Guidance on the requirement for data protection (privacy) by design and default

A. Introduction

This document provides guidance to staff and students on the requirements imposed by data protection legislation in respect of 'data protection by design and default' (often referred to as 'privacy by design and default').

It aims to help you to meet the obligation to ensure that data protection requirements are built into the design and implementation of any new technologies or processes that involve the 'processing' (e.g. the collection, storage and use) of personal data.[1]

B. Scope

This guidance applies to all staff and students who are processing personal data as part of their work or studies at UCL.

C. What does 'data protection by design and default' mean?

(a) Data protection by design

'Data protection by design' means ensuring that data protection is integrated into UCL's systems and processes, from the design phase of a project or activity until the very end of its lifecycle. Under data protection legislation, UCL must, both at the design/planning phase and for the duration of the processing:

- Implement appropriate technical and organisational measures (e.g. pseudonymisation) designed to apply fundamental data protection principles;[2] and

[1] Please see the Appendix to this document for the full definitions of 'personal data' and 'processing'.

[2] Please see the Appendix to this document for further detail on the data protection principles.

- Integrate necessary safeguards into our processing activities in order to meet our obligations under data protection legislation and to protect the rights of individuals whose personal data is processed.

When considering how to meet this obligation, UCL must take into account factors such as:

- The current 'state of the art';
- The cost of implementing relevant measures;
- How and why the personal data is processed; and
- The risks posed to individuals' rights as a result of the processing.

(b) Data protection by default

This means that, by default, only the personal data that is strictly necessary for each specific purpose of the processing must be collected, stored and used.

Data protection legislation requires UCL to implement appropriate technical and organisational measures to ensure that, by default, UCL:

- Only collects and use personal data to the extent necessary for the stated purposes;
- Does not store that personal data for longer than is necessary for those stated purposes; and
- Does not, by default, make personal data accessible (without the individual's intervention) to an indefinite number of other individuals.

D. What practical steps are you required to take?

The Information Commissioner's Office (ICO), the UK data protection regulator, advises that there is no 'one size fits all' solution that will work in all situations. The most appropriate method to use or

measures to put in place in order to help ensure data protection by design and default will depend on the circumstances. Nevertheless, we recommend taking the following general approach:

- Consider data protection issues as part of the design and implementation of systems, services, products and business practices involving the processing of personal data. In practice this means that privacy issues should be considered from the start in relation to new systems and projects and also incorporated into the design of changes to existing ones;

- Make data protection an essential component of the processing systems and services. In particular, you should ensure that 'data minimisation' and privacy-friendly default settings, along with other relevant measures set out in this list, are part of their core functionality;

- Try to anticipate events that may pose a threat to individuals' privacy before they occur, and take steps to prevent harm to individuals. For example, if personal data will be transferred to a third party outside the EEA, ensure that appropriate safeguards (e.g. the model contract clauses) are put in place. Please see here for further guidance on overseas transfers of personal data;

- Minimise the processing of personal data where possible. This means that you should only collect the personal data that is necessary for the stated purposes(s), and only use the data for those purposes, and you should not process additional data unless the individual decides you can. Personal data should be pseudonymised or anonymised as soon as possible, where appropriate;

- Ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals do not have to take any specific action to protect their privacy. You should put in place robust access controls to avoid unauthorised or unfair disclosures and encrypt personal data where possible. You should also keep security features under regular review and improve them on an ongoing basis;

- To help comply with UCL's transparency obligations under data protection legislation, inform individuals at the time their personal data is collected about how and why that data will be processed. You should use plain English for privacy notices and any other information provided to individuals so that individuals easily understand what how and why their personal

data will be used, and provide the identity and contact information of those responsible for data protection at UCL. Please see here for further guidance on preparing privacy notices;

- Where appropriate, provide individuals with tools so they can determine how their personal data is being used, and whether UCL's policies are being properly enforced. For example, if individuals are able to login and upload personal data to a particular system, you should ensure that they can check their privacy settings and include easily accessible links to UCL's relevant privacy notices, policies and procedures;

- Offer strong privacy default settings, user-friendly options and controls, and respect user preferences about privacy and how their personal data is treated. You should ensure that individuals are not given an 'illusory choice' as to how their personal data will be processed and provide options enabling them to exercise their rights under data protection legislation, such as the right to access, erasure, rectification, etc.;

- Only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design. Please note that if a third party processor is engaged, you will need to ensure that a contract incorporating all of the elements required under data protection legislation is entered into. Please contact the data protection team using the contact details set out at Section G below for further guidance on this issue;

- When you use third party systems, services or products in your processing activities, make sure that you only use those whose designers and manufacturers take data protection issues into account. This means that you will need to carry out appropriate due diligence on third party suppliers and other business partners/organisations with which UCL collaborates in any context; and

- Consider whether any specific technologies (e.g. software or hardware) may be used to help you meet the above data protection by design obligations.

E. Will the 'data protection by design and default' obligations apply to my project?

The above obligations relating to data protection by design and default will apply to **all** projects and activities carried out by UCL staff members and/or students where personal data is processed.

Nevertheless, examples of personal data processing activities where privacy by design and default issues may be of particular concern include the following (please note that this is not an exhaustive list):

- Use of systems or software that involve the storage of personal data overseas e.g. a cloud storage solution based in the USA;

- Design of systems, software or processes that monitor or profile individuals based on their personal data e.g. attendance monitoring, CCTV systems, wealth screening activities or learner analytics;

- Development of new organisational policies, services, products and processes that involve processing personal data;

- Use of personal data already held by UCL for new or novel processing activities e.g. research involving the use of apps, artificial intelligence or the use of existing personal data in other ways it is not already used; or

- New data sharing initiatives between UCL and another organisation, e.g. a collaboration between UCL and another university over a survey for research purposes.

F. Data Protection Impact Assessments (DPIAs)

Where the processing is considered 'high risk', e.g. because it involves significant volumes of personal data and/or special category personal data, a Data Protection Impact Assessment (DPIA) will need to be completed as part of the 'privacy by design and default' approach. Please see here for further guidance on DPIAs at UCL.

G. Questions and further information

If you require any further information or would like to discuss the issues raised in this document, please contact the data protection team at data-protection@ucl.ac.uk.

Appendix: Definitions and Data Protection Principles

(a) Definitions

Data protection legislation: the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA).

Personal data: any information relating to an identified or identifiable living individual. The definition of personal data in law is broad and covers direct identifiers (like a person's name) and indirect identifiers (like a full postcode). An **identifiable individual** is one who can be identified:

> *'…directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'*
>
> [GDPR, Article 4]

Processing:

> *'…any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'*
>
> [GDPR, Article 4]

(b) ***Data Protection Principles***

Principle	**Personal Data shall be:**
Lawfulness, fairness and transparency	Processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Accurate and, where necessary, kept up to date.
Storage limitation	Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
Integrity and confidentiality	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

In accordance with the additional 'Accountability' principle, UCL must also be able to demonstrate compliance with each of the above principles.