CAMBRIDGE CENTRE FOR EVIDENCE-BASED POLICING

Approved: CEO, CCEBP, 23.02.2023
Review by: 31.03.2024
Owned by: Chief Administrator, CCEBP

DATA PROTECTION POLICY

1. Introduction

This policy provides a framework for ensuring that Cambridge Centre for Evidence-Based Policing (CCEBP) complies with the Data Protection Act 2018 (DPA 18) and the UK General Data Protection Regulation (UK GDPR).

It also explains key roles and responsibilities relevant to internal compliance and how this will be monitored.

CCEBP complies with data protection legislation guided by the six data protection principles. In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner;
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;
- adequate, relevant, and limited to what is necessary;
- accurate and, where necessary, up to date;
- not kept for longer than necessary; and
- kept safe and secure.

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of our processing of their personal data. We must also be ready to produce that evidence to the Information Commissioner's Office (ICO) should this be required.

To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. CCEBP recognises that failure to so comply can result in a breach of legislation, reputational damage or financial implications due to fines.

2. Scope of policy

This policy applies to all processing of personal data carried out by CCEBP including processing carried out by joint controllers, contractors and processors. It is applicable to all staff working within CCEBP including employees, contractors and other staff or service providers.

3. Information covered by Data Protection Legislation

This paragraph will give a brief description of terms that are used in this policy (a fuller description is contained in a glossary at the end of this policy).

The UK GDPR definition of 'personal data' includes any information relating to an identified or identifiable natural living person, regardless of where they live and what they do.

A 'data subject' is any living person whose personal data is processed.

Pseudonymised personal data is covered by the legislation. Anonymised data is not regulated by the UK GDPR or DPA 18, but may also be treated as an adequate method of achieving data minimisation so long as the anonymisation is effective and irreversible.

Some personal data is more sensitive and is afforded extra protections. This is referred to as special categories of personal data (Article 9, UK GDPR) and criminal offences data (Article 10, UK GDPR). In summary, this is information related to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convictions and offences).

There are also additional protections in relation to the processing of children's personal data.

4. CCEBP's main activities in relation to personal data

As part of its day-to-day business, CCEBP is both a Data Controller and a Data Processor.

Its Data Controller responsibilities principally relate to its role as an employer, its provision of training and as a source of research material (including the Cambridge Crime Harm Index) that is utilised, most commonly, by both research students and policy makers. CCEBP collects and uses information about its customers, staff and those who work or interact with us.

Another aspect of CCEBP's work is research and project work for organisations concerned with public safety and crime prevention. In undertaking this work CCEBP is a Data Processor (or potentially a sub-processor) of personal data and works on the Data Controller's documented instructions. The principle of data minimisation is particularly important where special categories of personal data and criminal offences data is involved. This principle is typically achieved through the pseudonymisation or anonymisation of sensitive data by the Data Controller thereby

ensuring that only aggregated data (information that will not identify a living person) is transferred to CCEBP for further analysis and manipulation This often means that the personal data that CCEBP is processing is limited in terms of both its quantity and sensitivity.

It is understood by those within CCEBP as to how to fulfil their GDPR responsibilities, including breach and other reporting duties.

5. How we ensure compliance with this policy

CCEBP is committed to compliance with GDPR and other relevant legislation and regards responsible handling of personal data as a fundamental obligation and one that is pivotal to our reputation as a provider of high quality research and training. Staff at CCEBP are aware of their responsibilities and the requirement to apply this policy when processing personal data.

Our compliance is achieved through:

- **Effective project management**- with information security a central feature in how we plan, manage, review and learn from projects and other workstreams;
- **Contracts**- data processing agreements and contracts are closely managed to ensure that GDPR data minimisation principle is achieved: particularly important where special categories of personal data and criminal offences data is involved;
- **Privacy Notice**- CCEBP provides privacy information in the form of a Privacy Notice to individuals at the time we collect their personal data from them. This takes place when a person enrols for a course or to access research and archival information held by CCEBP (and is to be found at the CCEBP website home page). The Privacy Notice informs individuals of their rights under UK GDPR;
- **Data security**- the procedures and technology we have in place to maintain the security of personal data;
- **Information rights**- we have processes in place to handle subject access requests and other information rights requests;
- **Breaches**- we consider the risks of personal breach incidents within our planning, monitoring and review processes. Our staff are trained in their responsibilities and understand reporting rules and the different decision making and action depending on whether CCEBP is a Data Controller or Processor. In the event of a potential breach we will assess whether we need to report to the ICO; it is recognised that a breach of personal data that presents a likely risk to people's rights and freedoms has to be reported to the ICO within 72 hours of being made aware of the breach (by the Data Controller);
- **Training**- our staff have been trained in GDPR and receive an annual refresher input. This is augmented by regular phishing awareness exercises;
- **Communication**- we have clear systems for communication with regular briefings and de-briefings taking place. We encourage organisational learning and seek to embed a culture of privacy/ information risk recognition and management; and

- **Policies and procedures**- we produce project-specific instructions and broader policies that support our operational procedures and application of the data protection legislation, this includes a Data Retention Policy and Data Breach Response and Notification Policy.

6. Roles and responsibilities

CCEBP has systems in place to ensure that risks including information security risk are effectively managed. The roles and structure by which this is delivered includes:

- **Risk and Governance Group**- is responsible for the overview and scrutiny of information management arrangements and for making recommendations to the CCEBP Senior Information Risk Owner as to data protection and compliance issues;

- **Data Protection Officer responsibilities-** the Chief Administrator of CCEBP fulfils the responsibilities of a Data Protection Officer (there is also a designated deputy also able to fulfil DPO responsibilities). This includes monitoring internal compliance with UK GDPR, informing and advising on data protection obligations (including Data Protection Impact Assessments) and acting as a contact point for Data Subjects and the ICO;

- **Senior Information Risk Owner**- this role is performed by the Chief Executive Officer of CCEBP, who owns the overall risk arising from the processing of personal data by CCEBP.

7. Monitoring of compliance with this policy

Compliance with this policy will be monitored by the Chief Administrator and the deputy reporting to the Chief Executive Officer and the CCEBP Director.

8. Feedback or questions

Any questions about this policy or data protection queries should be addressed to: chief@cambridge-ebp.co.uk.

Glossary

Personal data: any information relating to an identifiable living individual who can be identified from that data or from that data and other data. This includes not just being identified by name but also by any other identifier such as ID number, location data or online identifier, or being singled out by any factors specific to the physical, physiological, genetic, mental, cultural or social identity of the individual.

Processing: anything that is done with personal data, including collection, storage, use, disclosure, and deletion.

Special category personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

Data Controller: the organisation (or individual) which, either alone or jointly with another organisation (or individual) decides why and how to process personal data. The Data Controller is responsible for compliance with the DPA 18 and UK GDPR.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.