Data Protection Safeguards Policy

Appropriate policy document

Scottish Information Commissioner

Contents

Glossary and abbreviations

Term used	Explanation
FOISA	Freedom of Information (Scotland) Act 2002
EIRs	Environmental Information (Scotland) Regulations 2004
DPA 2018	Data Protection Act 2018
SIC, The Commissioner, we	Scottish Information Commissioner
DPA 2018	Data Protection Act 2018
GDPR	General Data Protection Regulation (EU) 2016/679

Part A: Sensitive processing for law enforcement purposes

Introduction

1. As part of the Scottish Information Commissioner's statutory functions, we can investigate (and report for prosecution) public authorities and their employees for offences committed under section 65 of the Freedom of Information (Scotland) Act 2002 (FOISA) and regulation 19 of the Environmental Information (Scotland) Regulations 2004 (the EIRs). The Commissioner is named as a competent authority for the purpose of Part 3 of the Data Protection Act 2018 (the DPA 2018), which applies to the processing of personal data by such authorities for law enforcement purposes.

2. These purposes are set out at section 31 of the DPA 2018 and include the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, which might include safeguarding against and preventing threats to public security.

3. Not all of our processing of personal data relating to law enforcement (such as information about convictions or alleged offences) will be carried out for our functions relating to section 65 and regulation 19. We may process such data for other purposes (for example, where such information has been withheld by a Scottish public authority in response to an information request and we need to consider it when investigating an appeal). This general processing, which is not for the primary purpose of law enforcement and which we do not carry out as a competent authority, will be covered by the General Data Protection Regulation (the GDPR) and Part 2, Chapter 2 of the DPA. Please see Part B of this document for more information about this processing, and about our processing of special category data (e.g. personal data relating to health).

Sensitive processing

4. Sensitive processing is defined at section 35(8) of the DPA as:

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

5. We carry out sensitive processing under section 35(3) of the DPA 2018 only:

   - in reliance on the consent of the data subject, or
   - where it is strictly necessary for a law enforcement purpose and it meets one of the conditions in Schedule 8 to the DPA 2018. ("Strictly necessary" in this context means that the processing has to relate to a pressing social need, and we cannot reasonably achieve it through less intrusive means.)

6. In both of these cases, we are required to have an appropriate policy in place (section 42 of the DPA 2018), explaining our procedures and policies in relation to sensitive processing, including how we:

- comply with the relevant data protection principles (i.e. specific data protection principles set out in Part 3, Chapter 2 of the DPA 2018 in relation to law enforcement processing) , and
- manage the retention of the data in question.

The principles (sensitive processing)

Section 35 – the first data protection principle

7. The first principle is that processing for law enforcement purposes must be lawful and fair. It is only lawful if and to the extent it is based on law and either:
   - the data subject has given their consent for the processing, or
   - the processing is necessary for a law enforcement purpose, performed by a competent authority.
8. The additional conditions to be met for sensitive processing are set out above. Here, we must consider how we will meet at least one Schedule 8 condition when carrying out such processing.
9. Our processing for law enforcement purposes satisfies the first Schedule 8 condition, as it is necessary for the exercise of a function conferred on the Commissioner by FOISA, and is also necessary for reasons of substantial public interest. We are required to investigate and, where appropriate, report for prosecution possible offences under section 65 of FOISA and regulation 19 of the EIRs. There is a substantial public interest in doing so, including sensitive processing of personal data where necessary.
10. In circumstances where we seek consent, we make sure the consent is:
    - specific to the processing in question, informed and unambiguous
    - given by an affirmative action
    - recorded as the condition for processing.

Section 36 – the second data protection principle

11. Under the second principle:
    - the law enforcement purpose for which the data are collected must be specified, explicit and legitimate, and
    - the personal data must not be processed in a manner that is incompatible with that purpose.
12. We process personal data for the law enforcement purposes listed at section 31 of the DPA 2018, specifically the investigation, detection or prosecution of criminal offences. Any offences would be under section 65 of FOISA or regulation 19 of the EIRs.
13. We are authorised by law to process personal data for these purposes. We may process personal data collected for one of these purposes (whether by us or another controller) for any of our other law enforcement purposes, providing the processing is necessary and proportionate to that purpose.
14. We may use data collected for a law enforcement purpose for purposes other than law enforcement, but only where we are authorised by law to do so.

15. If we are sharing data with another controller, we will document that (and the basis on which) they are authorised by law to process the data for their purposes.

Section 37 – the third data protection principle

16. For the third principle to apply, personal data processed for a law enforcement purpose must be adequate, relevant and not excessive in relation to that purpose.

17. We do not systematically collect or harvest personal data for law enforcement purposes. Any sensitive processing we carry out for such purposes is necessary for and proportionate to those purposes. The processing is carried out in the context of us carrying out processes which enable us to meet our stated purposes for processing.

18. Where personal data covered by any of the categories of sensitive processing are provided to or obtained by us, but are not relevant to our stated purposes, we will erase them.

Section 38 – the fourth data protection principle

19. The fourth principle states that:

    - personal data processed for a law enforcement purpose must be accurate and, where necessary, kept up to date, and
    - every reasonable step must be taken to ensure the erasure or rectification of any such data found to be inaccurate, without delay, having regard to the law enforcement purpose for which they are processed.

20. Where we become aware that personal data processed for law enforcement purposes are inaccurate or out of date, we will consider whether we can erase or rectify the data while still discharging our law enforcement purposes properly. If we can, we will take every reasonable step to ensure that the data are erased or rectified without delay. If we decide not to either erase or rectify the data, we will document our decision.

21. As far as possible, we distinguish between personal data based on facts and personal data based on personal assessments or opinions, and mark the file to reflect the distinction. There are circumstances where this is not possible.

22. Where relevant, and as far as possible, we distinguish between personal data relating to different categories of data subject, such as:

    - people suspected of committing an offence
    - people convicted of a criminal offence
    - known or suspected victims of a criminal offence
    - witnesses or other people with information about offences.

23. We do this by marking the relevant records.

24. Consistent with those purposes, we take reasonable steps to ensure that personal data which are inaccurate, incomplete or out of date are not transmitted or made available for any of the law enforcement purposes. We do this by verifying any data before sharing them externally. We also provide the recipient with the necessary information we hold to assess the accuracy, completeness and reliability of the data.

25. If we discover, after transmission, that the data were incorrect or should not have been transmitted, we will tell the recipient as soon as possible.

26. It should be noted that (unless the Commissioner is required by law to share them with anyone else) the recipients of personal data we process for law enforcement purposes will, apart from the person making the allegation (with whom only very limited information will ever be shared), only be Police Scotland or the Crown Office and Procurator Fiscal Service, with whom the Commissioner has a Memorandum of Understanding governing the investigation and reporting of offences under section 65 of FOISA and regulation 19 of the EIRs.

27. We document our decisions to make personal data available for any of the law enforcement purposes.

Section 39 – the fifth data protection principle

28. Under the fifth principle, personal data processed for a law enforcement purpose must be kept for no longer than is necessary for that purpose.

29. We have a corporate File Plan and Retention Schedule here, which applies to data processed for these purposes, and retain information processed for the purposes of law enforcement for five years from closure of the matter, unless there is a legitimate reason to retain it for longer. We will document any decision to retain.

Section 40 – the sixth data protection principle

30. The sixth principle requires processing for any of the law enforcement purposes to be in a manner that ensures appropriate data security (including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage), using appropriate technical and organisational measures.

31. Electronic information is processed within our secure network. Hard copy information is processed within our secure premises.

32. Electronic and hard copy information processed for the law enforcement purposes is only available to the limited number of staff who carry out the processing for these purposes. Our electronic systems and physical storage have appropriate access controls applied.

33. The systems we use to process personal data for law enforcement purposes allow us to erase or update personal data at any point in time. They also allow us to log the following information:

    - Collection
    - Alteration
    - Consultation (access)
    - Identity of person who accessed
    - Disclosures
    - Combination of records
    - Erasure.

Retention

34. We have a corporate File Plan and Retention Schedule here which applies, amongst other things, to sensitive information processed for law enforcement purposes.

35. This policy satisfies the requirements of section 42 of the DPA and is therefore an appropriate policy document in support of our compliance with the first data protection principle for law enforcement purposes, in terms of section 35(4) and (5) of the DPA.

Part B: General processing of special category and criminal convictions etc. data

Introduction

36. In carrying out the Scottish Information Commissioner's statutory functions, we are required to process special categories of personal data, as defined in Article 9(1) of the GDPR. These are biometric data uniquely identifying a living individual, and personal data about:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- health
- a person's sex life or sexual orientation.

37. Article 9(2) of the GDPR sets out various conditions under which special category data may be processed, but a number of these require further specific legal provision.

38. We are also required to process (for purposes other than law enforcement – see above) personal data relating to criminal convictions and offences or related security measures. Under Article 10 of the GDPR, such processing may be carried out only under the control of official authority or as authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects.

39. Section 10 of the DPA 2018 makes further provision for the processing of special category and criminal convictions etc. data. The specific conditions under which processing may be carried out are set out in Parts 1, 2 and 3 of Schedule 1 to the DPA 2018. For a number of these conditions to apply, we are required to have in place an appropriate policy document, explaining:

- our procedures for securing compliance with the data protection principles in Article 5 of the GDPR, when relying on that condition for processing, and
- our policies for managing retention of the data in question.

Schedule 1 conditions

40. We may need to carry out processing of special category or criminal convictions etc. data under the following conditions in Parts 1 and 2 of Schedule 1, which require the data controller to have an appropriate policy document in place when carrying out the processing:

Part 1 (Conditions relating to employment, health and research, etc.)

40.1 Condition 1 – processing necessary for the purposes of performing or exercising obligations or rights imposed or conferred by law in connection with employment, social security or social protection.

Part 2 (Substantial public interest conditions)

40.2 Condition 6 – processing necessary for the exercise of a function conferred on a person by an enactment or rule of law.

40.3 Condition 7 – processing necessary for the administration of justice.

40.4 Condition 8 – processing of specified categories of personal data, necessary for the purposes of identifying or keeping under review equality of opportunity or treatment between specified groups of people, with a view to enabling the promotion or maintenance of such equality.

40.5 Condition 10 – processing necessary for the purposes of prevention or detection of an unlawful act.

40.6 Condition 12 – processing necessary for the purposes of complying with a regulatory requirement involving taking steps to establish whether a person has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct.

The principles – general processing

41. When relying on the above conditions, we will secure compliance with the data protection principles as follows.

The first data protection principle

42. Under the first principle, personal data must be processed fairly, lawfully and in a transparent manner in relation to the data subject.

43. We will adhere to recognised principles of necessity in applying these conditions, within our powers and obligations under our governing legislation and as an employer. We are required to investigate and, where necessary, take appropriate action in relation to potential breaches of that governing legislation. We are also required to secure compliance with equalities legislation in our employment practices. There is a substantial public interest in doing so, including processing of special category and criminal convictions etc. data where necessary.

44. Our Privacy Notice here tells data subjects what to expect in relation to our processing of their personal data, including processing of special category and criminal justice etc. data where necessary. In relation to all such processing, we will comply fully with our duties under the GDPR and the DPA in relation to the rights of the data subject.

The second data protection principle

45. The second principle limits the collection of personal data to specified, explicit and legitimate purposes, and requires that the data will not be further processed in a manner incompatible with those purposes.

46. We process personal data for the purposes set out in our Privacy Notice, including fulfilment of our responsibilities under our governing legislation and as an employer. We are authorised by law to process personal data for these purposes. We may process personal data collected for one of these purposes (whether by us or another controller) for any of our other purposes, providing the processing is necessary and proportionate to that purpose.

47. If we are sharing data with another controller, we will document that (and the basis on which) they are authorised by law to process the data for their purposes.

The third data protection principle

48. Under the third principle, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

49. We do not systematically collect or harvest personal data for any of our purposes. Any processing we carry out for such purposes is necessary for and proportionate to those purposes. The processing is carried out in the context of us carrying out processes which enable us to meet our stated purposes for processing.

50. Where special category or criminal convictions etc. data are provided to or obtained by us, but are not relevant to any of our stated purposes, we will erase them.

The fourth data protection principle

51. The fourth principle requires personal data to be accurate and, where necessary, kept up to date.

52. Where we become aware that special category or criminal convictions etc. data are inaccurate or out of date, we will consider whether we can erase or rectify the data while still discharging the relevant purposes properly. If we can, we will take every reasonable step to ensure that the data are erased or rectified without delay. If we decide not to either erase or rectify the data, we will document our decision.

53. As far as possible, we distinguish between personal data based on facts and personal data based on personal assessments or opinions, and mark the file to reflect the distinction. There are circumstances where this is not possible.

The fifth data protection principle

54. Under the fifth principle, personal data can be kept (in a form permitting identification) for no longer than is necessary for the purposes for which they are processed.

55. We have a corporate File Plan and Retention Schedule here, which applies to, amongst other things, special category and criminal convictions etc. data, and sets out the periods (depending on the nature of the data) for which the data will be retained. We will document any decision to retain for longer than the relevant specified period.

The sixth data protection principle

56. For the sixth principle to be met, personal data must be processed in a manner ensuring appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage (all using appropriate technical or organisational measures).

57. Electronic information is processed within our secure network. Hard copy information is processed within our secure premises.

58. Our electronic systems and physical storage have appropriate access controls applied.

59. The systems we use to process personal data, including special category and criminal convictions etc. data, allow us to erase or update personal data at any point in time.

Retention

60. We have a corporate File Plan and Retention Schedule here.

General

61. This policy satisfies the requirements of Schedule 1, Part 4 of the DPA 2018 and is therefore an appropriate policy document in support of our compliance with the data protection principles in relation to special category and criminal convictions etc. data, in terms of that Part.

Review

62. This Safeguards Policy will be reviewed every two years or revised more frequently where necessary.

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and Status. *E.g. C5 Key Documents Handbook v01 CURRENT ISSUE*	C5 Data Protection Safeguards Policy: Appropriate policy document v01
VC FileId	126558
Type	Procedure
Approver	SMT
Responsible Manager	HOE and HOCS
Date of next planned review	October 2021
Approval & Publication	
Approval Date (major version)	16 October 2019
For publication *(Y/N)*	Y
Date published	08/11/19
Name of document in website file library	DataProtectionSafeguardsPolicy
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	

Summary of changes to document				
Date	**Action by** *(initials)*	**Version updated** *(e.g. v01.25-36)*	**New version number** *(e.g. v01.27, or 02.03)*	**Brief description** (*e.g. updated paras 1-8, updated HOPI to HOOM, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding*)
08/11/19	BOW	01.00	01.01	New document created following approval of draft
08/11/19	BOW	01.01	01.02	DCS updated, published on website

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info