DATA PRIVACY IMPACT ASSESSMENT (DPIA)

Contents

NOTE:

This template is provided as an example of the key types of information that can be considered during the DPIA process. If you think it needs adjustment, please let the Data Protection Team know on data-protection@ucl.ac.uk

1. Project summary and requirement for DPIA

Describe the project and what it intends to achieve by addressing the following key points:

- Describe the project as a whole
- Summarise why a DPIA was required
- (Check answers to E. PRIVACY IMPACT SCREENING QUESTIONS in your Research Registration Form)
- What are you trying to achieve with this project?
- Is the project a one-off initiative or part of a bigger, ongoing research project?
- Describe what the DPIA covers and what it doesn't cover, e.g. what parts of the organisation, project, systems, or IT infrastructure are included

2. Flows of personal data

- Identify and describe the type of personal information involved and what is happening with it.
- You should include the collection, use and deletion of personal data here.
- Refer to an information flow diagram or another way of explaining data flows if necessary.

> "Personal data" is any information that is capable of identifying a living human being. It doesn't have to be particularly sensitive or negative information.
>
> However, the level of sensitivity and the level of impact on individuals will affect whether your information handling is likely to breach the law, or whether there are other privacy risks that need to be mitigated.

Describe both the **current** and **future** information flows so that the differences are visible at a glance.

Show, for example:

i. what personal data is collected and used, and how it flows through the system

ii. how the project will change the information flow

iii. all changes to personal data involved in the project – for instance:

- Is new personal data being collected? Where is it coming from?
- Will information that the organisation already holds be used for a new purpose? Why and how?
- What is the nature of the personal data collected and the source?
- What measures are in place to ensure the personal data is accurate and up to

date?

- Will you tell the individuals what's happening to their personal data? How will it tell them?
- How is personal data managed, handled or protected?
- Who will have access to the personal data (whether inside or outside the organisation)?
- How long will the personal data be retained and how will it be disposed of?

3. DPIA TABLE: assessing the privacy impact on individuals and compliance with data protection legislation

This section lets the decision-makers see at a glance whether the policy or proposal will comply with data protection legislation.

Each row in the following table summarises the key requirements of the data protection principles and outlines some key questions or considerations you should address. A risk assessment table can help you identify the privacy risks relevant to your initiative.

The accompanying Risk mitigation table (see 4 below) provides a more detailed explanation of how the project fits with the privacy principles. Either cut and paste from the Risk and Mitigation Table into this section of the DPIA Report (and then omit those details from the "Risk assessment" section of this report, to save repetition), or provide a brief overview here and then expand on it in the "Risk assessment" section

DPIA TABLE

Ref no.	Description of data protection principle *(delete if not relevant to your project – but at least consider each principle)*	Summary of personal information involved, use and process to manage	Assessment of compliance risk	Assessment of privacy risk
	Principle 1(a) - Personal data shall be processed lawfully, fairly and in a transparent manner *(lawfulness, fairness and transparency)*	*Have you got the consent of participants?* *Have participants been provided with a research information sheet or privacy notice?* *If so, is everything you intend to do on the research information sheet so participants are fully informed?* *Is your method of collection fair and appropriate in the circumstances?* *Would anything be beyond individuals' reasonable expectations?* *Is collection proportionate to the aims of the project?*	*Note for each principle whether the project complies or risks being non-compliant.* *Risk should be categorised as 'low', 'medium' or 'high'*	*Assess the privacy risks to individuals here.* *Consider:* *- the nature of the personal data, e.g. is sensitive personal data involved?* *- could processing likely to be intrusive?* *- could processing have a detrimental effect on individuals?* *Risk should be categorised as 'low', 'medium' or 'high'*

DPIA TABLE

Ref no.	Description of data protection principle *(delete if not relevant to your project – but at least consider each principle)*	Summary of personal information involved, use and process to manage	Assessment of compliance risk	Assessment of privacy risk
	Principle 1(b) – collected for specified, explicit and legitimate purposes *('purpose limitation')*	*Identify each element of personal information and satisfy yourself that it is necessary for the project. Consider:* *- What is the purpose of collecting the personal information involved here? Is it 'necessary'?* *- How will that enable your project to do what it needs to do?* *- Are you only collecting what you actually need? For example, do you really need "date of birth", or will "age" or "over 18" be enough?*		
	Principle 1(c) – adequate, relevant and limited to what is necessary *('data minimisation')*	*Be clear about the purpose for having and using the information.* *Is this what the individual will expect?* *Are you using it for a different purpose from the one for which you collected it? If so, is there an exception justifying this use?*		

DPIA TABLE

Ref no.	Description of data protection principle *(delete if not relevant to your project – but at least consider each principle)*	Summary of personal information involved, use and process to manage	Assessment of compliance risk	Assessment of privacy risk
	Principle 1(d) – accurate and kept up to date *('accuracy')*	*This section should consider how the organisation will deal with a request for personal information to be corrected or for a statement of correction to be attached*		
	Principle 1(e) - kept for no longer than is necessary *('storage limitation');*	*How long are you proposing to keep the information for?* *Are there any obligations to hold the information for a specific period, such as under legislation or from a research funder?* *Have you considered UCL's retention schedule? (https://www.ucl.ac.uk/library/docs/retention-schedule.pdf)* *If no such obligations exist, what would be considered to be a reasonable length of time to hold the information?* *Can you store it in a form that no longer identifies the participant, e.g. pseudonymised data* *How will you dispose of it?*		

DPIA TABLE

Ref no.	Description of data protection principle *(delete if not relevant to your project – but at least consider each principle)*	Summary of personal information involved, use and process to manage	Assessment of compliance risk	Assessment of privacy risk
	Principle 1(f) – Security of personal data *('integrity and confidentiality')*	*Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.* *There will be a number of methods to help you safeguard the personal data you hold, such as policies and codes of conduct, through to physical or technical controls that protect the information. It is useful to refer directly to any documents or information that are available to support this.* *Safeguards may include: physical security; IT security; staff training; policies that staff have to observe; confidentiality clauses in contracts with external providers etc.* *Consider whether there are vulnerabilities in each part of the information pathway – identify any weak links*		

DPIA TABLE

Ref no.	Description of data protection principle *(delete if not relevant to your project – but at least consider each principle)*	Summary of personal information involved, use and process to manage	Assessment of compliance risk	Assessment of privacy risk
	Principle 2 – demonstrate compliance with Principles 1(a)-(f) *('accountability')*	*So that you can demonstrate you have taken the necessary steps to protect privacy keep sufficient records relating to your project including:* *- this PIA* *- any fair processing or privacy notices* *- the research information sheet* *- specific security protocols you are using*		
	Articles 44-9 - transfers of personal data outside the UK	*Are you transferring personal data outside the UK?* *If so, follow UCL guidance for storing or transferring personal data outside of the UK* *http://www.ucl.ac.uk/legal-services/guidance/dp-data-transfer*		

4. Risk mitigation

This section describes the privacy risks you've identified through the DPIA process and how you propose to mitigate and manage those risks. It can be useful to link this back to the privacy principles to show why these risks and the proposed actions are relevant.

Note: A DPIA doesn't set out to identify and eliminate every possible privacy risk: its role is to identify genuine risks that are not unreasonably small or remote.

Risk mitigation						
Ref. no.	Description of the risk	Rationale and consequences: i. for the individual (if a privacy risk) ii. for UCL (if a compliance risk)	Existing controls that contribute to manage risks identified	Assessment of residual current risk	Recommended mitigations or privacy enhancements	Residual risk remaining despite new safeguards
	Describe any privacy or compliance risk identified in the PIA table above	*Explain the potential adverse impact on individuals*	*Systems and safeguards currently in place that act to minimise these identified risks, e.g. specific training, encryption of data, pseudonymisation or anonymization of data*	*Assess the likelihood of the risk happening (high, medium or low) and how severe the harm would be with no new protections (serious to minimal)*	*Include recommendations for how these residual risks can be removed, managed, or mitigated, or further privacy safeguards to ensure the individual is protected*	*Detail any remaining vulnerabilities in the design that need to be managed.* *Note risk level (high, medium or low) and the likely severity of harm without any new safeguards.*

5. Action plan, review and integration of DPIA outcomes into project plan

This section of the report should describe what actions are being taken (whether short or long term) and how they'll be monitored.

Reporting on the outcome of the mitigation may be necessary. If the DPIA is being performed as part of a project, then the project is likely to require some reporting on the implementation as part of governance arrangements. Once the project is completed, any on-going privacy monitoring should be incorporated into normal business operations.

In the case of a particularly long or complex programme of work, the DPIA may need to be reviewed a number of times to ensure that it continues to be relevant. This section should describe how this will be achieved.