



Data Protection Policy

TITLE	Data Protection Policy
SUBJECT	Sets out the way in which the CCRC handles personal information and how it complies with the Data Protection Act 1998
OWNER	Data Protection Officer
DOCUMENT & VERSION NUMBER	1943526 v1
IMPLEMENTATION DATE	October 2016
LAST REVIEW DATE	September 2016
NEXT REVIEW DATE	September 2018
RELATED POLICIES	

CCRC Data Protection Policy

Background

This document sets out the way in which the Criminal Cases Review Commission (CCRC) handles personal information and how it complies with the Data Protection Act 1998 (DPA).

The CCRC is the organisation set up to investigate suspected miscarriages of justice in England, Wales and Northern Ireland. The CCRC has to gather information in relation to the cases it reviews. Case related data contains the personal data and sensitive personal data of the applicants whose cases the CCRC is reviewing or has reviewed. They may also contain the personal data and sensitive personal data of witnesses in those cases and other individuals.

Definitions

Personal data means data which relates to a living individual who can be identified from the data and other information which the organisation has or is likely to have. This includes any expression of opinion about the individual and any indication of the intentions of any person in respect of the individual.

Sensitive personal data means personal data consisting of information about the following matters:

- a. the racial or ethnic origin of the data subject,
- b. his or her political opinions,
- c. his or her religious beliefs or other beliefs of a similar nature,
- d. whether he or she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- e. his or her physical or mental health or condition,
- f. his or her sexual life,
- g. the commission or alleged commission by him or her of any offence, or
- h. any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.

How personal data is obtained

Personal data about the applicant and details of the conviction and/or sentence they would like the CCRC to review primarily is obtained directly from the applicant through a completed application form and other submissions. Additional and more detailed information relating to the applicant and their conviction may be obtained from any other organisations or individuals who have had involvement in or hold information relevant to the

applicant's case. Such information is likely to also include information about the victim(s) and witnesses.

Data Protection Principles

The DPA regulates the processing of data relating to living and identifiable individuals; the individual who is the subject of the personal data is called the "data subject". Processing includes the obtaining, holding, using or disclosing of such data.

There are eight straightforward principles which underpin DPA:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained/processed for specific lawful purposes.
3. Personal data held must be adequate, relevant and not excessive.
4. Personal data must be accurate and kept up to date.
5. Personal data shall not be kept for longer than necessary.
6. Personal data shall be processed in accordance with rights of data subjects.
7. Personal data must be kept secure.
8. Personal data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection.

The principles apply to personal data which are held on the CCRC's computer systems or in its manual filing systems from which the data subjects are identifiable ("relevant filing systems").

Scope

This policy applies to all processing of personal information undertaken by the CCRC in relation to its main business purpose of reviewing suspected miscarriages of justice.

Roles and Responsibilities

For the purpose of DPA, the CCRC is a "data controller". As such, the Chief Executive / Board of the CCRC is ultimately responsible for ensuring the security of all personal data the CCRC holds about employees, applicants (to the CCRC) or any other individuals.

All Commissioners and employees of the CCRC, including contractors and temporary staff, have a personal responsibility to comply with DPA and must follow the principles set out in the act.

The CCRC will:

- ensure that there is a Data Protection Officer (DPO) in place, who ensures organisational compliance with Data Protection principles and provides information and guidance on the processing of all personal data;
- provide training for all staff members who handle personal information;
- provide clear lines of report and supervision for compliance with data protection;
- carry out regular checks to monitor and assess new processing of personal data and to ensure that the CCRC notifies the Information Commissioner of any changes in processing of personal data;
- develop and maintain DPA procedures to include: roles and responsibilities, notification, subject access, training and compliance testing.

Employees and Commissioners will:

- handle all personal data carefully and in accordance with the CCRC's policies and guidelines;
- ensure that personal data is recorded accurately and kept up to date;
- ensure that recorded personal data is not excessive and kept to the minimum necessary for the purpose for which it has been obtained;
- keep all personal data they process, whether in paper or electronic format, securely and within the CCRC's designated and appropriately controlled storage systems;
- report to an appropriate person any concerns that the data protection procedures are not being adhered to or that a breach of those procedures may occur;
- ensure that information is destroyed, in accordance with the provisions of DPA and in line with the CCRC's retention policies, when it is no longer required;
- understand that breaches of this policy may result in disciplinary action, including dismissal;
- on receipt of a request from an individual for information held about them (a subject access request) will without delay notify the CCRC's information team, who will deal with such a request.

Retention

Personal data of the applicant and others relevant to the case under review will be held securely by the CCRC during the time the application is active. At the end of the review, any files obtained from a third party will be returned to them or destroyed. CCRC generated application files will only be held for a specified time and thereafter will be destroyed securely, in line with CCRC retention periods.

Access

Only CCRC Commissioners and employees will normally have access to case-related information and any personal data contained therein. All Commissioners and employees are made aware of this policy and their obligations not to disclose case-related data to anyone who is not entitled to have this information.

Case-related data will not be passed to anyone outside of the CCRC unless specific exemptions in the DPA allow for the disclosure of information where there would otherwise be a breach of DPA. For example, the disclosure of the information is required by law, or is necessary for the purpose of, or in connection with, any legal proceedings. This would include data the CCRC discloses to a third-party expert it has instructed in a case review.

An individual will be supplied with a copy of any of their personal data held by the CCRC to which they are entitled if they make a valid subject access request and unless a specific exemption from disclosure means the data should be withheld.

All requests for information must be passed, in the first instance, to the CCRC's information team.