Data Protection Policy

1. Purpose and scope

1.1. The purpose of this policy is to ensure compliance with the General Data Protection Regulation (GDPR) and related EU and national legislation ('data protection law'[1]). Data protection law applies to the storing or handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects').

1.2. This policy applies to Cambridge Enterprise Ltd ('CE'), as a single organisation ('data controller').

1.3. This policy applies to all staff except when acting in a private capacity. In this policy, the term 'staff' means anyone working in any context within Cambridge Enterprise at whatever level or grade and whether permanent, fixed term or temporary, including but not limited to employees, workers, trainees, interns, seconded staff, agency staff, agents, volunteers, and external members of committees.

1.4. This policy is not, and should not be confused with, a privacy notice[2] (a statement informing data subjects how their personal data is used by CE).

1.5. This policy should be read in conjunction with the obligations in the following documents, which supplement this policy where applicable:

1.5.1. staff employment contracts and comparable documents (e.g. worker agreements), which impose confidentiality obligations in respect of information held by CE;

1.5.2. information security policies, procedures and terms and conditions, which concern the confidentiality, integrity and availability of CE information, and which include rules about acceptable use, breach reporting, IT monitoring, and the use of personal mobile devices[3];

---

[1] See http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[2] For which see https://www. [add link here to CE website places] and other notices (including those on related webpages).

[3] See https://www.uis.cam.ac.uk/about-us/governance/uis-policies-and-guidelines and related webpages as CE is a service user of the University Information Services.

1.5.3. The University's records management policies and guidance, which govern the appropriate retention and destruction of CE information[4];

1.5.4. any other contractual obligations on CE or individual staff which impose confidentiality or data management obligations in respect of information held by CE, which may at times exceed the obligations of this and/or other policies in specific ways.

1.5.5. the Data Protection Policy of the University of Cambridge; as a wholly owned subsidiary of the University of Cambridge, CE staff will use specific services and facilities offered by the University.

2. Policy statement

2.1. CE is committed to complying with data protection law as part of everyday working practices.

2.2. All data collected and/or stored by CE is done so for the sole purposes of CE's service provision or business (including its legitimate interests), and an individual's relationship with CE. CE tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing, in its privacy notices. It will not process personal data of individuals for other reasons. Where CE relies on its legitimate interests as the basis for processing data, it carries out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

2.3. Where CE processes special categories of personal data[5] to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

2.4. Complying with data protection law may be summarised as but is not limited to:

2.4.1. understanding, and applying as necessary, the data protection principles when processing personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

[4] See https://www.information-compliance.admin.cam.ac.uk/records-management and [Insert a link to the new CE Retention Guidelines]

[5] See Appendix One for definition

2.4.2. understanding, and fulfilling as necessary, the rights given to data subjects under data protection law: to be informed; access; rectification; erasure; restriction; data portability; and objection (including in relation to automated decision-making).;

2.4.3. understanding, and implementing as necessary, CE's accountability obligations under data protection law, including implementing appropriate data protection policies;

2.4.4. implementing data protection by design and default in projects, procurement and systems;

2.4.5. using appropriate contracts with third party data controllers and data processors;

2.4.6. holding relevant records about personal data processing; implementing appropriate technical and organisational security measures to protect personal data;

2.4.7. reporting certain personal data breaches to the Information Commissioner's Office;

2.4.8. conducting Data Protection Impact Assessments where required; and

2.4.9. ensuring adequate levels of protection when transferring personal data outside the European Economic Area.

3. Roles and responsibilities

3.1. CE has a corporate responsibility as a data controller (or when acting as a joint data controller or a data processor) for:

3.1.1. complying with data protection law and holding records demonstrating this;

3.1.2. cooperating with the Information Commissioner's Office (ICO) as the UK regulator of data protection law; and

3.1.3. responding to regulatory/court action and paying administrative levies and fines issued by the ICO.

3.2. The CE Senior Management Team is responsible for:

3.2.1. reviewing (at least once every five years) and approving this policy;

3.2.2. assessing the overall risk profile and ensuring appropriate resources and processes are in place and implemented to enable compliance with data protection law.

3.3. The Deputy Director, as the named person within CE with responsibility for data protection compliance, is responsible for:

3.3.1. monitoring and auditing CE's compliance with data protection law, especially its overall risk profile, and reporting when necessary to the Senior Management Team;

3.3.2. advising on all aspects of CE's compliance with data protection law (including its use of Data Protection Impact Assessments), seeking advice from the University Information Compliance Office where necessary;

3.3.3. acting as CE's standard point of contact with the ICO with regard to data protection law, including in the case of personal data breaches;

3.3.4. acting as an available point of contact for any complaints from data subjects;

3.3.5. handling data subject rights requests;

3.3.6. publishing and maintaining core privacy notices and other CE data protection documents;

3.3.7. managing and/or handling Data Protection Impact Assessments; and

3.3.8. ensuring all CE staff are aware of this policy as necessary;

3.3.9. ensuring that appropriate processes and training are implemented to enable compliance with data protection law; and

3.3.10. ensuring that appropriate processes are implemented to enable information assets containing personal data within CE to be included in the University's Information Asset Register where appropriate.

3.4. Individual staff, in order to enable CE to comply with data protection law, are responsible for:

3.4.1. completing relevant data protection training;

3.4.2. following relevant advice, guidance and tools/methods provided to staff, regardless of whether access to and processing of personal data is through CE-owned and managed systems, University-owned and managed systems, or through their own or a third party's systems and devices;

3.4.3. when processing personal data on behalf of CE, only using it as necessary for their contractual duties and/or other CE roles and not disclosing it unnecessarily or inappropriately;

3.4.4. recognising, reporting internally, and cooperating with any remedial work arising from personal data breaches;

3.4.5. recognising, reporting internally, and cooperating with the fulfilment of data subject rights requests;

3.4.6. ensuring compliance with CE's Data Retention policy, deleting and removing data in accordance with the policy; and

3.4.7. on leaving CE ensuring that all data housekeeping requirements are fulfilled, only deleting, copying or removing personal data as agreed with their Head of Team and as appropriate.

3.5. Non-observance of the responsibilities in paragraph 3.4 may result in disciplinary action.

3.6. The roles and responsibilities in paragraphs 3.1 to 3.5 do not waive any personal liability for individual criminal offences for the wilful misuse of personal data under data protection law.[6]

4. Contact

4.1 Contact details for data protection purposes are published on our website[7].

[6] These criminal offences include: unlawfully obtaining, disclosing or retaining personal data; recklessly re-identifying de-identified personal data without the data controller's consent; deliberately altering or deleting personal data to prevent disclosure in accordance with data subject access rights; forcing a data subject to exercise their access rights; and knowingly giving false statements to the ICO.

[7] www.enterprise.cam.ac.uk [add data protection link when known]

UNIVERSITY OF CAMBRIDGE enterprise

Appendix One

Data Protection - Definitions

'Personal data' is any information that relates to a living individual who can be identified from that information, in particular by reference to:

- an identifier such as a name, an identification number, location data or an online identifier (such as an IP address); or
- factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

'Special categories of personal data' means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data. GDPR specifies that special categories of personal data should be treated with particular care due to its sensitive nature.

'Processing personal data' refers to any operations performed on personal data (whether those operations are automated or not). Common types of personal data processing include (but are not limited to) collecting, recording, organising, structuring, storing, modifying, consulting, using, publishing, combining, erasing, disseminating and destroying data.

'Data Subject' refers to a person who lives in the EU, who GDPR defines as 'identified or identifiable natural person[s]'.

'Data Controller' is a company/organisation that collects people's personal data and makes decisions about what to do with it. Data Controllers must comply with applicable data privacy legislation.