



PRIVACY NOTICE

Equality

In accordance with the Equality Act 2010, we will make any reasonable adjustment necessary to assist those with a protected characteristic or substantive health condition to engage fully with the Commission. If you require any assistance with this document please let us know.

We are a member of Happy to Translate and can, upon request, provide language assistance with this document or make it available in alternative formats.



HAPPY TO TRANSLATE

Tel: 0141 270 7030

info@scrc.org.uk

1.0 Introduction

- 1.1 The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) require the Scottish Criminal Cases Review Commission to explain how and why it processes personal data and special categories of personal data.
- 1.2 This privacy notice explains the personal data-processing activities that we carry out. It provides information about the Commission's general data protection duties.¹
- 1.3 Personal data identify a living individual, and include information about criminal convictions.
- 1.4 We are the controller of the personal data that we process.
- 1.5 We process personal data for a law enforcement purpose (including sensitive processing for such a purpose), but we also process personal data for recruitment, personnel and procurement purposes and where people contact us for information.
- 1.6 Special categories of personal data include employment, social security and health details.
- 1.7 Sensitive processing for the law enforcement purposes means the processing of data about a person's racial or ethnic origin, political opinions, religious or philosophical

¹ As is required by s44 (1) DPA.

beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation.

2.0 Appropriate Policy Documents

2.1 DPA requires us to produce a policy document in which we explain how we comply with DPA in sensitive processing for the law enforcement purposes and in processing special categories of personal data. You can find our data protection policy on our website, www.sccrc.co.uk

3.0 Law Enforcement Processing

3.1 Part 3 of DPA provides for the processing of personal data by competent authorities for the law enforcement purposes. The processing must be lawful and fair. processing for the purposes of law enforcement is lawful where it is necessary for the performance of a task carried out for that purpose by a competent authority.

3.2 The law enforcement purposes are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3.3 The Commission is a competent authority within the meaning of s30 of DPA: in Schedule 7 to DPA we are listed as an authority with investigatory functions.

What is our lawful basis for processing personal data for a law enforcement purpose?

3.4 Our lawful basis for processing such data for such a purpose derives from our functions and powers at s194A–T of the Criminal Procedure (S) Act 1995 (CPSA). These provisions set out that we may, on the consideration of any conviction of a person in Scotland or the sentence imposed in such a case, refer the case to the High Court of Justiciary for determination where we believe there may have been a miscarriage of justice and it is in the interests of justice to make such a reference (s194B and C of CPSA). Simply put, we process such data for such a purpose so that we can carry out our primary statutory function.

Whose personal data are we processing for such a purpose?

3.5 The people about whom we process such data (the data subjects) include:

- People convicted of offences
- Victims of crime
- Witnesses, including expert witnesses

What personal data are we processing for such a purpose?

3.6 The types of personal data we process include:

- Personal details, such as names and addresses
- Information about offences committed including criminal records

- Information provided by victims and witnesses to the Commission or to other law enforcement authorities e.g. in police witness statements

3.7 We also carry out sensitive processing, which is the processing of:

- Data about racial or ethnic origin
- Genetic data
- Health data
- Data about one's sex life or sexual orientation

For how long do we retain personal data for a law enforcement purpose?

3.8 We retain such data in accordance with our data retention policy.

To whom do we disclose personal data?

3.9 We may disclose such data to:

- Applicants to the Commission
- Legal representatives of an applicant
- Scottish Courts and Tribunal Service
- Crown Office and Procurator Fiscal Service
- Police Scotland
- Expert witnesses

3.10 The above list is not exhaustive and may vary on a case-by-case basis. The Commission generally will not transfer personal data outside the UK unless it is entitled to do so by law.

What is the source of the personal data we obtain?

3.11 We will obtain information about an applicant's conviction and sentence from the Scottish Court and Tribunal Service. We may obtain more information about the circumstances of the offences from the Crown Office and Procurator Fiscal Service and Police Scotland as well as the applicant's legal representatives. The information obtained will likely contain the personal data of victims of crime and witnesses.

Automated Decision Making

3.12 We do not use automated decision making in the cases we review.

What are your rights?

3.13 DPA sets out certain rights, including the rights of access, rectification and erasure, where a controller is processing personal data for any of the law enforcement purposes.

- 3.14 Where a data controller is processing personal data for law enforcement purposes it may restrict the data subjects rights for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to:
- Avoid obstructing an official or legal inquiry, investigation or procedure
 - Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
 - Protect public security
 - Protect national security
 - Protect the rights and freedoms of others
- 3.15 Where the controller restricts the rights of the data subject it must inform them without undue delay of the restriction, the reasons for it and their right to make a request to the ICO, complain to the ICO or to apply to the relevant court. The controller does not need to inform the data subject of the immediately foregoing information where doing so would undermine the purpose of the restriction.
- 3.16 We make sure, however, that we process your personal data in accordance with the six data protection principles set out in Part 3 of DPA: see our data protection policy.

Pseudonymisation

- 3.17 When we make a decision to refer or to not refer an applicant's conviction and/or sentence to the High Court, we produce documents known as statements of reasons. These documents will contain the personal data, including the criminal conviction data and possibly the special category data, of the applicant concerned. The statements of reasons may also contain the personal data, criminal conviction data and special category data of co-accused, complainers and witnesses. The statements of reasons are not public documents. We are prohibited by section 194J of CSPA from making the documents public. Applicants to whom the statement of reasons is sent are under no such restriction. In order to minimise the risk that a statement of reasons might become public, the Commission may, in cases relating to:
- the complainer(s) in a sexual offence case
 - child witnesses in a sexual offence case.
 - any other witness where it is reasonable to suspect that the revelation of their identity in a public forum would have serious negative consequences.

take appropriate steps to disguise the personal data of complainers, witnesses, child witnesses and possibly the applicant (in, for example, cases involving intra-family abuse) too, in order to limit the possibility of identifying an individual who would ordinarily give evidence in a closed court or where it is reasonable to suspect that the revelation of the individual's identity in a public forum would have serious negative

consequences. e.g. we would use an initialism in the place of a name so John Doe would be AZ and his daughter Jane Doe would be BZ etc.

4.0 General Processing

4.1 The purposes and lawful bases for our general processing of personal data, and the types of personal data we process, are set out below.

Recruitment

4.2 We process personal data in applications for employment positions with us.

4.3 Our lawful basis for such processing is Article 6(1)(e) of UK GDPR (public task).

4.4 Personal and/or special category data provided by the data subject include the person's name, address, date of birth, national insurance number, nationality, employment details and email address.

4.5 Personal data provided by a person to whom the data do not relate include employment references.

4.6 We also process personal data for equality and diversity monitoring. Our lawful basis for such processing is Article 9(2)(a) and (b) of UK GDPR (explicit consent/obligations in the field of employment).

4.7 Personal and/or special category data provided by the data subject for equality and diversity monitoring include the person's age, gender, nationality, racial/ethnic origin, sexual orientation and religious beliefs.

Personnel

4.8 We process personal data for the purposes of employment, including employment contracts, termination of contracts, retirement and ill-health.

4.9 Our lawful bases for such processing are Article 6(1)(b) (performance of a contract) and Article 9(2)(a) and (b) of UK GDPR (explicit consent/obligations of a controller in the field of employment).

4.10 Personal and/or special category data provided by the data subject include the person's name, address, date of birth, national insurance number and health information.

4.11 Personal data provided by a person to whom the data do not relate include the employee's next of kin, doctor's lines and occupational health reports.

Procurement

4.12 We process personal data for the purposes of contract tenders and awards.

- 4.13 Our lawful basis for such processing is Article 6(1)(b) of UK GDPR (performance of a contract or to take steps before entering into a contract).
- 4.14 Personal data provided by the data subject include the person's name, address, telephone number, email address and job title.

CCTV and Secure Entry

- 4.15 We use a CCTV system at our office which records and stores images of individuals attending the premises. The images, which are the personal data of the individuals captured, are processed for the legitimate interests of crime prevention and detection and security including data security. The purpose is to protect from theft, the hardware held in the office as well as the information and data stored on that hardware or otherwise stored within the premises. The data that we process for law enforcement purposes includes a significant volume of criminal conviction data and special category data which could, if left unsecure, pose a risk to the rights and freedoms of data subjects and as such the employment of this measure is proportionate and necessary.
- 4.16 We retain the CCTV footage for a period of 20-days before it is automatically overwritten. We may retain footage for a longer period where it relates to a data breach or where we have reason to suspect that a criminal offence may have been committed and the CCTV footage has captured this.
- 4.17 We employ a secure door entry system to our office. The system will, when activated, record images of individuals attending. This personal data is processed for the legitimate interests of security. The personal data captured by the secure entry system is deleted on a daily basis.

Contacting the Commission

- 4.18 We process personal data where a person contacts us for information.
- 4.19 Our lawful basis for such processing is Article 6(1)(a) and (1)(e) of UK GDPR (consent/public task).
- 4.20 Personal data provided by the data subject include the person's name, telephone number and email address.
- 4.21 We retain personal data for all general processing in accordance with our data retention policy.

General Processing – Your Rights

Right of access – you may request to see the data that we hold about you (although there are exceptions to this); this is known as a ‘subject access request’.

You can make a subject access request either by completing the form on our website, at www.sccrc.co.uk/contact-us, emailing info@sccrc.org.uk, telephoning 0141 270 7030, or writing to the Scottish Criminal Cases Review Commission, 4th Floor, Portland House, 17 Renfield Street, Glasgow G2 5AH.

Right to rectification – we must correct, without delay, the data that we hold about you which is inaccurate. There are exceptions to this right, but we shall tell you where those exceptions apply where you contact us. Where it is not possible to establish the accuracy of your personal data, we shall restrict who can see your data, or to whom we disclose your data.

Right to erasure – you may request that we delete your personal data, but we shall do so only where we are not legally required to keep your data. It may be more appropriate for us to restrict how we process your personal data by restricting who can see your data, or to whom we disclose your data.

Right to object – you may object to the processing we carry out where our legal basis for processing your personal data is for carrying out a task in the public interest, exercising our lawful duty or we believe it is in our legitimate interests.

Right to withdraw consent – where we process your personal data on the basis of your consent, you may withdraw your consent. Where you withdraw your consent, we shall destroy your personal data on our receipt of your withdrawal-of-consent notification, unless there is an overriding purpose for continuing to process your personal data.

Where you wish us to correct or delete your personal data, or where you wish to object to our processing your data, or where you wish to withdraw your consent, you can tell us either by completing the form on our website, at www.sccrc.co.uk/contact-us, or contacting our Data Protection Officer Stephen Lynn by emailing info@sccrc.org.uk, telephoning 0141 270 7030, or writing to the above-mentioned postal address.

If we decide not to comply with your requests under the above-mentioned rights, you may ask the Information Commissioner’s Office (ICO) to check whether our decisions are correct.

If you are not content with how we have processed your personal data, you may complain to the ICO. You can also seek an enforcement notice from your local court.

You can contact the ICO either by way of its website, at www.ico.org.uk, telephoning 0303 123 1113, or writing to the ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Date first approved	August 2021
Date of this review	14 October 2022
Date of next review	August 2023