |
| 1. **Processing is necessary to protect** someone’s life **(i.e. vital interests)**

Yes [ ]  No [ ] If ‘Yes’, whose vital interest are involved (e.g. students, visitors)?  ……..……………………………………………………. |
| 1. Necessary for the performance of a task carried out by the College in the **public interest** or in the exercise of its **official authority** Yes [ ]  No [ ]

If ‘Yes’ what do you consider to be the statute or common law for the relevant task, function or power for which you are processing the personal data?……………………………………………………. |
| 1. Necessary to protect the College in the event of a **legal claim** (excluding contractual) Yes [ ]  No [ ]
 |
| 1. **Consent** of the data subject**\*** Yes [ ]  No [ ]

If ‘Yes’:1. How do you capture and record consent\*?

…………………………………………………….1. When and how do you plan to refresh this consent\*?

…………………………………………………….1. What actions will you take if/when consent is withdrawn?

……..…………………………………………………….\* Where possible, avoid relying on **consent**, as it can be time-limited or withdrawn and processing must cease as a result. |
| 1. Are you using the personal data for the purposes for which it was collected?

Refer to the relevant published data protection statement(s) | Yes [ ]  No [ ] If ‘Yes’, list the original purposes of the personal data ……..……………………………………………………. |
| 1. Do you need to use personal data to complete the processing?
 | Yes [ ]  No [ ]   |
| 1. Could you achieve the desired outcome(s) of the activity/project using anonymised data instead?
 | Yes [ ]  No [ ] If ‘No’, provide the reason(s) for your decision: ……..……………………………………………………. |
| 1. Are you confident that the personal data you will use is up-to-date (and otherwise accurate)?
 | Yes [ ]  No [ ]  |
| 1. What security measures (technological, physical, organisational) exist to protect the personal data?
 |  |
| 1. How is information about the project or processing provided to the data subject?

For example, listed under a heading in a data protection statement; outlined directly at the point of data collection, etc. |  |
| 1. Is it likely that the data subject would be surprised to know you were processing their data in this way?
 | Yes [ ]  No [ ]  |
| 1. Do you have measures in place to manage requests from individuals to:
 | Access their personal data Yes [ ]  No [ ]  N/A [ ] Obtain and reuse their personal data for their own purposes Yes [ ]  No [ ]  N/A [ ] Rectify their personal data Yes [ ]  No [ ]  N/A [ ] Delete their personal data Yes [ ]  No [ ]  N/A [ ] Object to or restrict processing Yes [ ]  No [ ]  N/A [ ] Withdraw consent (e.g. to automatic decision making) Yes [ ]  No [ ]  N/A [ ]  |
| 1. Will personal data be transferred to a country outside of the European Economic Area (EEA)?
 | Yes [ ]  No [ ] If ‘Yes’, describe what arrangements will be in place to safeguard the personal data: ……..……………………………………………………. |
| 1. Prior consultation
 | Will you be seeking individuals’ views during this process?Yes [ ]  Describe how and when you will seek to consult data subjects: ……..…………………………………………………….No [ ]  Give reasons why consultation with data subjects is not appropriate: ……..…………………………………………………….Will you be asking any external data processors to assist with this process?Yes [ ]  No [ ] Do you plan to consult with external information security or other experts, e.g. the ICO? Yes [ ]  No [ ] If ‘Yes’, whom: ……..…………………………………………………….Note: Processing should not begin until after consultations are completed. If the DPIA relates to an existing activity, processing may need to cease until after the consultation. Please speak to your College Data Protection Lead (CDPL) for guidance. |

***Section D: Risk Assessment*** *(Article 35(7)(c) GDPR)*

This section assists you in identifying the risks that the processing activity may cause to data subjects, as well as solutions you intend to implement in order to eliminate, reduce or accept them.

For each risk, you should consider the **likelihood** of each risk from occurring (or recurring) and the **potential impact** (harm or damage) your processing may have on individuals. The impact could be physical, emotional or material.

You should use your answers in the earlier sections when detailing the nature and level of risks. Pay close attention to processing that may result in:

* Loss of access to, or control over, personal data
* Loss of access to services or opportunities
* Physical harm
* Reputational damage
* Loss of confidentiality
* Identity theft
* Fraud, including financial loss
* Re-identification of pseudonymised data

Examples of risks include (but are not limited to):

* How would any outputs or outcomes of processing be affected if it turns out that the personal data you are using contains errors?
* Is there any negative impact on the privacy of the data subjects?
* What impact\* would the loss or accidental disclosure of the outputs have on the data subject(s) or the College?

\* *Consider all types of impact (e.g. social, financial, and/or reputational)*

Measures that can be employed to address risk may include (but are not limited to):

* Ensuring data subjects are fully aware of the data processing and its implications to them
* Ensuring data subjects can exercise their rights
* Delivering staff training to help minimise risk
* Checking that you have identified the purpose and conditions for processing
* Incorporating suitable technical measures to eliminate (or at least reduce) risk. Some examples include:
	+ Limiting access to personal data (either through physical or digital security)
	+ Ensuing new software allows you to amend, anonymise or delete data as necessary
* Incorporating suitable organisational measures to eliminate (or at least reduce) risk. For example:
	+ Being clear in business processes of appropriate delegated authority and channels of escalation
	+ Amending privacy notices as necessary
	+ Updating security measures, including reporting procedures
* Identifying the minimum amount of personal data that could be used in the project without compromising its purpose

The risk matrix below has been provided to assist you to record the details of each risk, and your plans to address them. You should consult your College Data Protection Lead (CDPL) to ensure you identify all personal data risks and consider appropriate measures.

A guide to the main definitions appears below the matrix.

**Personal Data Risk Matrix** (See guidance below for definitions)

Add as many rows as necessary to record ALL identified risks to rights and freedoms of data subjects. The first three entries are examples.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **What are the potential risks to the individuals whose personal data you hold?** | **What is the origin/source of the risk?** | **Likelihood of this happening**1 Very Unlikely2 Unlikely3 Possible4 Likely5 Very Likely | **Impact**1 Negligible2 Minor3 Moderate4 Major5 Catastrophic | **Overall risk score**(Likelihood xImpact = Score)1-3 Low4-6 Moderate8-12 High15-25 Extreme | **Risk will be**Eliminated,Reduced, orAccepted | **Mitigating action to eliminate or reduce risk****OR****Justification if accepting risk\***\* If risk is accepted, skip next column | **How will action reduce or eliminate the risk?** | **Expected completion date** | **Responsible****owner** |
| 1 | Duplicate sets of same data held in two departments | Copies of same data stored locally rather than shared (and updated) centrally | 2 | 2 | 4 (Moderate) | Reduced | Project team will put a data cleansing and validation procedure in place | Eliminates duplicates and results in one master list of accurate data | 01/09/2019 | Project team |
| 2 | Inadequate data sharing agreements (DSAs) in place | DSAs are reviewed locally and not checked against data protection requirements | 2 | 3 | 6 (Moderate) | Eliminated | All new DSAs to be reviewed by the Senior Information Risk Owner (SIRO) and College Data Protection Lead (CDPL) with involvement of the College’s DPO as needed and, where necessary, signed off by lawyers | Ensures terms of DSA are legally robust and fit for purpose | As required | SIRO and CDPL |
| 3 | Difficulty fulfilling subject access requests due to mixture of business and personal emails | Staff using work emails for personal reasons | 4 | 2 | 8 (High) | Accepted | College has re-issued its email policy to all staff, asking them to sign and return a confirmation that they have read and understood it. It will speak to individuals as issues come to light, but systematic monitoring of staff adherence is not possible within existing resources | N/A | Email Policy circulated 01/05/2019 | SIRO, CDPL and HR |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

**Guidance for Definitions**

|  |  |
| --- | --- |
|  |   |
|  |  |

***Section E: Evaluation and consultation***

Using the information in this DPIA, you should be able to determine whether the proposed personal data processing is necessary and proportionate in relation to the purpose(s) of the project/programme. Once you are confident that all possible impact on individuals has been considered and addressed appropriately, you should sign the section below and send the completed form to your College Data Protection Lead (CDPL).

If you consulted data subjects, data processors, or the Information Commissioner’s Office (ICO), please provide a summary below:

This DPIA is a dynamic document and must be reviewed regularly throughout the project lifecycle or change programme. In particular, you should update the risk matrix to reflect progress on addressing existing risks as well as recording new ones that you have identified since the last review. You may find it easier to incorporate the risk matrix into your project’s overall risk assessment.

The DPO recommends that DPIAs be reviewed **three years** after the completion or delivery of each project/programme. It should occur sooner if:

* the risk profile of the processing changes,
* there is substantial change to any aspect of the processing
* the organisational or societal circumstances relating to the processing change significantly

You must send a copy of each updated version to your CDPL for signing off. They will send a copy of the updated DPIA to the DPO as well.

**DPIA completed by:**

**Signed**: **Date:**

**Name:**

**Date of next review:**

***Section F: Data Protection Officer Notification/Consultation***

**Notification date:**

**Date(s) and summary of any discussions with DPO:**

***Section G: College Data Protection Lead (CDPL) Approval***

**DPIA approved, including sign-off of risks and appropriate mitigation measures**

**Signed**: **Date:**

**Name:**

**Role (if not CDPL):**