

# UCL Data Protection Impact Assessment:

## Guidance Professional Services

version 2 - August 2018

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 data 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?

(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](mailto: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

