DATA PROTECTION POLICY

Equality

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

We are also a member of Happy to Translate (HTT) and can provide language assistance with this document or make it available in alternative formats if required upon request.

☎ 0141 270 7030

info@sccrc.org.uk

INTRODUCTION

1.0 Policy statement

1.1 The Scottish Criminal Cases Review Commission (the Commission) recognises the importance of protecting the privacy of its staff and other individuals about whom it obtains, records and discloses information. It recognises that the information about those individuals, or 'personal data',[1] it processes must be processed in accordance with the General Data Protection Regulation (GDPR)[2] and the Data Protection Act 2018 (DPA).

1.2 The Commission regards the fair and lawful processing of personal data as essential to the successful performance of its statutory functions and its four strategic aims. To that end, the Commission fully endorses and complies with the principles of data protection.

1.3 The Commission recognises that a failure by it to comply with GDPR and DPA is unlawful and could result in the taking of legal action.

1.4 The purpose of this policy is to make sure that Board Members, staff and the Commission's other stakeholders are clear about the principles of data protection.

---

1 The person to whom the data relate is called the 'data subject'.

2 'GDPR' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

2.0 Policy authorisation

2.1 On 14 August 2020 the Board of the Commission approved this version of this policy.

3.0 Related polices

3.1 This policy must be read in conjunction with the Commission's data retention and disclosure policies, its case handling procedures and its records management plan.

4.0 Definitions

4.1 The terms used in this policy are used in accordance with their interpretation in Article 4 of GDPR and Parts 1, 2 and 3 of DPA.

GDPR

5.0 Subject matter and scope of GDPR

5.1 GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data; it applies both to the processing of such data by automated means and data which form part of a filing system; and it applies to the processing of personal data in the context of activities of an establishment of a 'data controller'[3] or a processor in the European Union (EU).[4]

5.2 The processing of personal data includes collecting, recording, disclosing and destroying such data.

6.0 Data protection principles

6.1 GDPR requires that the data must be:

(a) processed fairly, lawfully and in a transparent manner
(b) collected for specified, explicit and legitimate purposes
(c) adequate, relevant and limited to what is necessary
(d) accurate
(e) kept no longer than necessary
(f) processed securely[5]

6.2 An organisation is required to show how it complies with the principles ('the accountability principle').[6]

---

[3] The Board of the Commission is the data controller in relation to the personal data that the Commission processes.
[4] Articles 1–3 of GDPR.
[5] Article 5(1).
[6] Article 5(2).

6.3 An organisation may transfer personal data outside the EU only in compliance with the conditions for transfer set out in chapter V of GDPR.

7.0 Lawfulness of processing

7.1 GDPR provides that processing shall be lawful only if at least one of the conditions listed in Article 6(1) applies.

7.2 The processing that the Commission undertakes is processing that is necessary either for the performance of a contract, for compliance with a legal obligation to which it is subject, to protect the vital interests of the data subject or of another natural person, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Commission.[7]

7.3 GDPR provides, however, that Member States may introduce more specific provisions to adapt the application of the rules with regard to processing for compliance with Article 6(1)(c) and (e) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing.[8] Reference is made in that regard to s8 of DPA.

7.4 Reference is made also to data that are processed for 'the law enforcement purposes' under Part 3 of DPA (discussed below under **Case-related data**).

8.0 Consent

8.1 Where it is seeking to process information about an individual for purposes other than the aforementioned purposes, the Commission will request the express consent of the individual concerned.

8.2 An individual who has provided his or her consent has the right to withdraw it at any time.

9.0 Criminal convictions and offences

9.1 GDPR provides that the processing of personal data relating to criminal convictions shall be carried out only under the control of official authority or when the processing is authorised by EU or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.[9]

10.0 Rights of individuals

10.1 GDPR provides for certain rights of individuals, including the following rights:

---

7 Article (6)(1)(b), (c) and (e).
8 Article 6(2) and (3).
9 Article 10. See also ss10 and 11 of, and Schedule 1 to, DPA.

(1) to be informed
(2) access
(3) rectification
(4) erasure
(5) restriction of processing
(6) 'data portability' (provision of information in an electronic form)
(7) to object[10]

11.0 Restrictions

11.1 GDPR enables Member States to restrict the scope of the obligations and rights that Articles 12–22 provide.[11] Reference is made in that regard to s15 of DPA and Schedule 2, Part 1, to DPA.

12.0 Responsibilities

12.1 It is, ultimately, the responsibility of the data controller (in the Commission's case this is, as noted, the Board of the Commission) to implement appropriate technical and organisational measures to make sure and to be able to demonstrate that processing is performed in accordance with GDPR[12] (and DPA).

12.2 It is, however, an organisation's designated 'data protection officer' (DPO) who takes responsibility for data protection compliance.[13] The Commission's designated DPO is its Head of Casework (contact: info@sccrc.org.uk). The DPO:

- informs and advises the Commission and its staff about their obligations to comply with GDPR
- monitors compliance with GDPR, including managing internal data protection activities and advising on data protection impact assessments
- trains staff and conducts internal audits
- is a point of contact for the data subjects and the Information Commissioner's Office (ICO)
- reports to the Board of the Commission[14]

[10] Articles 12–22.
[11] Article 23.
[12] Article 24.
[13] Article 37.
[14] Articles 38 and 39.

CATEGORIES OF DATA

13.0 Categories of data

13.1 In having regard to GDPR and DPA, the Commission has categorised the personal data it processes into the following two broad categories:

- **Non-case-related data**: data about Board Members, staff, former staff and prospective staff ('Board Members/staff')

- **Case-related data**: data about applicants, witnesses in cases that the Commission is reviewing or has reviewed, and any other individuals whose data feature in the cases that the Commission is reviewing or has reviewed

14.0 Non-case-related data

Purposes

14.1 The Commission processes personal data about Board Members/staff. Such data are processed for, among other purposes, the following specified purposes:

- recruitment
- equal opportunities monitoring
- administering maternity, paternity, dependant-care and other leave
- disciplinary and grievance
- payroll
- holidays and absences
- the proper administration of the contract of employment
- CCTV – crime prevention and/or staff monitoring

Rights of access, rectification, erasure etc

14.2 Board Members/staff have the right to gain access to data that the Commission holds about them.[15] The right applies, for example, to information held in sickness records, disciplinary, grievance or training records, appraisal or performance-review notes, emails, general personnel files and interview notes.

14.3 As soon as is reasonably practicable, but within one month of his receipt of the written request for access to the personal data, the Commission's Director of Corporate Services (DOCS) will provide the requester with his or her personal data, in an intelligible form (including, where appropriate, by electronic means), and the following information:

- the purposes of the processing

- the categories of personal data

- the recipients to whom the personal data have been disclosed (if any)

[15] Article 15.

- the right to request the Commission to rectify, erase and restrict the processing of personal data or restriction, and the right to object to such processing

- the right to lodge a complaint with the ICO

- (where the personal data have not been collected from the data subject) any available information about their source[16]

14.4 The Commission will not disclose personal data where it adversely affects the rights and freedoms of others.

14.5 Board Members/staff have the right to obtain from the Commission without undue delay the following: the rectification of inaccurate data about them; the erasure of their personal data where, for example, those data are no longer necessary in relation to the purposes for which they were collected and otherwise processed; and the restriction of processing of their personal data.[17] The DOCS will, where it applicable to do so, rectify, erase and restrict the data, and notify the data subject.

Excluded information

14.6 Staff are not entitled to have access to certain information, including the following information:

- confidential references about the individual concerned given on behalf of the Commission by, for example, one of its Board Members or its Chief Executive

- any documents privileged on the grounds of legal professional privilege

- data used for the prevention or detection of a crime

- personal data being processed for the purposes of management forecasting or planning

14.7 References received from other people/organisations are not treated in the same way as references about a staff member that a Board Member or the Chief Executive gives.

14.8 In the former case, where the individual about whom the reference was made asks the Commission to disclose to him or her the information in the reference, the Commission will ask the referee whether he or she consents to the disclosure of the information to the individual. Where the referee states that he or she does not want the Commission to release the reference, the Commission will provide the reference to the individual only if it considers that it is reasonable in all the circumstances to comply with the request without the referee's consent. In taking such a decision, the Commission will take into account the following factors:

- any express assurance of confidentiality given to the referee

- any relevant reasons the referee gave for withholding the information

[16] *Ibid.*
[17] Articles 16–19.

- the potential or actual effect of the reference on the individual
- the fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy
- that good employment practice suggests that an employee should have already been informed of any weakness that he or she has.
- any risk to the referee
- whether it is possible to keep the identity of the referee secret

Accuracy

14.9 The Commission will take reasonable steps to make sure that the non-case-related data that it keeps are accurate.

14.10 Board Members and staff are required to inform the DOCS of changes in their contact details as soon as reasonably practicable, in order to assist the Commission in keeping their personal data up to date.

Security[18]

14.11 The data are kept in a secure filing cabinet or on a password-protected computer file. Every effort is made to make sure that paper-based data are stored in organised and secure systems. Only those staff who have a legitimate business need to access such personal data may access them.

14.12 Personal data about former staff will be separated from personal data about existing staff, and will be placed in marked folders. Each folder will be marked with the name of the former staff member, his or her date of birth and the dates of employment.

14.13 The Commission operates a clear desk policy at all times in respect of non-case-related data.

Retention

14.14 The Commission keeps such data in accordance with its data retention policy and with its associated data retention and destruction procedures.

14.15 All documents containing such data that are destroyed are destroyed securely and in accordance with the data protection principles. The DOCS has responsibility for overseeing the destruction of such data.

Post

14.16 All confidential post must be opened by the addressee only.

[18] Discussed in more detail below under **Case-related data**.

Use of photographs

14.17 The Commission will seek consent from a Board Member or a staff member before displaying a photograph in which he or she appears. It will remove any photograph where the Board Member or staff member asks it to do so.

Contact details

14.18 The contact details of a Board Member or staff member are made available only to other Board Members or other staff members. They are not passed on to anyone outside the Commission without the consent of the Board Member or the staff member (unless the Commission is entitled by law to do so).

14.19 Any other employee-related information is not accessed during the day-to-day running of the organisation.

14.20 The emergency contact details of each Board Member and each staff member are kept in an appropriate file to be used in emergency situations.

Sickness and injury records/absence records

14.21 Sickness and injury records include information about the physical and mental health of employees. They constitute 'data concerning health'.[19] The term 'absence record' is used to describe a record that may give the reason for absence as 'sickness' or 'accident' but does not include any reference to specific medical conditions. It does not constitute data concerning health.

14.22 The Commission restricts its record-keeping in that regard, so far as practicable, to absence records.

Third-party disclosure requests

14.22 The Commission may receive requests from a third party for information about Board Members/staff. In dealing with such requests, the Commission has a responsibility to safeguard the interests of the Board Members/staff.

14.23 In some cases, however, the Commission will have no choice but to respond positively to such a request for information – where, for example, the police need information in connection with a criminal investigation. In other cases, a third party may want information in connection with a legal action. The Commission may disclose the information in such cases where it is entitled by law to do so (for more information, please see the Commission's disclosure policy).

14.24 The Board of the Commission takes any decisions about whether to comply with such requests.

[19] As defined in Article 4(15) of GDPR and processed in accordance with Article 9 ('Processing of special categories of personal data').

15.0 Case-related data

Part 3 of DPA: Law enforcement purposes

15.1 Part 3 of DPA, which implements the Law Enforcement Directive,[20] provides for the processing of personal data by competent authorities for 'the law enforcement purposes'.

15.2 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.[21]

15.3 Processing of personal data for the law enforcement purposes must comply with the data protection principles set out in ss34–40 of DPA.[22] In particular, processing of personal data for such purposes must be, in terms of 'the first data protection principle', 'lawful and fair'.[23]

15.4 Where the data subject has not consented to the processing, the processing of data for any of the law enforcement purposes is lawful only if, in terms of the first data protection principle, the processing is necessary for the performance of a task carried out for that purpose by a competent authority within the meaning of s30 of DPA.[24]

15.5 Where the processing for any of the law enforcement purposes is 'sensitive processing'[25] and where the data subject has not consented to the processing, the processing is permitted only where, in terms of the first data protection principle, it is strictly necessary for the law enforcement purposes and meets at least one of the conditions in Schedule 8 to DPA and the controller has an appropriate policy document in place.[26]

15.6 The Commission is a competent authority within the meaning of s30 of DPA (it is listed as such in Schedule 7 to DPA). It is a 'controller'[27] for the processing of data for law enforcement purposes.

Purpose

15.7 The Commission's legal basis for processing such data derives from its function and powers as set out in the Criminal Procedure (S) Act 1995 (CPSA), s194A–T. In other words, the Commission processes such data so that it can carry out its primary statutory function.[28]

15.8 Such data include the personal data of the applicants whose cases that the Commission is reviewing or has reviewed. They may also include personal data of witnesses in those cases

---

[20] Which means Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.
[21] Section 31 of DPA.
[22] Those principles mirror the principles set out in Article 5 of GDPR.
[23] Section 35(1) of DPA.
[24] Section 35(2)(b) of DPA.
[25] Which includes processing of data concerning health (s35(8) of DPA).
[26] Section 35(3)–(5) of DPA.
[27] In terms of s32 of DPA.
[28] The Commission 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 it believes there may have been a miscarriage of justice and it is in the interests of justice to do so (s194B and C of CPSA).

and of other individuals. They are collected, recorded and – in limited circumstances – disclosed to third parties.

15.9 As regards the Commission's processing of such data it holds about cases which constitutes sensitive processing, it occurs only where it is strictly necessary for law enforcement purposes and it meets at least one of the conditions in Schedule 8 to DPA – ie, it is necessary for the exercise of a function conferred on the Commission by an enactment (by virtue of s194 of CPSA) and for reasons of substantial public interest (see condition 1 in Schedule 8), or it is necessary for the administration of justice (condition 2). In addition, the Commission processes such data in accordance with the safeguarding requirements set out in s42 of DPA.

The controller's general duties and the rights of access, rectification, erasure etc of the data subjects

15.10 The controller's general duties and the rights of access, rectification, erasure etc of the data subjects where data is processed for law enforcement purposes are set out in s45–48 of DPA. However, those sections do not apply in relation to the processing of 'relevant personal data'[29] in the course of criminal investigation or criminal proceedings, including proceedings for the purpose of executing a criminal penalty.[30]

15.11 The Commission processes relevant personal data. In doing so, it relies on s43, which dis-applies ss44–48 of DPA. It does, however, take appropriate measures to protect the data subject's rights and freedoms and legitimate interests.

15.12 Any requests for information must be passed, in the first instance, to the designated legal officer.

Disclosure

15.13 It is only Board Members and staff who will normally have access to such data. All Board Members and staff are made aware of this policy and their obligation not to disclose such data to anyone who is not supposed to have them.

15.14 Such data is passed to a person outside the Commission without the data subject's consent only where the Commission is entitled by law to do so (for more information, please see the Commission's disclosure policy).

Accuracy and relevancy

15.15 The Commission takes reasonable steps to make sure that it stores and retains only those data which are or were relevant to its case reviews.[31]

15.16 It takes reasonable steps to make sure that such data it keeps are accurate.[32]

[29] As defined in s43(4) of DPA.
[30] Section 43(3) and (4) of DPA..
[31] In terms of the requirements set out in ss34 and 37 of DPA.
[32] In terms of the requirements set out in ss34 and 38 of DPA.

Security

15.17 The Commission handles all such data it processes in a secure and responsible manner.[33] Its security arrangements – both in terms of its physical and technological security and its management and organisational security – reflect the large volumes of such data it processes and the levels of sensitivity and confidentiality of those data, and the harm that might result from the improper use of those data or from their accidental loss or destruction. A summary of those arrangements follows.

- The Commission classifies most of the data it processes as 'official'.[34]
- The data that the Commission processes are subject to extensive physical security arrangements: the Commission's premises are protected by an alarm, a shutter, security lighting and CCTV; visitors to its premises are subject to controlled access.
- The Commission operates its own IT system from its premises, which has been designed with specific security arrangements, arrangements which are subject to ongoing testing. For example, the data kept electronically are kept on a password-protected computer file; the IT system has been installed with a firewall, an anti-spyware tool and virus-checking software, and downloads the latest security updates; regular back-ups of all data on its computers are taken; and all such data are securely removed from its old computers before the computers are disposed.
- Physical information the Commission sends and receives is undertaken in a secure manner, using vetted courier services or the Royal Mail.
- Where it sends case-related data electronically, the Commission does so using a secure email system.
- The Commission makes every effort to make sure that case-related data kept in a paper-based system are kept in organised and secure systems.
- The Commission has put in place procedures that staff must follow concerning, among other things, the instruction of a third party and case-related data given to the third party, case-related data that a staff member takes out the office, and the use of letters, emails and faxes (see the Commission's case handling procedures).
- All case-related data kept off-site are kept securely. Where, for example, Board Members/staff are working from home, the data is held electronically, on a password-protected device and in an encrypted environment.
- All staff are subject to Disclosure Scotland 'standard disclosure'; 'enhanced disclosure' is in place for Board Members and all staff at legal officer level and above; Board Members and several key staff have been cleared to 'security clearance' level.
- All waste paper containing case-related data is destroyed securely.

[33] In terms of the requirements set out in ss34 and 40 of DPA (see also Article 32 of GDPR).

[34] See the Government Security Classifications, as issued by the Cabinet Office, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

- The Commission operates a clear desk policy at all times in relation to case-related data.

Retention

15.18 The Commission retains all case-related data in accordance with s39 of DPA: see its data retention policy and its associated data retention and destruction procedures.

15.19 All documents containing case-related data that are destroyed are destroyed securely and in accordance with the data protection principles. The Head of Casework has responsibility for overseeing the destruction of such data.

OTHER MATTERS

16.0 Breaches

16.1 The Commission recognises that, if a 'personal data breach'[35] occurs, it is important to deal with the breach effectively, in accordance with the requirements set out in Articles 33 and 34 of GDPR.

16.2 Accordingly, the Commission has a 'response plan for personal data breaches'. The plan sets out the Commission's strategy for dealing with a breach of security, and includes the following three elements:

- containment and recovery
- notification of the breach
- evaluation and response

16.3 Where the personal data breach is likely to result in a risk to the rights and freedoms of individuals – ie, such a breach, if unaddressed, is likely to have a significant detrimental effect on individuals, resulting in discrimination, damage to reputation, financial loss or loss of confidentiality – the Commission will report the breach to the ICO without undue delay, and not later than 72 hours after it became aware of the breach.[36] In doing so, it will:

- describe the nature of the personal data breach
- the categories and approximate number of individuals concerned
- the categories and approximate number of personal data records concerned
- communicate the name and contact details of the DPO
- describe the likely consequences of the breach
- describe the measures it has taken, or proposes to take, to address the breach[37]

16.4 Where the personal data breach is likely to result in a high risk[38] to the rights and freedoms of individuals, the Commission will inform those individuals concerned directly and without undue delay.[39]

---

[35] A personal data breach means a breach of security leading to the destruction, loss, alteration and unauthorised disclosure of, or access to, personal data.
[36] Article 33(1) of GDPR.
[37] Article 33(3).
[38] A 'high risk' means the threshold for informing is individuals is higher than for notifying the ICO.
[39] Article 34.

16.5 Where it decides to tell individuals about a breach, the Commission will provide the name and contact details of the DPO and will describe, in clear and plain language, the nature of the breach, the likely consequences of the breach and the measures it has taken, or proposes to take, to address the breach.

'The law enforcement purposes'

16.6 Where it is processing data for law enforcement purposes, in terms of Part 3 of DPA, and there is a data breach, the Commission will apply the relevant DPA provisions about notification to the ICO and the data subjects, namely ss67 and 68, the terms of which mirror the above-mentioned steps about notification.

17.0 Data protection impact assessment (DPIA)

17.1 A DPIA is a tool that can help an organisation identify the most effective way to comply with its data protection obligations and to meet individuals' expectations of privacy.

17.2 The Commission will carry out a DPIA when:

- it is using new technologies, or using technologies in a new environment; and
- the processing of data is likely to result in a high risk to the rights and freedoms of individuals[40] (which will include large scale processing of special categories of data or personal data relating to criminal convictions).

18.0 Offences

18.1 It is an offence for a Board Member or a staff member, knowingly or recklessly and without the Commission's consent, to obtain or disclose personal data, or to procure the disclosure of the personal data, to another person outwith the Commission.

18.2 It is an offence for a Board Member or a staff member to sell, or to offer to sell, personal data which have been unlawfully obtained.

19.0 Compliance

19.1 It is the responsibility of all Board Members and all staff to make sure that they are familiar with the terms of this policy and that they comply with it at all times.

19.2 Any questions or concerns about the application of this policy should be referred to the Head of Casework.

20.0 Review

20.1 The Head of Casework will review this policy at least annually.

[40] Articles 35 and 36.

Date first approved	16 August 2013
Date of this review	14 August 2020
Date of next review	13 August 2021