UCL DATA IMPACT ASSESSMENT TEMPLATE FOR RESEARCH

Why do I need to complete this Data Protection Impact Assessment (DPIA)?

A DPIA helps identify data privacy risks when planning new, or revising existing, projects and to identify actions to mitigate these risks. In the rare cases where risks cannot be mitigated at all it may be necessary to consult with the Information Commissioner's Office (ICO). Under data protection legislation it is a legal requirement to complete a DPIA in the following circumstances:

- where data processing is likely to result in a high risk of harm to individuals, e.g. new, invasive technology is proposed
- when large volumes of personal data are processed, e.g. use of behavioural profiles based on website usage
- when processing special category personal data on a large scale, e.g. genetic tests to assess and predict the disease/health risks
- when individuals are evaluated based on automated processing or profiling, e.g. credit screening
- where publicly accessible areas are monitored, e.g. CCTV or when filming public areas

It is UCL policy to carry out a DPIA in the following circumstances:

- Where datasets have been matched or combined for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the individuals concerned.
- Where the personal data concerns vulnerable individuals, e.g. children, vulnerable adults, or where there is an imbalance of power.
- When applying innovative use or applying technological solutions, e.g. 'internet of things' applications.
- When data is transferred outside the European Union.

In circumstances in which it is unclear whether a DPIA is required under data protection legislation, it is advisable to carry one out as a useful tool to ensure any privacy risks to individuals are considered. Failing to carry out a DPIA correctly or failing to consult the ICO where required can each result in fines.

When should I complete this DPIA?

The DPIA should be started as early as possible during project planning while there is still time to influence project design. The DPIA should be completed prior to any contractual negotiations and before the processing of personal data begins.

Who should complete this DPIA?

While the controller (i.e. UCL) is responsible for ensuring that DPIAs are carried out, the Principal Investigator should complete this DPIA, and then submit it to Data Protection Office as part of their research registration forms. Relevant stakeholders, such as partners, colleagues and participants, should be consulted throughout the DPIA process to assist in identifying privacy risks where necessary.

How should a DPIA be completed?

This table sets out the steps UCL should take to comply with data protection legislation when carrying out a DPIA prior to processing personal data. It is important to note that the size and level of detail in a DPIA should be proportionate to the scale of the project and the related privacy risk. Account should be taken of the nature, scope, context and purpose of the data processing.

UCL DATA IMPACT ASSESSMENT TEMPLATE FOR RESEARCH

Step 1 – DPIA team			
	Name	Job Title	Email Address (as contact point for future privacy concerns)
Principal Investigator owning DPIA			
Third Part(y/ies) assisting with DPIA (if any)			
Step 2 – Research summary			
Project Name			
Department /entity			
Date			
Step 3 – Identify the need for a DPIA			
Describe the purpose/aims of the research. In your description set out the benefits to: i. UCL ii. individuals iii. the wider public			
Please explain: - the role of personal data in the project; - the risks to privacy there are in your project (please list), and - why the processing of personal data is necessary and proportional for the purposes of your project.			
Step 4 - Please describe the information flows. If this is described in another document, please attach it to this DPIA			
Information Flows: means the collection, retention, use, transfer and deletion – i.e. all types of data processing as part of the project's lifecycle - of personal data should be described here. 'Transfers' would include emails between the team members. If information is sent outside the EU/EEA, you should state that here. It would also be helpful to produce and refer to a flow diagram or another way of explaining data flows.			

UCL DATA IMPACT ASSESSMENT TEMPLATE FOR RESEARCH

Step 5 – What steps or controls are you taking to minimise risks to privacy?

Please tick

a. Risks to individual privacy are minimal	☐	j. Special category personal data is not used	☐
b. Personal data is pseudonymised	☐	k. Randomisation	☐
c. Encryption of data at rest, i.e. when stored	☐	l. Participant opt out at any stage of the research	☐
d. Encryption used in transfers	☐		
e. Total number of participants is less than 50	☐	m. Personal data kept in the EEA	☐
f. Information compliance training for staff has been completed - data protection, information security, FOI	☐	n. Research is not used to make decisions directly affecting individuals	☐
		o. De-identification	☐
g. Hashing or salting employed	☐	p. Short retention limits	☐
h. Adherence to privacy by design principles	☐	q. Restricted access controls	☐
i. Probalistic risk management	☐	r. Other (please specify)	

Step 6 – What steps have you taken to make sure the research is as accurate as possible and there are minimal unintended consequences? Please tick

a. data management plan in place	☐	d. this study builds on a pilot study	☐
b. data management plan is peer reviewed	☐	e. an extension to a previous similar	☐
c. PI experience levels - no experience;	☐	study registered by DPO,	☐
some experience;	☐	if there is, please provide the number	☐
very experienced	☐		

Step 7 – How have you assessed what participants will think of the research? What have you done to address concerns raised? Please tick

a. pilot project	b. use of focus group	c. information sheet/consent form	d. experience drawn from previous study
☐	☐	☐	☐

Step 8 – For the controls/steps specified in Step 5, who will make sure the controls are put in place? Please tick

a. PI	b. Head of School	c. other body (please specify)
☐	☐	