UCL Data Protection Impact Assessment:

Guidance Professional Services

version 3 – November 2020

Step 1 DPIA Team – complete the boxes.

Step 2 Project Summary – complete the boxes.

Step 3 Identify the need for a DPIA – complete the boxes.

Step 4 Describe the personal data flows, envisaged processing operations and the overall purposes.

The collection, retention, use, transfer and deletion (all data processing) of personal data should be described here.
It would also be helpful to produce and refer to a flow diagram (see appendix 1 as an example) or another way of explaining data flows.

Ensure that you provide details on the following:

- Data controller and any processors
- Nature, scope, context, purpose(s) of processing
- What data are processed
- How data are collected, stored, processed and destroyed (identify assets human, technical…)
- Any other recipients of data

In addition to the above, please identify any of the following:

- High risk of harm to individuals’ rights?
- Systematic evaluation of data based on automated processing (e.g. profiling)?
- Large scale processing of sensitive information (e.g. data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, data concerning health, sex life or sexual orientation,) or data relating to criminal convictions and offences?
- Large scale surveillance of public areas?

Step 5 Assess project against the key Data Protection

Principles (i) Lawfulness, fairness and transparency

What categories of personal data are being collected and are any special categories of data being collected (e.g. data revealing racial or ethnic origin, political opinions, religious beliefs, trade-union membership, health, or sexual orientation)?

- Where do you obtain the personal data from?
- What information about the processing is provided to the individual? Please provide a copy of any privacy notice.
- How will you make the processing lawful (pick one):
  - consent? Please provide a copy of the consent language (note that consent must be freely given, specific, informed and unambiguous) and a description of how it will be recorded. Consent cannot be a condition of providing a service, and so will typically require to be dealt with separately from the terms and conditions/privacy policy

- contract performance to collect and process the data?
- compliance with a legal requirement to collect and process the data? Please explain
- necessary for the performance of a task carried out in the public interest
- legitimate interests to collect and process the data? Please describe why this condition is applicable and UCL's interests and set out why there is no unwarranted prejudice to the rights and freedoms of the data subject.

(ii) Purpose limitation

- For what purposes do you wish to use the personal data collected?
- How will you notify individuals of these purposes?
- How will you ensure the data are not further processed for incompatible purposes?

(iii) Data minimisation

- Are all the personal data collected necessary for the purposes for which they are processed?
- Is your processing of personal proportional to the purposes you want to achieve?
- What steps are you taking to ensure you only collect the minimum personal data you need for the purposes of this project?

(iv) Accuracy

- If you are procuring new software does it allow you to amend and update the data where necessary?
- How will you ensure that the personal data collected are accurate e.g. use of reliable sources?
- How will you verify the accuracy of the data, and how often? How will you erase or correct personal data promptly, if there are errors?

(v) Storage limitation

- What retention periods are suitable for the personal data you are collecting?
- If you plan to anonymise data, so that individuals can no longer be identified, please explain how you will do this, and when.

(vi) Rights of individuals

- Will the project systems allow you easily to provide, amend or delete information on request, or restrict the processing of the information?
- Where processing is based on consent or contract necessity, and automated, will the project systems allow you easily to provide personal data to an individual?
- Where processing is based on consent, will the project systems enable the individual to withdraw that consent as easily as it was given?
- Will any decisions that affect individuals be made solely on the basis of processing by automatic means? If so, will the project systems allow the individual to object to any processing?
- If this is a marketing project, can individuals opt-out of their information being used for a purpose (e.g. for profiling in the course of targeted advertising)?

(vii) Security, integrity and confidentiality

What technical security measures will be in place eg:

- encryption, firewalls, logical access control, traceability, monitoring (including of configurations)
- Anonymisation, encryption, data partitioning
- Integrity checks, backups, workstation management, malware
- Secure communications

What physical measures, eg:

- *Location, protection from non-human risk sources (fire, water,…)*
- *physical access control*
- *security of hardware and paper, both stored and in transmission*

Organisational, eg:

- *Policy, risk management, project management,*
- *Staff management, third parties, maintenance*
- *Document marking, archiving*
- *Supervision*
- *Training*
- *Incident management*
- *Audits, logs*

(viii) International transfer

- Will personal data be transferred outside the EU?
- If so, what adequate safeguards will be put in place e.g. EU model clauses?
- Has the party to whom the data is being transferred been subject to a due diligence exercise to determine their security and handling of personal data to ensure compliance with UCL's standards and the Data Protection Laws?

In July 2020 The Court of Justice of the European Union (CJEU) passed a judgement with wide ranging implications for international transfers of personal data. The judgement invalidated the EU-US Privacy Shield (a mechanism to enable data transfer to the US) though the wider impact is that all international transfers should be individually risk-assessed and measures put in place to ensure that EU standards of data protection travel with the data when it goes overseas.
These measures normally take the form of Standard Contractual Clauses (SCCs). However, the judgement also suggests that even SCCs would be insufficient for data transfers to US companies that are covered by US security legislation that allows agencies to access that data.
This results in considerable complexity when assessing international transfers as part of the DPIA process. Below are some key considerations to help with this assessment:

Consideration	**Detail and potential mitigation options**
Is the data being transferred to the US?	As set out above, all data transfers to the US now carry some risk. It is important to ensure that appropriate technical measures are in place to protect the data, such as encryption.
Will SCCs be put in place to cover the data transfer in questions?	It is strongly recommended that SCCs are in place for all international data transfers although they do not eradicate all risk as outlined above.
Does the data transfer require a new contract?	Continuation of existing contracts is considered a lower risk while we await further guidance on the impact of the CJEU judgment.

What awareness will the data subject have of the specific data transfer?	Depending on the legal basis used for the transfer (e.g. consent vs legitimate interests) and the process by which the data was captured, different levels of awareness can be anticipated. Greater awareness could mean a lower risk that a data subject may object to the transfer.
What benefits does the data subject get from the processing that involves the data transfer?	A free service providing significant benefits to the data subject may have less risk of complaint than a data transfer that is done purely for UCL's benefit.
What personal data is included in the transfer?	Transfer of special category data may carry greater risk.
Is the processing/transfer in an area that has seen ICO enforcement?	The ICO follow a risk-based enforcement policy. Their assessment of risk can be inferred from historic enforcement activity. In particular you should consult the DPO if your proposed processing activities involve international transfer in relation to unsolicited marketing, data scraping or includes information that might be of interest to intelligence services.
Is the data transfer unique to UCL or part of common service?	Data transfers deriving from use of popular/widespread services may carry less risk that a complaint would be made to UCL specifically.
Does the processing / data transfer help adherence to other data protection requirements?	For example, a project to standardise UCL activity with one selected supplier would carry considerable benefits for data accuracy, data minimisation, purpose limitation etc. These benefits may partially mitigate the risks associated with a transfer.
Does the third party demonstrate a decent level of GDPR compliance?	For example, do they still rely on the Privacy Shield, do they explain how they comply with the GDPR?

If you do not believe you can mitigate the risk, this matter must be escalated to the Data Protection Officer

(ix) Data processors

- Will any third-party process UCL's data? If so, what reasonable steps has UCL taken to ensure that any third party handling personal data complies with data protection requirements?
- How did you assess their data security measures? How do you ensure that they comply with these measures?
- Does the contract in place with the third-party vendor contain suitable data processor obligations in line with the requirements of Data Protection Laws?
- Do you have clear audit/governance measures to monitor the third-party's on-going compliance?

(x) Local laws and regulations

Has confirmation been obtained from the relevant local market lawyers that this project complies with local laws and regulations in the countries in which data is being collected and processed?

Step 6

(i) Identify and rate the privacy risks of the project based on your answers in Step 3 (if applicable) and Step 5 using ‘low/medium/high’.

(ii) Rate the likelihood of privacy risk materialising using ‘remote/possible/likely’.

(iii) Identify solutions to the privacy risks.

Step 7 Evaluation

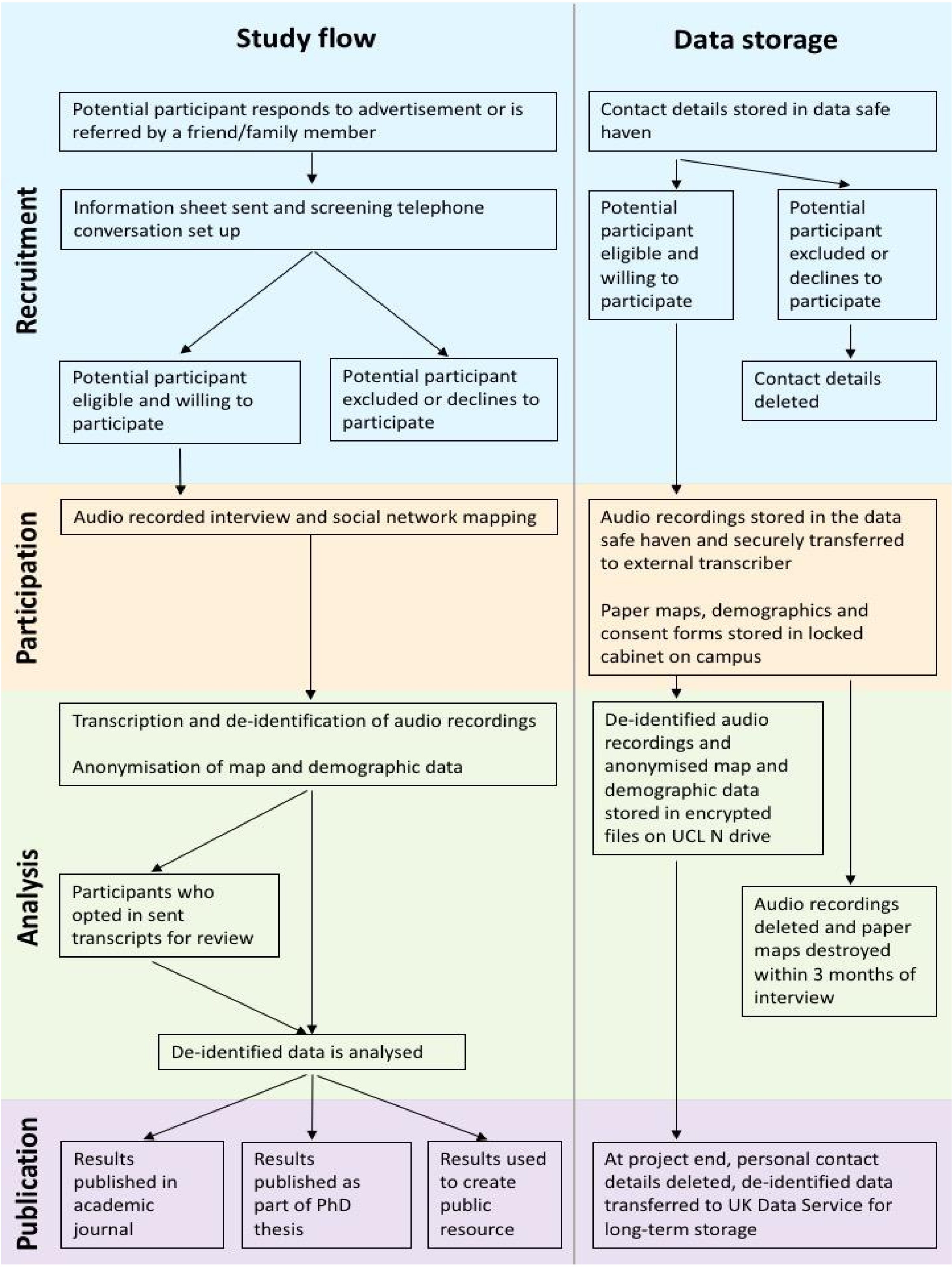
Simply answer the question. If the answer is ‘no’, please contact data-protection@ucl.ac.uk

Step 8 List any issues with integrating the DPIA outcomes back into the project plan

Set out any problems or challenges with incorporating the DPIA outcomes of Step 6 into your project plan.

Step 9 Approval of DPIA, including risks and solutions identified – complete the box.

Appendix 1 – example of data flow diagram


Study flow
Data storage
Recruitment
Potential participant responds to advertisement or is referred by a friend/family member
Information sheet sent and screening telephone conversation set up
Potential participant eligible and willing to participate
Potential participant excluded or declines to participate
Contact details stored in data safe haven
Potential participant eligible and willing to participate
Potential participant excluded or declines to participate
Contact details deleted
Participation
Audio recorded interview and social network mapping
Audio recordings stored in the data safe haven and securely transferred to external transcriber
Paper maps, demographics and consent forms stored in locked cabinet on campus
Analysis
Transcription and de-identification of audio recordings
Anonymisation of map and demographic data
Participants who opted in sent transcripts for review
De-identified data is analysed
De-identified audio recordings and anonymised map and demographic data stored in encrypted files on UCL N drive
Audio recordings deleted and paper maps destroyed within 3 months of interview
Publication
Results published in academic journal
Results published as part of PhD thesis
Results used to create public resource
At project end, personal contact details deleted, de-identified data transferred to UK Data Service for long-term storage