Data Protection Policy and Handbook

Scottish Information Commissioner

Contents

Introduction **1**

Policy Statement **1**

Data Protection Act 2018 ..... **3**

Personal data 3

Special categories of personal data 3

Processing 3

Data Controller 4

Data Processor 4

Data Subject 4

Information Commissioner's Office (ICO) 4

The UK General Data Protection Regulation (UK GDPR) **4**

Lawful basis for processing **5**

Individual Rights **6**

Accountability **6**

Contracts 6

Documentation 7

Data protection by design and default 9

Data Protection Impact Assessments 11

Data Protection Officer 11

Security **12**

Breaches of personal data and data incidents **13**

International transfers **14**

Governance arrangements **14**

Senior Management Team (SMT) 14

The Head of Corporate Services (HOCS) 14

Finance and Administration Manager (FAM) ..... **Error! Bookmark not defined.**

All staff 15

Appendix 1: Data Protection Principles **16**

Appendix 2: Processing of personal data **18**

Why is the principle of lawful processing important? **18**

When is processing necessary? 19
How do we decide which lawful base to use? 19
Can we change our lawful basis? 20
How do we document our lawful basis? 20
Consent 20
Obtaining, recording and managing consent 21
Managing consent 21
Consent Records 22
Contract 23
Legal obligation 24
Vital interests 25
Public Task 26
Legitimate interests 27
Purpose test 28
Necessity test 28
Balancing test 29
Legitimate interests assessment (LIA) 29
New purpose 30
Individual rights 30
Special Category Data 30
The conditions for processing special category 31
Criminal convictions 33
Appendix 3 – Individual Rights 34
Right to be informed 34
Right of access (subject access requests) 34
Introduction 34
What are Subject Access Requests? 34
Receipt and allocation of SARs 35
Charging 36
“Validity” of SARs 37
Searching for personal data 38

Assessment of SARs 38
Exemptions 43
Timescales for responding to SARs 43
Responding to SARs 45
Right to rectification 45
Right to erasure ("right to be forgotten") 46
Right to restriction of processing 47
Right to object 48
Rights related to automated decision making and profiling 49
Appeals and complaints 49
Appendix 4 Data Processor Checks 50
Guidance when considering whether a data processor meets UK GDPR requirements 50
Follow up questions 51
Appendix 5 Data Protection Impact Assessments 52
Guidance when considering whether a full DPIA is needed 52
Full DPIA required 53
Appendix 6 Breaches of personal data and data incidents 55
Document control sheet 58

Glossary and abbreviations

Term used	Explanation
BSM	Business Support Manager
BST	Business Support Team
DHOE	Deputy Head of Enforcement
DIL	Data Incident Log
DIMP	Data Incident Management Plan
DO	Designated Officer
DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EEA	European Economic Area
EIRs	Environmental Information (Scotland) Regulations 2004
FOISA	Freedom of Information (Scotland) Act 2002
UK GDPR	UK General Data Protection Regulation (i.e. GDPR as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data (Use and Access) Act 2025

HOBS	Head of Business Support
HOE	Head of Enforcement
HOPI	Head of Policy and Information
ICO	(UK) Information Commissioner's Office
LIA	Legitimate Interests Assessment
SAR	Subject access request
Commissioner	The Scottish Information Commissioner, staff/office of the Commissioner depending on context
SMT	Senior Management Team
VC	Virtual Cabinet
WP	Workpro

Introduction

1. The Scottish Information Commissioner (SIC/the Commissioner) is the independent public official responsible for promoting and enforcing Scotland's freedom of information law:

    - The Freedom of Information (Scotland) Act 2002 (FOISA) - is an Act of the Scottish Parliament which gives everyone the right to ask for any information held by a Scottish public authority

    - The Environmental Information (Scotland) Regulations 2004 (the EIRs) – secondary legislation passed by the Scottish Parliament but based on a European Directive on access to environmental information. The EIRs give everyone the right to ask for environmental information held by a Scottish public authority (and some other bodies)

2. The main functions of the Commissioner are: investigating appeals, promoting the public's right to know, promoting good practice to public authorities and intervening when public authority practice is not compliant with freedom of information law.

3. The Commissioner can also receive applications about the view and discovery provisions of the INSPIRE (Scotland) Regulations 2009. These regulations also come from a European Directive and create a right to discover and view spatial datasets (e.g. map data) held by Scottish public authorities.

4. As part of the SIC's statutory functions, we can investigate (and report for prosecution) public authorities and their employees for offences committed under section 65 of FOISA and regulation 19 of the EIRs. The SIC is a competent authority for the purpose of Part 3 of the DPA 2018, which applies to the processing of personal data by such authorities for law enforcement purposes. For more information about what we do this data, see Privacy Notice: Investigations for Law Enforcement Purposes.

5. Under section 43F of the Employment Rights Act 1996, whistleblowers may qualify for employment protections if they disclose information to a "prescribed person". The list of prescribed persons is set out in the Schedule to the Public Interest Disclosure (Prescribed Persons) Order 2014. The Commissioner is a "prescribed person."

6. The DPA 2018 and the UK GDPR impose obligations on the processing of personal data held by the SIC and have implications for every part of the organisation.

7. This document sets out how the SIC complies with the DPA 2018 and the UK GDPR. The policy and the related procedures and guidance aim to ensure SIC meets the requirements of the DPA 2018 and the UK GDPR.

Policy Statement

8. As a data controller the SIC must collect and use certain types of information about individuals.

9. Most of the personal data we process is provided to us directly for one of the following reasons:

    - by an employee of SIC or by someone who has applied to work with the SIC

    - by an enquirer making an enquiry to the SIC

- by an applicant making an application (appeal) to the SIC
- by a representative of a Scottish public authority subject to FOI legislation
- by a person making an information request or subject access request to the SIC
- by a person indicating they wish to attend, or having attended, an event organised by the SIC.
- by a person subscribing to our email service
- by a complainant making a complaint to the SIC
- by a person making a whistleblowing complaint to the SIC
- by a person or company providing contracted services to the SIC

10. We may also receive personal information indirectly, in the following scenarios:

- we have contacted a Scottish public authority about an appeal made to SIC and it provides personal information about another person as part of the investigation
- an applicant provides personal information about another person in their application correspondence
- an applicant provides personal information about another person in their correspondence when making an information request or subject access request to the SIC
- a complainant provides personal information about another person in their complaint
- a person making a whistleblowing complaint provides personal information about another person in their reporting to us
- we have received personal information about another person from other public authorities, regulators or law enforcement bodies
- an employee of the SIC provides personal information about another person, for example contact details, emergency contact details or a referee

11. The SIC aims to ensure that all personal data is processed in a way that is lawful and correct in accordance with the DPA 2018 and the UK GDPR principles however it is collected, recorded and used, irrespective of its format and including for example paper copies, computer records, datasets and data held on applications and devices.

12. The SIC understands that privacy by design and the lawful and correct treatment of personal data is central to successful operations and to maintaining confidence between the SIC and those with whom we interact.

13. The SIC's Privacy Notice, which is regularly updated, provides comprehensive information regarding the personal data processing undertaken by the SIC.

14. Data protection relates to the fair and proper use of information about people.

15. The UK data protection regime is set out in the DPA 2018, together with the UK GDPR (which also forms part of UK law), and it takes a flexible, risk-based approach which puts the onus on data controllers and data processors to think about and justify how and why they use personal data. The Information Commissioner's Office (ICO) regulates data protection in the UK.

16. As a public authority, the DPA 2018 applies to all personal data held by SIC, both electronically and manually.

Personal data

17. Personal data is information that relates to an identified or identifiable individual.[1]

Special categories of personal data

18. Some of the personal data that is held and processed can be more sensitive in nature and requires a higher level of protection. The UK GDPR[2] refers to these types of data as 'special categories of personal data' which is personal data about an individual's:

- race
- ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data (where this is used for identification purposes)
- health
- sex life
- sexual orientation

19. Personal data can also include information relating to criminal convictions and offences[3]. This also requires a higher level of protection, as do personal data relating to children.

Processing

20. Almost anything we do with personal data counts as processing: including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

[1] UK GDPR Art.4(1); s3(2) of the DPA 2018
[2] UK GDPR Art.9
[3] Part 3 of the DPA 2018

Data Controller

21. A data controller is the person that decides how and why to collect and use the personal data.

22. The SIC is a data controller, as defined in Article 4(2) of the UK GDPR and the DPA. The SIC is obliged to ensure that all of the DPA and UK GPDR requirements are implemented to satisfy its duties. These duties will vary depending on whether the SIC is a data controller or data processor.

Data Processor

23. A data processor is a separate person or organisation (not an employee) who processes data on behalf of the data controller and in accordance with their instructions.

Data Subject

24. This is the legal term for the individual whom particular personal data is about. In this policy and handbook we generally refer to the data subject as an "individual".

Information Commissioner's Office (ICO)

25. The ICO is the supervisory authority for data protection in the UK and offers advice and guidance, promotes good practice, monitors breach reports, conducts audits and advisory visits, considers complaints, monitors compliance and takes enforcement action where appropriate.

26. The ICO also cooperates with data protection authorities in other countries.

The UK General Data Protection Regulation (UK GDPR)

27. The UK GDPR sets out seven key principles which must inform and be at the core of processing personal data.

28. The seven key principles[4] which must inform and lie at the heart of our processing of personal data are:

    (a) Lawfulness, fairness and transparency

    (b) Purpose limitation

    (c) Data minimisation

    (d) Accuracy

    (e) Storage limitation

    (f) Integrity and confidentiality

    (g) Accountability

[4] UK GDPR Article 5

29. The text of each of these principles is set out in full in **Appendix 1: Data Protection Principles.** Further guidance on how we comply with each principle is set out in **Appendix 2: Processing of personal data**

Lawful basis for processing

30. The SIC must have a valid lawful basis in order to process personal data and the lawful bases for processing are set out in UK GDPR[5]. At least one of these must apply whenever the SIC processes personal data:

    (a) **Consent:** the individual has given clear consent to the processing of their personal data for one or more specific purposes.

    (b) **Contract:** the processing is necessary for a contract with the individual, or because they have asked to take specific steps before entering into a contract.

    (c) **Legal obligation:** the processing is necessary to comply with the law (not including contractual obligations).

    (d) **Vital interests:** the processing is necessary to protect someone's life.

    (e) **Public task:** the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

    (f) **Legitimate interests:** the processing is necessary for the Commissioner's or a third party's legitimate interests, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks[6].)

    (g) **Special category data:** there are ten conditions for processing special category data in the UK GDPR itself, but the DPA 2018 introduces additional conditions and safeguards. At least one of these must be met for any such processing, in addition to at least one of conditions (a) to (f) above.

    (h) **Criminal offence data:** the UK GDPR rules for special category data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures[7].

31. The lawful basis must be determined before the processing of the personal data takes place and should be documented. A different lawful basis at a later date should not be used without good reason. Which basis is most appropriate to use will depend on the SIC's purpose and relationship with the individual and no single basis is better or more important than the others.

32. Most of the lawful bases require that processing is "necessary" for a specific purpose. (Here, "necessary" means "reasonably" rather than absolutely or strictly necessary.) If there is a reasonable way to achieve the same purpose without processing the personal data, generally, there will not be a lawful basis. If the purposes for processing the personal data change, it may be possible to continue processing under the original lawful basis if the new

[5] UK GDPR Article 6
[6] UK GDPR Article 6(1)
[7] UK GDPR Article 10

purpose is compatible with the initial purpose (compatibility is defined further in section 71 of the Data (Use and Access) Act 2025: consult HOE if this appears to be an issue). However, it is not usual to swap from consent to a different basis.

33. If special category data is being processed, both a lawful basis for general processing and an additional condition for processing this type of data need to be identified.

34. Further guidance on the lawful bases for processing personal data is provided in **Appendix 2: Processing of personal data.**

35. If we are processing criminal conviction data or data about offences we need to identify a condition for processing this type of data in Chapter 2 of Part 3 of the DPA 2018 – see our Safeguards Policy**.**

36. Our Privacy Notice includes the lawful basis for each type of personal data processing as well as the purposes of the processing.

Individual Rights

37. The UK GDPR provides the following rights for individuals as regards their personal data:

- right to be informed
- right of access
- right to rectification
- right to erasure
- right to restrict processing
- right to data portability
- right to object
- rights in relation to automated decision making and profiling.

Accountability

Contracts

38. Where SIC uses a data processor to process personal data on its behalf we must be satisfied that the contractor is taking adequate steps to allow the SIC to meet its obligations under the DPA 2018. Contracts between the SIC and data processors must ensure[8] that all necessary security procedures and other appropriate measures are specified in the contract, and the contract must be monitored to ensure that they are being adhered to.

39. The SIC must only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet UK GDPR requirements and protect data subjects' rights[9]. The detailed guidance on determining

[8] UK GDPR Art.28
[9] UK GDPR Art 28(1).

whether a data processor meets these requirements is set out in **Appendix 4 Data Processor Checks**.

40. The SIC has standard contract conditions, which should be used for contracts relating to goods and services. Where any contracts relate to the processing of personal data on the SIC's behalf the standard terms and conditions provide for the following:

- the data processor must only act on the controller's documented instructions, unless required by law to act without such instructions
- the data processor must ensure that any person processing the data is subject to a duty of confidence
- the data processor must take appropriate measures to ensure the security of processing
- the data processor must only engage a sub-processor with the SIC's prior authorisation and under a written contract
- the data processor must take appropriate measures to help the SIC, as data controller, to respond to requests from individuals to exercise their rights
- taking into account the nature of the data processing and the information available, the data processor must assist the SIC, as data controller, in meeting its UK GDPR obligations in relation to the security of data processing, the notification of personal data breaches and data protection impact assessments
- the data processor must delete or return all personal data to the SIC, as data controller, at the end of the contract, and the data processor must also delete existing personal data unless the law requires its storage
- the data processor must submit to audits and inspections
- the data processor must also give the SIC, as data controller, whatever information is needed to ensure they are both meeting their UK GDPR Article 28 obligations.

41. Where SIC's standard terms and conditions are not used for a contract for the processing of personal data on behalf of SIC, the contract relating to the data processing must contain provisions relating to the matters set out in paragraph **40** above.

Documentation

42. The UK GDPR contains explicit provisions about documenting our data processing activities and data controllers and data processors each have documentation obligations. We must maintain written records on matters such as data processing purposes, data sharing[10] and data retention.

43. When preparing for the implementation of the DPA 2018 and the UK GDPR we carried out an information audit to determine what personal data our organisation holds and where it is.

[10] If any such agreement is put in place it should comply with Data sharing: a code of practice issued by the ICO

44. Documenting our data processing activities is important, not only because it helps to meet our legal requirements but also because it supports good data governance and helps us to demonstrate our compliance with other aspects of the UK GDPR.

45. As we have fewer than 250 employees we are only legally required to document processing activities that:

- are likely to result in a risk to the rights and freedoms of individuals or
- are not occasional or
- involve the processing of special categories of data or criminal conviction and offence data.

46. Under Article 30 of the UK GDPR we document the following information:

- the name and contact details of our organisation and our DPO
- the purposes of our processing
- a description of the categories of individuals and categories of personal data
- the categories of the recipients of personal data
- details of our transfers to third countries including documenting the transfer mechanism safeguards in place
- retention schedules
- a description of our technical and organisational security measures

47. We also document the following information

- the information required for our Privacy Notice/s, such as:
  - the lawful basis for the processing
  - the legitimate interests for the processing
  - individuals' rights
  - the existence of automated decision-making, including profiling
  - the source of the personal data
  - retention periods
- records of consent
- our data controller-processor contracts
- the location of personal data
- Data Protection Impact Assessments
- records of personal data breaches

48. If we process special category or criminal conviction and offence data, we document ("appropriate policy document", or Safeguards Policy:

- the condition for processing we rely on in the DPA 2018;
- the lawful basis for our processing; and
- whether we retain and erase the personal data in accordance with our policy document.

49. We keep our records up to date and ensure that they reflect our current processing activities.

Data protection by design and default

50. The UK GDPR[11] requires us to put in place appropriate technical and organisational measures to implement data protection concerns in every aspect of our data processing activities. This is generally referred to as "data protection by design and by default". This recognises the importance of integrating data protection into our processing activities and business practices, from the design stage right through the lifecycle of the operation.

51. Data protection by design is about considering data protection and privacy issues upfront in everything we do and it helps ensure that we:

- comply with the UK GDPR's fundamental principles and requirements
- consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

52. Data protection by design covers many areas in our organisation, for example:

- the development of new IT systems, services, products and processes that involve processing personal data
- the development of organisational policies, processes, business practices and/or strategies that have privacy implications
- physical design of officers, storage, etc
- any data sharing initiatives we undertake[12]
- using personal data for new purposes.

53. Data protection by default requires us to ensure that we only process the personal data that is necessary to achieve our specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation and means we need to specify the personal data before the processing starts, appropriately inform individuals and only process the personal data we need for our purpose. When we are doing this we should:

- adopt a "privacy-first" approach with any default settings of systems and applications
- ensure we do not provide an illusory choice to individuals relating to the data we process

[11] UK GDPR Article 25

[12] If any such agreement is put in place it should comply with Data sharing: a code of practice issued by the ICO

- not process additional data unless the individual says we can (where we are relying on consent to process data)
- ensure that personal data is not automatically made publicly available to others unless the individual says that this can happen
- provide individuals with sufficient controls and options to exercise their rights
- ensure that any new processing of existing data is compatible (in line with Article 5(1)(b) of the UK GDPR and section 71 of the Data (Use and Access) Act 2025) with the purposes for which the data were collected.

54. The SIC, as data controller, has overall responsibility for complying with data protection by design and by default but there are different requirements and responsibilities in different areas for the organisation, for example:

- the Senior Management Team (SMT) ensures that policies and procedures are developed with data protection in mind
- our IT service providers take into account data protection requirements and assist us in complying with our obligations
- our business processes are designed to ensure that data protection is embedded into all our internal processes and procedures.

55. If we use another organisation to process personal data on our behalf, we ensure that that organisation can provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the UK GDPR and ensure the protection of the rights of the data subject[13] under the UK GDPR.

56. When considering what products and services we need for processing personal data, we consider whether the provider of the product or service has taken data protection into account.

57. As an organisation, and in order to ensure that we embed “privacy by design and default” into all that we do, we:

- consider data protection issues as part of the design and implementation of systems, services, products and business practices
- make data protection an essential component of the core functionality of our processing systems and services
- only process the personal data we need in relation to our purpose(s), and only use the personal data for that/those purpose(s)
- ensure personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy

[13] UK GDPR Article 25

- make sure the identity and contact information of those responsible for data protection are available both within the organisation and to individuals
- adopt a “plain language” policy for any public documents so that individuals easily understand what we are doing with their personal data
- provide individuals with the tools so they can determine how we are using their personal data, and whether we are properly enforcing our policies
- offer strong privacy defaults, user-friendly options and controls and respect user preferences.

58. A pre-Data Protection Impact Assessment (DPIA) check is carried out in respect of the design and implementation of systems, services, products and business practices which involve the processing of personal data. Where the pre-DPIA check indicates that it is needed, a full DPIA will be carried out to identify and reduce the data protection risks of our processing activities. See paragraphs **59** to **63** below and **Appendix 5 Data protection Impact Assessments.**

Data Protection Impact Assessments

59. The UK GDPR introduced an obligation to carry out a DPIA before carrying out types of processing likely to result in high risk to individuals’ rights and freedoms, particularly if new technologies are being used. If a DPIA identifies a high risk to individuals’ rights which we cannot mitigate we need to consult the ICO.

60. A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process.

61. We must also seek the advice of our DPO on all DPIAs and we will also consult with relevant individuals and other stakeholders throughout the process as required.

62. We will publish DPIAs where possible.

63. The detailed guidance on DPIAs is set out in **Appendix 5 Data protection Impact Assessments.**

Data Protection Officer

64. By law, we must have a DPO[14]. Our DPO does a number of things, including:

- giving us advice on data protection laws
- monitoring our compliance with data protection laws
- providing advice on DPIAs
- acting as our point of contact for our staff and the ICO

65. Our DPO is Robin Davidson.

66. These are the DPO’s contact details:
Scottish Parliament
Edinburgh

[14] UK GDPR Article 37

EH99 1SP
Telephone: 0131 348 5281
Email: dataprotection@parliament.scot

67. We have an agreement with our DPO. The agreement can be read here.

68. If there is a conflict of interest, Euan McCulloch, HOE, acts as our DPO.

Security

69. The UK GDPR requires us to process personal data securely. This is generally referred to as the "security principle". This security principle also needs to be considered alongside the other UK GDPR requirements relating to the security of our processing of personal data[15].

70. Under the security principle, every aspect of our processing of personal data is covered, not just cybersecurity. This means the security measures we have in place should seek to ensure that:

- the personal data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority given to them)
- the personal data we hold is accurate and complete in relation to why we are processing it, and
- the personal data remains accessible and usable, that is, if personal data is accidentally lost, altered or destroyed, we should be able to recover it and prevent any damage or distress to the individual/s concerned.

71. The UK GDPR does not define the security measures that we should have in place but it does require us to have a level of security that is 'appropriate' to the risks presented by our processing of personal data.

72. In preparing for the implementation of the DPA 2018 and the UK GDPR we assessed our information risk, reviewed the personal data we hold and the way we use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the personal data was compromised and took account of the following:

- the nature and extent of our organisation's premises and computer systems;
- the number of staff we have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on our behalf.

73. We have also considered our cybersecurity and have looked at:

- system security
- data security
- online security
- device security

[15] UK GDPR Art 32(1)

74. We are Cyber Essentials and Cyber Essentials Plus accredited and seek annual re-accreditations.

75. We regularly review, test, assess and evaluate the effectiveness of the security measures that we have in place

76. All staff understand the importance of protecting personal data, are familiar with our security measures and put our information security procedures into practice.

77. We provide appropriate initial and refresher training to all staff, including training on:

- the SIC's responsibilities as a data controller under the UK GDPR
- staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority
- the proper procedures to identify callers
- the dangers of people trying to obtain personal data by deception (e.g. by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks), or by persuading staff to alter information when they should not do so, and
- any restrictions placed on the personal use of our systems by staff (e.g. to avoid virus infection or spam).

Breaches of personal data and data incidents

78. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

79. As soon as we become aware of a personal data breach or personal data incident, we try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

80. Under the UK GDPR we are required to report certain types of personal data breach to the ICO and must do this within 72 hours of determining that a breach has occurred, where this is feasible.

81. If the personal data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we may also have to inform those individuals without undue delay.

82. The SIC is required to document the facts relating to any personal data breach, its effects and the remedial action taken. We will investigate whether or not the breach of personal data was as a result of human error or a systemic issue and see how a recurrence can be prevented, whether through better processes, further training or other corrective steps.

83. We record all personal data breaches, regardless of whether or not they need to be reported to the ICO.

84. If we need to notify an individual about a breach of personal data we will:

- describe, in clear and plain language, the nature of the personal data breach

- provide the name and contact details of our DPO
- provide a description of the likely consequences of the personal data breach
- provide a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

85. Detailed guidance on what to do if there is a breach of personal data or potential breach of data or data incident is set out in **Appendix 6 Breaches of personal data and data incidents.**

International transfers

86. The Data (Use and Access) Act 2025 makes new provision for international transfers of personal data, with regulations setting up new (UK-specific) adequacy arrangements. We will follow the ICO guidance in relation to transfers, and any processing involving a potential international transfer will be referred to the SMT for consideration and approval.

Governance arrangements

87. In order to comply with the DPA 2018, in addition to this Data Protection Policy, the SIC has business processes and systems which include:

- identifying a role with specific responsibility for data protection
- the provision and implementation of procedures for SIC staff on handling personal data
- training for all SIC staff in data protection and best practice
- the maintenance and application of retention and disposal schedules for all SIC records to ensure information is only retained for as long as it is required
- adherence to established information security procedures for both manual and electronic records, subject to appropriate risk assessment
- notification with the ICO of all uses of personal data within SIC
- an annual report on information and records management to the Senior Management Team

Senior Management Team (SMT)

88. The SMT has overall responsibility for the Data Protection Policy and Handbook.

89. The SMT is responsible for ensuring the Data Protection Policy and Handbook are followed and that staff competence is maintained and developed.

The Head of Enforcement (HOE)

90. The HOE is the Responsible Manager for the review and update of the Data Protection Policy and Handbook as necessary.

91. The HOE monitors compliance with the Data Protection Policy and Handbook, provides a quarterly update report to the SMT and provides assurance to the SMT that the Data Protection Policy and Handbook are being followed.

92. The HOE is the main point of contact with the DPO and keeps under review the log of all matters upon which advice is sought from the DPO or when the DPO is notified of a data incident. If the HOE is absent, the HOBS will be the main point of contact with the DPO.

Business Support Manager (BSM)

93. If a data incident takes place, the FAM (in consultation to the HOE, as required) has overall responsibility for coordinating the Data Incident Management Plan (DIMP) and, as required, reporting to and seeking the views of the SMT on any DIMP. The FAM will be the main point of contact if advice needs to be sought from the DPO on a DIMP.

94. The FAM has responsibility for ensuring that the Commissioner's[16] Data Protection Notification is kept up to date.

95. In cases where there is unlikely to be a significant data incident, the FAM will coordinate the DIMP.

All staff

96. All staff are required to be aware of the provisions of the DPA 2018 and the UK GDPR and their impact on the work SIC undertakes.

97. All staff must follow the guidance and procedures set out in the Data Protection Policy and Handbook.

[16] This is the annual notification provided to the ICO

Appendix 1: Data Protection Principles

98. Article 5 of the UK GDPR lists the data protection principles in the following terms. Personal data shall be:

    (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")

    (b) collected (whether from the data subject or otherwise) for specified, explicit and lawful purposes and not further processed by or on behalf of the controller in a manner that is incompatible with the purpose for which the controller collected the data ("purpose limitation")

    (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation")

    (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy")

    (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation")

    (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality") accordance with the rights of data subjects under [the DPA].

99. Article 5(2) requires that the controller shall be responsible for, and be able to demonstrate compliance with, the data protection principles ('accountability').

100. Compliance with the purpose limitation principle does not, by itself, make processing lawful. The legislation specifies certain purposes which are automatically compatible with the purpose for which the data are collected, for example, protecting public security, responding to emergencies, crime detection/prevention and complying with legal obligations.

101. In order to meet the data protection principles set out in the UK GDPR the SIC will:

- fully observe the conditions regarding the fair collection and use of personal data.
- meet its legal obligations to specify the purposes for which information is collected and used.
- collect and process personal data only to the extent that it is required to fulfil operational purposes or to comply with legal requirements.
- put in place adequate processes to ensure the quality of data.

- hold personal data on our systems only for the length of time necessary to fulfil our operational purposes and in line with our corporate records retention schedule.
- ensure all the rights of the individuals about whom we hold data can be fully exercised.
- take all appropriate technical and organisational security measures to safeguard personal data. Ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- ensure that personal data held by the Commissioner is not transferred to areas outside the EEA without appropriate safeguards.

Appendix 2: Processing of personal data

102. The SIC must have a valid lawful basis in order to process personal data and the lawful bases for processing are set out in UK GDPR[17]. At least one of these must apply whenever we process personal data (see paragraph **196** onwards for special category data and paragraph **204** onwards for criminal convictions data):

    - **Consent:** the individual has given clear consent to the processing of their personal data for one or more specific purposes.
    - **Contract:** the processing is necessary for a contract with the individual, or because they have asked to take specific steps before entering into a contract.
    - **Legal obligation:** the processing is necessary to comply with a legal obligation of the controller (not including contractual obligations).
    - **Vital interests:** the processing is necessary to protect someone's life.
    - **Public task:** the processing is necessary to perform a task of the controller in the public interest or for official functions of the controller, and the task or function has a clear basis in law.
    - **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
    - **Recognised legitimate interests:** the processing is necessary for the purposes of certain "recognised legitimate interests".

    (The last two points cannot apply if you are a public authority processing data to perform your official tasks.[18])

Why is the principle of lawful processing important?

103. The first principle requires us to process all personal data lawfully, fairly and in a transparent manner. If no lawful basis applies to our processing, our processing will be unlawful and in breach of the first principle.

104. Individuals also have the right to erase personal data which has been processed unlawfully.

105. The individual's right to be informed[19] requires us to provide people with information about our lawful basis for processing. This means we need to include these details in our privacy notice.

106. The lawful basis for our processing can also affect which rights are available to individuals.

[17] UK GDPR Article 6

[18] See section 38(5A) of FOISA and regulation 11(8) of the EIRs which allow Scottish public authority to rely on the legitimate interests condition in responding to information requests

[19] UK GDPR Articles 13 and 14

When is processing necessary?

107. Most of the lawful bases for processing depend on the processing being "necessary". Here, "necessary" means "reasonably" rather than absolutely or strictly necessary. It does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means, or by processing less data.

108. It is not enough to argue that processing is necessary because we have chosen to operate our business in a particular way. The question is whether the processing is objectively necessary for the stated purpose, not whether it is a necessary part of our chosen methods.

How do we decide which lawful basis to use?

109. This will depend on our specific purpose/s and the context of the personal data processing. When processing personal data, we need to think about why the data is to be processed and consider which lawful basis best fits the circumstances.

110. More than one basis may apply and if this is the case we should identify and document all of them from the start.

111. We cannot adopt a one-size-fits-all approach as no individual basis is considered as better, safer or more important than the any other basis and there is no hierarchy in the order of the list in the UK GDPR.

112. Several of the lawful bases relate to a particular specified purpose – a legal obligation, performing a contract with the individual, protecting someone's vital interests, or performing our public tasks. If we are processing for these purposes, then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

113. In other cases we are likely to have a choice between using legitimate interests or consent and, if so, we need to consider the wider context, including:

    - Who does the processing benefit?
    - Would individuals expect this processing to take place?
    - What is our relationship with the individual?
    - Are we in a position of power over them?
    - What is the impact of the processing on the individual?
    - Are they vulnerable?
    - Are some of the individuals concerned likely to object?
    - Are we able to stop the processing at any time on request?

114. We may prefer to consider legitimate interests as our lawful basis if we wish to keep control over the processing and take responsibility for demonstrating that it is in line with people's reasonable expectations and would not have an unwarranted impact on them. However, if we consider that individuals should be given full control over and responsibility for their data

(including the ability to change their mind as to whether it can continue to be processed), we may wish to consider relying on individuals' consent.

115. As we are a public authority for the purposes of the DPA 2018, the public task basis is more likely to be relevant to much of what we do. If we can demonstrate that the personal data processing is to perform our tasks as set down in UK law, then we are able to use the public task basis. However, if the personal data processing is for another basis we must consider what that other basis is.

Can we change our lawful basis?

116. If we find at a later date that the chosen basis is inappropriate, it may be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements. Therefore, it is important to thoroughly assess upfront which basis is appropriate and document this. It may be possible that more than one basis applies to the processing because we have more than one purpose, and if this is the case then we should make this clear from the start.

117. If there is a genuine change in circumstances or we have a new and unanticipated purpose which means there is a good reason to review our lawful basis and make a change, we need to inform the individual (subject to exceptions, for example, where doing so would involve disproportionate effort or would breach an obligation of confidentiality) and document the change.

How do we document our lawful basis?

118. The principle of accountability requires us to demonstrate that we are complying with the UK GDPR and have appropriate policies and processes in place. We need to be able to show that we have properly considered which lawful basis applies to each processing purpose and can justify our decision.

119. We keep a record of which basis we are relying on for each personal data processing purpose and reasons why this is the case in our **Personal Data Processing Register**[20] . This helps us to comply with our accountability obligations, and will also help us when writing privacy notices. We must ensure that we can demonstrate which lawful basis applies to the particular processing purpose.

Consent

120. Consent is one of the lawful bases for processing. Genuine consent should put individuals in control, build trust and engagement, and enhance our reputation. If we rely on an inappropriate or invalid consent this could destroy trust, harm our reputation and leave us open to enforcement action by the ICO.

121. When this is used as a lawful basis, the consent must be freely given, unambiguous and involve a clear affirmative action. The consent should be separate from other terms and conditions and should not generally be a precondition of signing up to any type of service. If we cannot offer a genuine choice, using consent as a lawful basis is not appropriate

[20] VC231878

122. We must keep clear records to demonstrate consent.

123. There is no set time limit for consent. How long it lasts will depend on the context. We should review and refresh consent as appropriate.

Obtaining, recording and managing consent

124. When relaying on consent as a lawful basis, our template consent forms must be used.

125. When using a consent form, the consent request must be prominent, concise, separate from other terms and conditions and easy to understand. It must also include:

- the name of our organisation
- the name of any third party controllers who will rely on the consent
- why we want the data
- what we will do with it; and
- a statement making it clear that individuals can withdraw consent at any time.

126. The data subject must be required to actively opt in. Pre-ticked boxes, opt-out boxes or other default settings must not be used.

127. Wherever possible, separate ("granular") options to consent to different purposes and different types of processing must be provided in the consent form.

128. If unsure about what to include (or not include) in a consent form, seek advice from your head of department or from the HOE.

Managing consent

Obtaining consent

129. Our data protection obligations don't end when we get consent and we need to keep all consents under review and refresh them if anything changes. For example:

- if our processing operations or purposes evolve, the original consent may not be specific or informed enough.
- if we have relied on parental consent, we may need to refresh consent more regularly as the data subject gets older and can consent for themselves.

130. If we are seeking consent to process personal data there must be a consent review process incorporated into the related business process. If we are in any doubt about whether the consent is still valid we should refresh it.

131. We also need to consider whether to automatically refresh consent at appropriate intervals. How often depends on the particular context, including people's expectations, whether we are in regular contact with the data subject and how disruptive repeated consent requests would be to the data subject. The ICO recommends that we consider refreshing consent every two years, but we may be able to justify a longer period, or need to refresh more regularly, to ensure good levels of trust and engagement.

132. Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

Withdrawing consent

133. The UK GDPR[21] gives people a specific right to withdraw their consent and we need to ensure that we have proper withdrawal procedures in place to record this and to ensure that processing no longer takes place.

134. The data subject has right to withdraw consent "at any time" and it is not enough to provide an opt-out only by reply. The data subject must be able to opt out at any time they choose and on their own initiative.

135. It must also be as easy to withdraw consent as it was to give it. This means the process of withdrawing consent should be an easily accessible one-step process. If possible, data subjects should be able to withdraw their consent using the same method as when they gave it.

Consent Records

136. We must have an effective audit trail of how and when consent was given, so we can provide evidence if challenged. Good records also help us to monitor and refresh consent as appropriate. The records of consent need to be kept for as long as we are still processing based on the consent, so that we can demonstrate our compliance in line with our accountability obligations.

137. Our records[22] must show the following:

- **who consented**
    - the name of the data subject, or other identifier (e.g., online user name, session ID)
- **when they consented**
    - a copy of a dated document
    - online record that include a timestamp
    - for oral consent - a note of the time and date which was made at the time of the conversation.
- **what they were told at the time**
    - a master copy of the document or data capture form containing the consent statement in use at that time, along with the privacy notice or other privacy information, including version numbers and dates matching the date consent was given.
    - if consent is given orally, a copy of the script used at that time.
- **how they consented**
    - for written consent, a copy of the relevant document or data capture form.

---

[21] UK GDPR Article 7(3)

[22] At present, these records are kept in VC - there must be an adequate record of times and review periods and these procedures are being worked on and guidance will be included in this guidance. In the meantime, if you have any questions about this please speak to your HOD or the HOE.

- if consent is given online, our records should include the data submitted as well as a timestamp to link it to the relevant version of the data capture form.
- if consent is given orally, we should keep a note of this made at the time of the conversation; however, it does not need to include the full record of the conversation.

- **whether they have withdrawn consent:**
  - if so, details of when and how.

138. The ICO provides detailed guidance on consent which can be found on their website.

Contract

139. This lawful basis can be relied on where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract[23].

140. "Necessary" in this context does not mean that the processing must be absolutely essential or the only way to perform the contract or take relevant pre-contractual steps. Here, "necessary" means "reasonably" rather than absolutely or strictly necessary. However, it must be:

- more than just useful, and more than just part of our standard contractual terms
- a targeted and proportionate step which is integral to delivering the contractual service or taking the requested action - this lawful basis does not apply if there are other reasonable and less intrusive ways to deliver the contractual service or take the steps requested
- necessary to perform the contract with this particular person - if the processing is instead necessary to maintain our business model more generally, or is included in our terms for other business purposes beyond delivering the contractual service, this lawful basis will not apply and we will need to consider another lawful basis, such as legitimate interests.

141. We can use this lawful basis for processing personal data if:

- we have a contract with the data subject and we need to process their personal data to comply with our obligations under the contract
- we have a contract with the data subject and we need to process their personal data so that we can comply with specific counter-obligations under the contract (for example, we are processing payment details)
- we haven't yet entered into a contract with the data subject, but we have asked them to do something as a first step (for example, provide a quote) and we need to process their personal data to do this. This applies even if we don't actually go on to enter into a contract with the data subject, as long as the processing was in the context of a potential contract with that data subject.

[23] UK GDPR Article 6(1)(b)

142. We cannot use this lawful basis for processing data when:

- we need to process one person's details but the contract is with someone else
- we collect and reuse the data subject's personal data for our own business purposes (distinct from the purposes of the contract), even if this is permitted under the related contractual terms
- we take pre-contractual steps on our own initiative, to meet other obligations, or at the request of a third party.

143. If processing of special category data is necessary for a contract, we also need to identify a separate condition for processing this data – see paragraphs **196** to **203**.

144. If the contract is with a data subject under 16, we need to consider whether they have the necessary capacity to enter into the contract. Children under 16 are taken to have capacity where they have a general understanding of what entering into the contract means. Children aged 12 or over are presumed to be of sufficient age and maturity to have such an understanding, unless the contrary is shown.[24]

145. If we have doubts about their competence, we may wish to consider an alternative basis such as legitimate interests, which can help us to demonstrate that the child's rights and interests are properly considered and protected.

146. If we are processing on the basis of contract, the individual's right to object and right not to be subject to a decision based solely on automated processing will not apply. However, the individual will have a right to data portability – see the Section on individual rights.

147. All processing of personal data on this basis must be documented to include information about the purposes relied on and the lawful basis. The relevant information must also be included in our Privacy Notice: https://www.foi.scot/privacy-notice.

Legal obligation

148. This provides a lawful basis for processing personal data where the processing is necessary for compliance with a legal obligation to which the data controller is subject[25], that is, when we are obliged to process the personal data to comply with the law.

149. The legal obligation must be laid down by domestic (UK) law[26] and can include a common law obligation. This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that the overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

150. The personal data processing must be necessary. Here, "necessary" means "reasonably" rather than absolutely or strictly necessary. If we can reasonably comply without processing the personal data, this basis does not apply. It is likely to be clear from the law in question whether the processing is actually necessary for compliance.

---

[24] Section 208 of the DPA 2018

[25] UK GDPR Article 6(1)(c)

[26] UK GDPR Article 6(3) - Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it and, therefore, it includes clear common law obligations.

151. We must document any decision to rely on this lawful basis and this needs to include:

- our reasoning and justification as to why this lawful basis should relied on
- the specific legal provision that clearly sets out our obligation
- include relevant details in the Privacy Notice (if required) – seek advice on this from HOCS or HOE

152. This lawful basis does not apply to contractual obligations as contractual obligations do not comprise a legal obligation in this context.

153. If we are processing on the basis of legal obligation, the data subject has no right to erasure, right to data portability, or right to object – see the Section on Individual Rights.

Vital interests

154. There is a lawful basis for processing where processing in necessary to protect the vital interests of the data subject or of another natural person[27]. Here, "necessary" means "reasonably" rather than absolutely or strictly necessary. The UK GDPR provides further guidance on this and states that the processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest for another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis[28].

155. The lawful basis for vital interests is very similar to the old condition for processing in the DPA 1998[29]. However, one key difference is that anyone's vital interests can now provide a basis for processing, not just those of the data subject themselves. (Although no longer directly applicable, in the UK, it is clear from Recital 46 to the GDPR that vital interests are intended to cover only interests that are essential for someone's life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death.)

156. In most cases, the protection of vital interests is likely to arise in the context of health data. As health data is one of the special categories of data, this means we will also need to identify a condition for processing special category data - see paragraphs **204** to **211**. We cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

157. We have reviewed our existing personal data processing to identify if we have any ongoing processing for this reason, or are likely to need to process for this reason in future. If we use this as a lawful basis we will need to document this basis and inform individuals if relevant. You must seek guidance from the HOE or a DHOE or the HOCS is you intend to use this as lawful basis for processing personal data before you do this.

[27] UK GDPR Article 6(1)(d)
[28] GDRP Recital 46
[29] DPA 1998 Schedule 2, Paragraph

Public Task

158. We can rely on this lawful basis to process personal data

- in the exercise of official authority - this covers public functions and powers that are set out in law, or
- to perform a specific task in the public interest that is set out in law[30].

159. The public task basis is similar to the old condition for processing for functions of a public nature in of the DPA 1998[31]. However, the relevant task or function must now have a clear basis in domestic (UK) law[32]. This will most often be a statutory function. The UK GDPR also clarifies that this does not have to be an explicit statutory provision, as long as the application of the law is clear and foreseeable[33]. This means that it includes clear common law tasks, functions or powers as well as those set out in statute or statutory guidance. The overall purpose must be to perform a public interest task or exercise official authority and that overall task or authority has a sufficiently clear basis in law.

160. The ICO uses the term “public task” to help describe and label this lawful basis. However, this is not a term used in the UK GDPR and is not the same as that referred to in the test used in the Re-use of Public Sector Regulations 2015

161. The DPA 2018[34] provides some examples of when the public task basis will cover personal data processing:

- the administration of justice
- parliamentary functions
- statutory functions
- governmental functions or
- activities that support or promote democratic engagement.

162. The above list is not an exhaustive list and we do not need a specific legal authority for the particular processing activity. However, the underlying task, function or power must have a clear basis in law. If there are other official non-statutory functions or public interest tasks, the public task basis can be relied on as long as the underlying legal basis for that function or task is clear and foreseeable.

163. The UK GDPR also makes it clear that public authorities can no longer rely on legitimate interests for personal data processing carried out in performance of their tasks[35]. Therefore, as a public authority, we need to consider the public task basis for more of our personal data processing.

---

[30] UK GDPR Article 6(1)(e)
[31] DPA 1998 Schedule 2
[32] UK GDPR Article 6(3)
[33] UK GDPR Recital 41
[34] DPA 2018 Section 8
[35] See section 38(5A) of FOISA and regulation 11(8) of the EIRs which allow Scottish public authorities to rely on legitimate interests in responding to information requests

164. As the Commissioner is a public authority (as defined in the DPA 2018), our ability to rely on consent or legitimate interests as an alternative basis is more limited, but the legitimate interests basis is still available for processing which falls outside our tasks as a public authority or for responding to requests under FOISA and the EIRs - and other lawful bases may also be relevant.

165. If we can show we are exercising official authority (including using discretionary powers), there is no additional public interest test. However, we must be able to demonstrate that the processing is "necessary" for that purpose. "Necessary" means that the processing must be a targeted and proportionate way of achieving our purpose.

166. The public task basis cannot be relied on as a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.

167. When we rely on this basis to process personal data we must document the following:

- the clear base either in statute or common law for the relevant task, function or power for which we are using the personal data
- update our Privacy Notice (if necessary) to show the lawful basis
- record that we have communicated this to the data subject/s

168. If we are processing special category data, we also need to identify an additional condition for processing this type of data – [see paragraphs **204** to **211** for guidance on this]

169. Individuals' rights to erasure and data portability do not apply if we are processing on the basis of public task. However, individuals do have a right to object. See our guidance on individual rights for more information.

170. If we originally processed personal data for a relevant task or function, we do not need a separate lawful basis for any further processing for:

- archiving purposes in the public interest
- scientific research purposes
- statistical purposes.

Legitimate interests

171. There is a lawful basis for personal data processing where processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child[36].

172. Public authorities (as defined in the DPA 2018) can only rely on legitimate interests if they are processing for a legitimate reason *other than performing their tasks as a public authority*.

173. Legitimate interests is considered the most flexible lawful basis for processing but, given the restriction set out in the previous paragraph, there are unlikely to be many circumstances in which it is relevant to us. However, section 38 of FOISA (Personal information) and

[36] UK GDPR Article 6(1)

regulation 11 of the EIRs (Personal data) were amended by the DPA 2018 to allow Scottish public authorities to rely on legitimate interests in responding to information requests. Guidance issued by the Commissioner on section 38 and regulation 11 recognises that, when responding to requests under FOISA or the EIRs, "legitimate interests" is likely to be the only lawful basis on which personal data can be disclosed.[37]

174. This basis is likely to be most appropriate where we use people's data in ways they would reasonably expect and which have a minimal privacy impact or where there is a compelling justification for the processing. If we choose to rely on legitimate interests, we are taking on extra responsibility for considering and protecting people's rights and interests.

- the UK GDPR is clearer that we must give particular weight to protecting children's data.
- the biggest change is that we need to document our decisions on legitimate interests so that we can demonstrate compliance under the new UK GDPR accountability principle
- we must include more information in our privacy information.

175. There are three elements to the legitimate interests basis this forms a three part test. If we seek to rely on this basis for processing personal data we need to:

- purpose test – are we pursuing a legitimate interest?
- necessity test – is the processing necessary for that purpose?
- balancing test – do the individual's interests, rights and freedoms override the legitimate interest?

Purpose test

176. The legitimate interests can be our own interests or the interests of third parties and can include commercial interests, individual interests or broader societal benefits (the latter are particularly relevant when responding to requests under FOISA or the EIRs). They need not be compelling, but less compelling interests are more likely to be overridden in the balancing test.

Necessity test

177. The processing must be necessary. Here, "necessary" means "reasonably" rather than absolutely or strictly necessary. Processing must therefore be a targeted and proportionate way of achieving our purpose. If we can reasonably achieve the same result in another, less intrusive way, legitimate interests will not apply.

178. We can consider legitimate interests for processing children's data but must take extra care to make sure their interests are protected. If children's data is to be processed relying on this basis, guidance must be sought from the HOE before any processing takes place. The ICO also has detailed guidance on Children and the UK GDPR which should be taken into account in the processing of any children's data.

[37] https://www.foi.scot/briefings-and-guidance.

179. We may be able to rely on legitimate interests in order to lawfully disclose personal data to a third party, but if we do this we should consider:

- why they want the information
- whether they actually need it and
- what they will do with it.

180. We will need to demonstrate that the disclosure is justified. However, it will be the responsibility of the third party to determine their lawful basis for their own processing. If you intend to disclose personal data to a third party relying on this basis, guidance must be sought from the HOE before doing so.

Balancing test

181. We must balance the interests (this could be our, or a third party's interest – see paragraph 176) against the individual's interests. In particular, if they would not reasonably expect their data to be used in the proposed way, or it would cause them unwarranted harm, their interests may override the interests in disclosure (this depends on what the legitimate interest is and how weighty it is). However, the legitimate interest in disclosure does not always have to align with the individual's interests. If there is a conflict, the legitimate interests can still prevail as long as there is a clear justification for the impact on the individual.

182. Recital (47) of the GDPR made it clear that much will depend on the reasonable expectations of the data subjects. We should therefore avoid legitimate interests as a basis for processing personal data if we are using personal data in ways people do not understand or would object to, or where processing could cause harm, unless we are confident that there is nevertheless a compelling reason to go ahead

183. If we are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests is unlikely to be the most appropriate basis for processing which is unexpected or high risk although, as noted above, it is likely to be the appropriate basis to consider when responding to a request for third party personal data under FOISA or the EIRs.

Legitimate interests assessment (LIA)

184. Where we are intending to rely on this basis to process personal data, we need to carry out a LIA. We have a LIA template[38] which must be completed before any personal data processing relying on this basis is carried out.

185. Where the processing is ongoing, the LIA must be kept under review and refreshed if there is a significant change in the purpose, nature or context of the processing (as opposed to the more likely "one off" disclosure when personal data are being disclosed in response to an FOI request).

[38] See VC146968

186. An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help us ensure that our personal data processing is lawful. In some cases an LIA will be quite short, but in others there will be more to consider.

187. Once the LIA has been completed, the HOE will make a decision as to whether legitimate interests is an appropriate basis. It is likely that this will mostly happen where third party data is being disclosed in response to a request for information, and in such a case the HOE or a DHOE will need to approve the use of legitimate interests in such circumstances.

188. A record of the LIA and the outcome must be filed in VC/WP as appropriate.

189. If a LIA identifies significant risks, we may need to do a DPIA to assess the risk and potential mitigation in more detail (assuming legitimate interests is still considered a potentially suitable basis).

190. Where we rely on this basis to process personal data, details of our legitimate interests must be included in the Privacy Notice.

New purpose

191. If we want to process the personal data for a new purpose, we may be able to continue processing under legitimate interests as long as the new purpose is compatible with our original purpose. However, a new LIA should still be conducted, as this will help us demonstrate compatibility.

Individual rights

192. If we rely on legitimate interests, the right to data portability does not apply.

193. If we rely on legitimate interests for direct marketing, the right to object is absolute and we must stop processing when someone objects. For other purposes, we must stop unless we can show that our legitimate interests are compelling enough to override the individual's rights. (See **Appendix 3 – Individual Rights**.)

Special Category Data

194. Special category data are personal data which the UK GDPR says are more sensitive, and so need more protection as processing this type of data could create more significant risks to a person's fundamental rights and freedoms by putting them at risk of unlawful discrimination. It relates to information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health

- sex life
- sexual orientation.

195. The UK GDPR does not include personal data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of data[39] (see paragraphs **204** to **207**).

196. There are ten conditions for processing special category data in the UK GDPR itself. The conditions for processing special category data under the UK GDPR in the UK are broadly similar to the Schedule 3 conditions under the DPA 1998 for the processing of sensitive personal data but the DPA 2018 introduces additional conditions and safeguards[40].

197. If we process special category data

- we must identify both a lawful basis[41] and
- a separate condition for processing special category data[42]

198. The choice of lawful basis does not dictate which special category condition must apply and vice versa. We should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example:

- if consent is the lawful basis, we are not restricted to using explicit consent for special category processing
- if the lawful basis is vital interests, it is highly likely that the condition for vital interests will also be appropriate.

The conditions for processing special category[43]

199. Special category personal data can only be processed if one or more of the following applies:

(a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes (note there will be some circumstances where even explicit consent is not a sufficient ground for processing)

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment and social security and social protection law** in so far it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject

(c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

---

[39] UK GDPR Article 10
[40] This will be updated/revised when the relevant ICO guidance on this is published
[41] UK GDPR Article 6
[42] UK GDPR Article 9
[43] UK GDPR Article 9(2)

(d) processing is carried out in the course of a foundation's, association's or other not-for-profit's body's **legitimate activities**, provided the processing is carried out with appropriate safeguards; the body has a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

(e) processing relates to personal data which are **manifestly made public** by the data subject

(f) processing is necessary for the establishment, exercise or defence of **legal claims** or whenever courts are acting in their judicial capacity

(g) processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of **health or social care** or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards set out in Article 9(3)

(i) processing is necessary for reasons of public interest in the area of **public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

(j) processing is necessary for **archiving purposes** in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

200. The above conditions need to read alongside the DPA 2018, which adds a wide range of more specific conditions and safeguards[44]:

- Schedule 1 Part 1 contains specific conditions for the various employment, health and research purposes under Articles 9(2)(b), (h), (i) and (j).
- Schedule 1 Part 2 contains specific "substantial public interest" conditions for Article 9(2)(g).

201. In some cases we must also have an "appropriate policy document" in place to rely on these conditions. See our Data Protection Safeguards Policy.

[44] The ICO is working on more detailed guidance in this area this will be updated in due course

Criminal convictions

202. The UK GDPR does not apply to information about criminal allegations, proceedings or convictions. The rules for processing this type of data are set out in Article 10 of the GDPR, which provides that processing shall be carried out only under the control of official authority or as authorised by domestic law (in practice, this means that a condition in Part 1, 2 or 3 of Schedule 1 to the DPA 2018 must be met).

203. Criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under the DPA 1998. However, it also extends to personal data linked to related security measures.

204. In addition, the Commissioner is a "competent authority" for the purposes of Part 3 of the DPA 2018 in relation to personal data processed in relation to the investigation of offences under section 65 of FOISA and regulation 19 of the EIRs.

205. We have issued specific guidance on this: Investigations for law enforcement purposes and we also have a Data Protection Safeguards Policy .

Appendix 3 – Individual Rights

Right to be informed

206. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

207. We must provide individuals with privacy information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with.

208. Privacy information must be provided to individuals at the time their personal data is collected from them.

209. If we obtain personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

210. There are a few circumstances when we do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

211. The information we provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

212. We must regularly review, and where necessary, update our privacy information.

213. We must bring any new uses of an individual's personal data to their attention before we start processing the personal data.

Right of access (subject access requests)

Introduction

214. Administratively, subject access requests will generally be processed in the same way as FOISA and EIRs requests. To avoid repetition, administrative guidance (opening files, searching for information, etc.) is not reproduced in this section, but references are made to other relevant guidance in this document.[45]

215. Those dealing with subject access requests must also take account of the ICO's UK GDPR guidance on the right of access.

What are Subject Access Requests?

216. Subject access requests (SARs) are requests to the Commissioner for information about (and identifying) a living person, made by that person. They are governed by Article 15 of the UK GDPR. Individuals the right to obtain the following:

- confirmation that we are processing their data
- a copy of their personal data and

[45] Following the review of RFI procedures there will be separate procedures for SARs.

- other supplementary information

217. If the request relates to our law enforcement purposes, the SAR will be governed by section 45 of the DPA 2018.

218. We must take reasonable steps to make sure that the person making the SAR is who they say they are and need to be satisfied as to the identity of the requester (or the person the request is made on behalf of) and further guidance on this is set out below. The timescale for responding to a SAR does not begin until we have received the requested information. Any request for ID documents should be made promptly.

219. In some cases, a SAR may be made by a third party, e.g.

    - by a parent on behalf of a young child (a child aged 12 or over is presumed to be of sufficient age and maturity to make a SAR on their own behalf)
    - by a representative on behalf of an adult with incapacity
    - by a solicitor on behalf of a client.

220. If someone is making a request on behalf of a third party before responding, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual**.**It is the third party's responsibility to provide us with evidence that they are entitled to act on behalf of the individual, for example by providing us with written authority, signed by the individual, stating that they give the third party permission to make a SAR on their behalf. Seek advice from the HOE/DHOE if you are uncertain whether a third party has the necessary authority.

221. If the third party does not have the authority to make the subject access request, their request should be treated as a request for third party personal information under FOISA or the EIRs and responded to in accordance with the RFI procedures.

222. Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. Generally, a child aged 12 or over is presumed to be of sufficient age and maturity to make a SAR on their own behalf. If the request is from a child and you are confident they can understand their rights, you should usually respond directly to the child. You may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

Receipt and allocation of SARs

Receipt

223. All SARs made by:

    - a current employee or by someone acting on behalf of a current employee
    - an ex-employee or by someone acting on behalf of an ex-employee
    - (provided the SAR relates to their application) anyone who has applied for a job with the Commissioner

    must be passed to the HOBS immediately. In the case of HOBS' absence or conflict of interest, the SAR will be passed to the HOPI for response.

224. All SARs made under section 45 of the DPA 2018 (law enforcement) must be passed to the HOE. In the case of HOE's absence or conflict of interest, the SAR will be passed to the Commissioner for response.

225. In all other cases, SARs must be passed to the BST immediately. The BST will create the case records (WorkPro and hard copy). Guidance on creating case records can be found in Responding to Information Requests: Guidance and Procedures.

226. All references to "HOE" in what follows should be taken to be a reference to "HOBS", "HOPI" or "the Commissioner" (as appropriate) for the cases referred in paragraphs **225** and **226**.

Allocation

227. After the case has been created, it will be passed immediately to the HOE (or DHOE in the HOE's absence) for allocation in line with guidance set out in the "responding to Information Requests: Guidance and Procedure which can be found on our website.

228. The HOE will allocate the case to the designated officer (DO).

Charging

229. We can charge a reasonable fee for complying with a SAR, but only where:

- the request is manifestly unfounded or excessive; or
- an individual requests further copies of their data following a request

230. Our general policy is not to charge. A charge may be made in either of the above circumstances, with the agreement of the Commissioner (or, in the Commissioner's absence, the HOE). When seeking agreement, it is important to state why a charge is considered appropriate in the circumstances (if the requests are considered manifestly unreasonable or unfounded, we must give the requester reasons for our decision).

231. When determining a reasonable fee, we can take into account the administrative costs of:

- staff time assessing whether we are processing the information
- locating, retrieving and extracting the information
- providing a copy of the information (e.g. cost of photocopying, printing, USB devices) and
- communicating the response to the individual (e.g. postage), including contacting the individual to inform them that we hold the information (even if we are not providing the information).

232. There is likely to be some overlap between these activities, so it is important not to "double-charge." A file note stating the reasons why a charge is being made, how the charge has been calculated and who has authorised the charge, must be included in the file.

233. There are specific provisions providing for access to "manual unstructured data" the SIC holds. If the data requested fall into this category, we are under no obligation to comply with the request where the cost of doing so exceeds £450. We are also under no obligation to comply unless the requester provides a description of the manual unstructured data they are seeking.

234. This issue is unlikely to arise in practice: basically, “manual unstructured data” are manual records which are not structured by reference to individuals or to criteria relating to individuals. We are likely to hold information in that form only where it is of exceptional sensitivity, in which case it is likely to be exempt from disclosure: any cases which appear to involve unstructured personal data should be discussed with the HOE (DHOE). (Note that the right to make a SAR under section 45 of the DPA 2018 does not extend to manual unstructured data.)

“Validity” of SARs

Format of SARs

235. A SAR does not have to mention the UK GDPR/DPA 2018. The requester might just ask for access to personal data/information/files/records relating to them.

236. There is no requirement that a SAR must be made in writing, although we will generally need documentary evidence of the data subject’s identity (see below). Requests can be made by email, fax, etc., as well as orally (although evidence of an oral request may be helpful, for example writing it down and sending a copy to the requester to confirm what they are looking for, particularly if the request is complex).

237. Depending on how it is framed, a SAR may also be an information request under FOISA or the EIRs: if it is, it should be refused as such under section 38(1)(a)/regulation 11(1), before going on to respond to the SAR. Remember that the timescales for responding are likely to be different for responding under FOISA/the EIRs and the UK GDPR/DPA 2018.

Making reasonable adjustments for disabled people

238. A person may have a disability and may find it difficult to communicate and, therefore, have difficulty making a SAR. Under the Equality Act 2010, the Commissioner has a duty to make reasonable adjustments. If the request is complex, it would be good practice to document it in an accessible format and send it to the person to confirm the details of the request.

239. We may also have to respond in a format which is accessible to a person who has a disability, for example, Braille, large print, email or audio formats. If this is needed, refer the matter to the HOCS for advice.

Verifying the identity of the Requester

240. It is important that the DO is satisfied as to the identity of the requester. Disclosure to the wrong person may have serious consequences. While we can ask for information to determine whether the requester (or the person the request is made on behalf of) is the person the data is about, we must be reasonable and proportionate about what we ask for. If the requester’s identity is obvious to us, or we have an ongoing relationship with the requester, it would not be reasonable and proportionate for us to ask, for example, for a copy of a utility bill or driving licence. The level of checks that can be made are also likely to depend on the possible harm and distress inappropriate disclosure could cause to the individual concerned.

241. The DO, taking guidance from the HOE (DHOE), will check the request to ensure that all of the necessary information has been provided to confirm the identification of the requester (and the location of the personal data).

Clarifying the request

242. In limited circumstances, we can ask the requester to clarify the information or processing activities their request relates to before responding to the request. However, clarification can only be sought where it is reasonably required (examples may be where we can't identify the data readily without clarification, or where we process a large amount of information about an individual/the request appears excessive and there may be potential for reducing its scope). (See paragraph 280 below regarding the impact of seeking clarification on the time for responding.)

243. Individuals are entitled to all the information we hold about them (subject to exemptions, etc.), so clarification should not be used to try to force the requester to narrow the scope of their request.

Acknowledging the request

244. The timescale for responding to a request will not begin until we have, where necessary, received proof of identity and we are clear what is being asked for. If we have all the information we need, the DO will issue letter **SAR01.**

245. Where further information is required, the DO will issue letter **SAR02**. This must be done as soon as possible.

246. As noted above, where a third party has made a SAR on behalf of another person, in addition to verifying the requester's identity, it is important to check that they have the authority to make the SAR. Use standard letter **SAR03**.

Searching for personal data

247. The UK GDPR places an expectation on us to provide information in response to a SAR. The DO should therefore make reasonable and proportionate efforts to find and retrieve the requested information.

248. The DO will initiate the search for the personal data, in line with guidance on searching in the guidance on Responding to Information Requests: Guidance and Procedures which can be found here**.**

249. The information to be provided in response to a SAR is the information we hold when the SAR is received (unless routine use of the data has resulted in it being amended or even deleted while the SAR is being dealt with). However, no amendments or deletions should be made to the information if we would not otherwise have made them: under the DPA 2018, it is an offence to amend personal data with the intention of preventing it being disclosed.

Assessment of SARs

Information to be provided

250. Under Article 15 of the UK GDPR, an individual is entitled to the following information:

- confirmation of whether the Commissioner (or a data processor on behalf of the Commissioner) is processing their personal data
- if their personal data are being processed by the Commissioner, a description of:
  - (a) the category or categories of personal data being processed
  - (b) the purposes for which the personal data are being or will be processed

(c) any recipients or classes of recipients to whom the personal data are or will be disclosed (basically, any person or organisation who is likely to receive the personal data in the course of processing, but not any person or organisation, for example, - the police or other law enforcement agency, who might obtain the data in pursuance of a statutory right

(d) the period for which the Commissioner intends to retain the data (or, where that is not possible, the criteria used to determine that period) – if in doubt, check the File Plan and Retention Schedule.

(e) the source of the personal data, where available and where the source is not the data subject

(f) the logic involved in any automated decision-making about the requester (highly unlikely to arise in relation to personal data held by the Commissioner)

(g) where personal data are being processed for law enforcement purposes (e.g. for the purposes of investigating whether an offence has been committed under section 65 of FOISA), the legal basis for processing. Such cases will always be dealt with by the HOE.

- if their personal data is/are being processed, information about exercising the following rights:

  (a) rectification (Article 16 of the UK GDPR)

  (b) erasure (Article 17)

  (c) restriction of processing (Article 18)

  (d) the right to object (Article 21)

  (e) the right to complain to the ICO (section 165 of the DPA 2018)

- a copy of any personal data being processed.

251. When describing the personal data, the purposes and the recipients, it is sufficient to refer to general categories rather than being any more specific. The personal data must be provided in an understandable, clear and easily accessible form. This must be a permanent form, generally in writing, unless the requester agrees otherwise: we should approach SARs on the basis that the data (and any other information to be provided to the requester) will be provided in permanent form. The data can be provided electronically, and should be (in a commonly used form) where the request has been made electronically, unless the requester specifically asks to be responded to in another form.

252. Any other information to be provided in accordance with paragraph 259 should be provided in an understandable, clear and easily accessible form, using plain language. Particular attention should be paid to this when responding to a child. (Remember also the SIC's duties under the Equality Act 2010.)

253. If the personal data contain codes or indicators which can only be understood by reference to a key, or if they contain abbreviations, technical terms or jargon, an explanation of these should be provided to the requester.

254. The requester is entitled to their personal data, as defined in Article 4(1) of the UK GDPR/section 3(1) of the DPA 2018. This means they will not necessarily be entitled to all of the information the Commissioner holds.

255. Where you are unsure whether information constitutes personal data, consider the relevant guidance issued by the ICO, particularly:

- What is personal data?
- Access to information held in complaint files

256. Any remaining questions should be discussed with the HOE (DHOE) or the HOCS (as appropriate).

257. Reasonable care must be taken to secure any information covered by a SAR against destruction between the time the SAR is received and the time it is responded to. (Under section 173 of the DPA 2018, it is a criminal offence to alter, deface, block, erase, destroy or conceal personal data with the intention of it being disclosed.) On receipt of a SAR, it is good practice to alert colleagues who are likely to hold personal data covered by the SAR that the SAR has been made in order to ensure that the data is not destroyed. Care must be taken when doing this – it would not be appropriate (and may be illegal) to alert everyone in the office that a SAR has been made by, for example, a colleague.

Can we refuse to comply with a request?

258. Yes. If an exemption applies, we can refuse to comply with a SAR (wholly or partly). Not all exemptions apply in the same way and you should look at each exemption carefully to see how it applies to a particular request.

259. We can also refuse to comply with a SAR if it is:

- manifestly unfounded; or
- manifestly excessive.

Manifestly unfounded requests

260. Where requests are manifestly unfounded, we can either charge (see paragraphs **231** onwards) or refuse to comply. Any decision to refuse to comply on this basis must be made by the HOE (in the HOE's absence another HOD). When seeking the HOE's approval, it is important to state why a refusing to comply is considered appropriate in the circumstances: it is for the Commissioner to demonstrate that the requests are manifestly unfounded, so we will need to give the requester (and, potentially, the ICO) reasons for the decision.

261. The ICO guidance states that a request may be manifestly unfounded if:

- the individual clearly has no intention of exercising their SAR rights – for example, if they make a SAR but offers to withdraw it in return for some form of benefit
- the request is malicious in intent and is being used to harass us with no real purpose other than to cause disruption. For example, the individual:
  - (a) explicitly states that they intend to cause disruption
  - (b) makes unsubstantiated accusation which are clearly prompted by malice
  - (c) targets a particular employee against whom they have a personal grudge or

(d) systematically sends different requests to us as part of a campaign with the intention of causing disruption.

262. We must consider requests in the context in which they are made. If the individual clearly wants to exercise their rights, the request is unlikely to be manifestly unfounded.

263. The use of abusive or aggressive language, while not acceptable, won't necessarily make a SAR manifestly unfounded.

Manifestly excessive requests

264. Where requests are manifestly excessive, we can either charge (see paragraphs **231** onwards) or refuse to comply. Any decision to refuse to comply on this basis must be made by the HOE (in the HOE's absence another HOD). When seeking the HOE's approval, it is important to state why refusing to comply is considered appropriate in the circumstances: it is for the Commissioner to demonstrate that the requests are manifestly excessive, so we will need to give the requester (and, potentially, the ICO) reasons for the decision.

265. The ICO's guidance states that in order to determine whether a request is manifestly excessive, we need to consider whether it is clearly or obviously unreasonable, based on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request.

266. We must take account of all the circumstances of the request, including:

- the nature of the requested information
- the context of the request, and our relationship with the individual
- whether a refusal to provide the information or acknowledge we hold it may cause substantive damage to the individual
- our available resources
- whether it overlaps with other requests
- whether the request largely repeats previous requests and a reasonable internal hasn't elapsed. (In considering whether a reasonable interval has passed, we need to take account of the nature of the data, including its sensitivity) and how often the data is amended.)

Manifestly unfounded or excess requests: general points

267. The burden of proof is on us to show that all reasonable steps have been taken to comply with the SAR and that the SAR is manifestly unfounded or excessive.

268. It might be helpful to discuss with the requester the information they are requesting, including seeking appropriate clarification. File notes must be kept of any discussions with the requester.

269. Even if the SAR is manifestly unfounded or excessive, we should still try to comply with the request in some other way. For example, even if we are not providing the personal data itself, is there other information we can give to the requester?

Third party information

270. Article 15 of the UK GDPR makes it clear that the requester's right to obtain a copy of their personal data cannot adversely affect the rights and freedoms of others.

271. Of course, personal data can relate to more than one person so, in some cases, it will be impossible to comply with a SAR in full without disclosing information relating to another individual who can be identified from that information. It will be possible to identify another individual where they can be identified simply from the information disclosed, or from that information and any other information the data controller considers it reasonably likely is (or will be) in the requester's possession: if you are unsure, seek guidance from the HOE (DHOE).

272. Where compliance would involve disclosure of information relating to another individual and/or identifying another individual, the request does not have to be complied with unless either:

- the other individual has consented to disclosure of the information or
- it is reasonable to comply with the request without that individual's consent.

273. The ICO suggests the following three step approach when deciding whether to disclose third party information. You must record your decision making against these three steps in WP.[46]

Step 1: Does the request require the disclosure of information that identifies a third party?

Is it possible for us to comply with the request without revealing information that relates to and identifies a third party? We need to think about the information covered by the SAR **and** any information we reasonably believe the person making the request may have, or get hold of, that would identify the third party.

We can delete names or edit documents if the third party information doesn't form part of the requested information.

If it is impossible to separate the third party information from the information that's been requested and still comply with the request, move to step 2.

Step 2: Has the third party consented?

It is good practice to ask third parties for their consent to their personal data being disclosed in response to a SAR.

We are not obliged to ask for consent. In some circumstances, it won't be appropriate to do this, for example where:

- we don't have their contact details
- seeking consent would potentially disclose personal data of the requester to the third party that they weren't already aware of
- it would be inappropriate for the third party to know that the requester has made a SAR

Step 3: Is it reasonable to disclose without consent?

If we don't have consent, we must consider whether it is reasonable to disclose the information about the third party anyway.

[46] Template to set up in WP

The DPA 2018 says we must take account of all relevant circumstances, including:

- the type of information that would be disclosed
  any duty of confidentiality owed to the third party
- any steps taken to seek the third party's consent
- whether the third party is capable of giving consent
- any stated refusal of consent by the third party

However, this is a non-exhaustive list, and ultimately the decision must be made, taking the relevant factors into account, along with the context of the information.

Format of the information

274. If the individual submitted the SAR electronically, we should provide a copy of the data in a commonly used electronic format. We can choose the format, unless the requester makes a reasonable request for us to provide it in another commonly used format (electronic or otherwise).

275. If the individual submitted the SAR by other means (e.g. by letter or verbally), we should provide a copy of the data in any commonly used format (electronic or otherwise), unless the requester makes a reasonable request for us to provide it in another commonly used format.

276. Where the information is sensitive, we must ensure it is transferred to the requester using an appropriately secure method (see guidance from the ICO here).

277. Information can be provided verbally, if this is what the requester wants and if it's appropriate for us to do this (we are not obliged to provide personal data in this way). However, we are still required to obtain proof of identity, etc., and the SAR must be recorded in WP (and VC) where appropriate).

Exemptions

278. In certain limited circumstances, the Commissioner can refuse to comply with a SAR, either in full or in part. Schedules 2, 3 and 4 of the DPA 2018 set out the exemptions which may be used to withhold information from data subjects. The exemption most likely to be relevant is in paragraph 11 of Part 2 of Schedule 2, which allows information (including the data themselves) to be withheld to the extent that providing it would be likely to prejudice the proper discharge of the SIC's regulatory functions under FOISA, the EIRs and/or INSPIRE.

279. Other examples of exempt information are:

- Personal data which are subject to legal professional privilege[47]
- Personal data in employment references given by the Commissioner (or an employee of the Commissioner, acting on their behalf) in relation to the data subject[48].

Timescales for responding to SARs

280. We must under the UK GDPR comply with a SAR without undue delay and, at the latest, within one (calendar) month of receiving a request or of receiving:

[47] DPA 2018 Sch 2 Part 4 para 19
[48] DPA 2018 Sch 2 Part 4 para 24

- any information requested to confirm the requester's identity or
- any fee (if one has been charged)
- Where we seek clarification (see paragraph 242 above), the clock will be stopped from the day on which we ask for clarification until the day on which we receive it.

How to calculate "one month"

281. The applicable time limit is calculated from the day the request is received (whether or not it is a working day) until the corresponding calendar date in the next month. According to guidance from the ICO, if this is not possible because the following month is shorter (meaning there is no corresponding date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or public holiday, we have until the next day to respond.

282. The DO must notify BST of the final day for complying with the SAR, in order that compliance with the request can be monitored.

283. The exact number of days for complying will vary depending on the month in which the request is made.

> **EXAMPLE (1)**
>
> If we receive a (valid) request on 3 September, we have until 3 October to comply with the request.
>
> If 3 October falls on a weekend, or is a public holiday, we have until the end of the next working day to comply.

> **EXAMPLE (2)**
>
> If we receive a (valid) request on 31 March, we have until 30 April to comply with the request (31 April does not exist).
>
> If 30 April falls on a weekend, or is a public holiday, we have until the end of the next working day to comply.

Extending the time for responding

284. Unless the SAR has been made under section 45 of the DPA 2018, the period for responding to the SAR may be extended by a further two months provided the request is:

- complex (see below) or
- the requester has made other requests to us – according to ICO guidance, this can include other types of requests relating to individuals' rights, for example if the requester has simultaneously made a SAR, a request for erasure and a request for data portability.

285. Extensions must be agreed by the Commissioner (or, in the Commissioner's 's absence, the HOCS). When seeking agreement, it is important to state why an extension is considered appropriate in the circumstances, so the requester can be given the required reasons.

286. The requester must be informed of any extension, within one month of receipt of the request. We must explain why we have extended the period for responding.

When is a request complex?

287. Whether a request is complex will depend on the circumstances. The ICO suggests that the following factors will be relevant:

- any technical difficulties in retrieving the information
- applying an exemption that involves large volumes of particularly sensitive information
- clarifying potential issues around disclosing information about a child to a legal guardian
- any specialist work involved in obtaining the information or communicating it in an intelligible form
- clarifying potential confidentiality issues around the disclosure of sensitive medical information to an unauthorised third party
- needing to obtain specialist (non-routine) legal advice
- searching large volumes of unstructured manual records

Responding to SARs

288. **SAR04** should be used when responding to a SAR to ensure that all relevant information is provided to the requester. **SAR04** also contains some standard text (to be updated as appropriate) to cover issues with third party data and the most common exemptions which may be applied by the Commissioner.

289. The requester should be provided with a contact or reference point should they wish to discuss any of the information provided in response to their SAR. This will generally, but not always, be the DO who dealt with the SAR.

Right to rectification

290. Data subjects have the right to have inaccurate personal data rectified (Article 16 of the UK GDPR).

291. Article 16 also gives data subjects the right to have incomplete personal data completed, **taking account of the purposes for which the data are being processed**. With that qualification, this right is unlikely to extend to adding data which are not relevant to those purposes.

292. This right is subject to the same provisions on timescales as SARs (see above). The SIC has one calendar month to respond (and must do so without undue delay) and there are the same requirements for extensions.

293. In all cases where a rectification request is refused, the requester must be given reasons for the refusal. They must also be given information on their right to complaint to the ICO if they

don't believe the SIC is complying fully with the DPA 2018 or the UK GDPR, and on seeking judicial remedies.

294. Where possible, and where it would not involve disproportionate effort, any third party with whom rectified data have been shared should be informed of the rectification.

295. The right is also subject to the provisions relating to manifestly unfounded and excessive requests (see above, in relation to SARs).

296. The exemption in paragraph 11 of Part 2 of Schedule 2 of the DPA 2018 applies to this right, so the SIC may refuse to agree to rectification/completion to the extent that doing so would be likely to prejudice the proper discharge of our regulatory functions under FOISA, the EIRs and/or INSPIRE. This is particularly likely to arise in requests arising out of investigations casework: any such cases should be discussed with the HOE before responding.

297. Where the data are being processed for a law enforcement purpose and we need to retain the data in their present form as evidence, we may restrict the processing of inaccurate personal data rather than rectifying them. Any such cases should be referred to the HOE.

298. See paragraphs **332** and **333** for guidance on the data subject's complaint and appeal rights.

Right to erasure ("right to be forgotten")

299. In certain circumstances, data subjects have the right to require the Commissioner to erase (i.e. delete) data being processed about them (Article 17 of the UK GDPR):

    (a) where processing is based on consent alone and that consent is withdrawn, or

    (b) in cases of unlawful processing (including where the data are no longer necessary for the purposes for which they have been processed, where the right to object has been claimed successfully or where erasure is required to comply with a legal obligation).

300. The right to erasure will not apply where the processing is necessary:

    (a) to comply with a legal obligation, or

    (b) for the pursuit or defence of a legal claim.

301. This right is subject to the same provisions on timescales as SARs (see above). The SIC has one calendar month to respond (and must do so without undue delay) and there are the same requirements for extensions.

302. In all cases where a request for erasure is refused, the requester must be given reasons for the refusal. They must also be given information on their right to complaint to the ICO if they don't believe the SIC is complying fully with the DPA 2018 or the UK GDPR, and on seeking judicial remedies.

303. Where we agree to erase personal data which have been made public, reasonable steps should be taken to inform other bodies known to be processing the data. Where possible, and where it would not involve disproportionate effort, any third party with whom erased data have been shared should be informed of the erasure.

304. The right is also subject to the provisions relating to manifestly unfounded and excessive requests (see above, in relation to SARs).

305. The exemption in paragraph 11 of Part 2 of Schedule 2 of the DPA 2018 applies to this right, so the SIC may refuse to agree to erasure to the extent that doing so would be likely to prejudice the proper discharge of our regulatory functions under FOISA, the EIRs and/or INSPIRE. This is particularly likely to arise in requests arising out of investigations casework: any such cases should be discussed with the HOE before responding.

306. Where the data are being processed for a law enforcement purpose and we need to retain the data in their present form as evidence, we may restrict processing rather than agreeing to a request for erasure. There are also additional circumstances in which erasure of such data will be required, with or without a request, and other differences which apply to this kind of processing. Any such cases should be referred to the HOE.

307. See paragraphs **332** and **333** for guidance on the data subject's complaint and appeal rights.

Right to restriction of processing

308. In certain circumstances, data subjects have the right to require the SIC to restrict processing of their personal data (Article 18 of the UK GDPR):

    (a) where they are contesting the accuracy of the data, pending verification

    (b) where the right to object has been claimed, pending the outcome of that claim

    (c) where the data are no longer necessary for the purposes for which they have been processed (but the data subject still needs them to pursue or defend a legal claim), or

    (d) in cases of unlawful processing, where the data subject asks for restriction rather than erasure.

309. Restriction will mean – in addition to storage – processing the data only:

    (a) with the data subject's consent

    (b) to pursue or defend a legal claim, or

    (c) to protect the rights of others.

310. This right is subject to the same provisions on timescales as SARs (see above). The SIC has one calendar month to respond (and must do so without undue delay) and there are the same requirements for extensions.

311. In all cases where a request for restriction is refused, the requester must be given reasons for the refusal. They must also be given information on their right to complaint to the ICO if they don't believe the SIC is complying fully with the DPA 2018 or the UK GDPR, and on seeking judicial remedies.

312. Where possible, and where it would not involve disproportionate effort, any third party with whom restricted data have been shared should be informed of the restriction.

313. The right is also subject to the provisions relating to manifestly unfounded and excessive requests (see above, in relation to SARs).

314. The exemption in paragraph 11 of Part 2 of Schedule 2 of the DPA 2018 applies to this right, so the SIC may refuse to agree to restriction to the extent that doing so would be likely to prejudice the proper discharge of our regulatory functions under FOISA, the EIRs and/or

INSPIRE. This is particularly likely to arise in requests arising out of investigations casework: any such cases should be discussed with the HOE before responding.

315. Where the data are being processed for a law enforcement purpose, the provisions relating to restriction are slightly different. Any such cases should be referred to the HOE.

316. See paragraphs **332** and **333** for guidance on the data subject's complaint and appeal rights.

Right to object

317. Data subjects have a right to object to processing of their personal data (Article 21 of the UK GDPR). Where the objection is to processing for direct marketing purposes, the data subject may exercise that right at any time and the SIC must stop processing for these purposes.

318. Data subjects can also object under Article 21 when the SIC is processing their personal data under Article 6(1)(e) – the condition relating to tasks performed in the public interest and the exercise of official authority (which will apply to most processing in pursuance of the Commissioner's statutory functions). Where objecting under this heading, the data subject must provide grounds relating to their own particular situation, for example, relating to damage or distress they are suffering (or are likely to suffer) as a result of the processing.

319. Where a data subject makes the kind of objection described in paragraph **320**, the SIC must consider the grounds on which their objection is founded. These may be outweighed by compelling legitimate grounds for our processing, if these can be established. In other words, a balancing exercise is required, and the onus is on the SIC to demonstrate that our legitimate grounds should prevail.

320. The SIC can also continue processing, notwithstanding an objection, if we can demonstrate that the processing is required to pursue or defend legal claims.

321. This right is subject to the same provisions on timescales as SARs (see above). We have one calendar month to respond (and must do so without undue delay) and there are the same requirements for extensions.

322. In all cases where an objection is refused, the requester must be given reasons for the refusal. They must also be given information on their right to complaint to the ICO if they don't believe the SIC is complying fully with the DPA 2018 or the UK GDPR, and on seeking judicial remedies.

323. The right is also subject to the provisions relating to manifestly unfounded and excessive requests (see above, in relation to SARs).

324. The exemption in paragraph 11 of Part 2 of Schedule 2 of the DPA 2018 applies to this right, so we may refuse to agree to an objection to the extent that doing so would be likely to prejudice the proper discharge of our regulatory functions under FOISA, the EIRs and/or INSPIRE. This is particularly likely to arise in requests arising out of investigations casework: any such cases should be discussed with the HOE before responding.

325. Where the data are being processed for a law enforcement purpose, there is no right to object. Any such cases should be referred to the HOE.

326. See paragraphs **332** and **333** for guidance on the data subject's complaint and appeal rights.

Rights related to automated decision making and profiling

327. The UK GDPR applies to all automated individual decision-making and profiling.

    - Automated individual decision-making is where a decision is made solely by automated means without any human involvement.
    - Profiling is the automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process

328. Article 22 of the UK GDPR has additional rules to protect individuals if we carry out solely automated decision-making that has legal or similarly significant effects on them.

329. We can only carry out this type of decision-making where the decision is:

    - necessary for the entry into or performance of a contract; or
    - authorised by domestic (UK) law applicable to the controller; or
    - based on the individual's explicit consent.

330. If any of our processing falls under Article 22 we must:

    - give individuals information about the processing;
    - introduce simple ways for them to request human intervention or challenge a decision;
    - carry out regular checks to make sure that your systems are working as intended.

331. We do not carry out any automated decision-making or profiling.

Appeals and complaints

332. The DPA 2018 (as amended by the Data (Use and Access) Act 2025) gives a data subject the right to make a complaint to us if they believe we have infringed the UK GDPR in connection with their personal data. This can include dissatisfaction with our handling of their SAR or other rights request. We will deal with these, and any complaints about the service provided in dealing with a rights request, under our complaints procedures.

333. If still dissatisfied, the data subject should be advised to contact the (UK) Information Commissioner (https://ico.org.uk/make-a-complaint/)

Appendix 4 Data Processor Checks

Guidance when considering whether a data processor meets UK GDPR requirements

334. In this Appendix, "we/our" refers to the Commissioner.

335. In terms of Article 28(1) of the UK GDPR, we need to satisfy ourselves that any processors we engage offer sufficient guarantees that they are implementing appropriate technical and organisational measures to meet the requirements of the UK GDPR and protect individuals' rights, that is, we need to know they are meeting their duties as a data processor under the UK GDPR in respect of the personal data they process on our behalf, and in respect of which we are the data controller.

336. We should also check that they are in a position to assist us to meet our duties under the UK GDPR where, in practical terms, we may rely on them to be able to do so (e.g. to comply with a subject access request, or a request to rectify inaccurate personal data).

337. We do not need to concern ourselves with their processing of personal data beyond this, e.g. personal data they process on behalf of other controllers, or personal data in respect of which they are the sole data controller.

338. The ICO guidance "Contracts and liabilities between controllers and processors"[49] indicates that we should consider the following to determine whether proposed data processors are offering sufficient guarantees under Article 28(1) of the UK GDPR.

    (a) the extent to which they comply with industry standards, if these apply in the context of the processing;

    (b) whether they have sufficient technical expertise to assist the controller, e.g. in carrying out obligations under Articles 32-36 of the UK GDPR (technical measures, breach notifications and DPIAs);

    (c) providing the controller with relevant documentation, e.g. their privacy policy, record management policy and information security policy; and

    (d) adherence to an approved code of conduct or a certification scheme (when they become available).

339. The ICO guidance notes that our responsibilities do not end there: we must ensure the processor's compliance on an ongoing basis in order to satisfy the accountability principle and demonstrate due diligence.

340. There may be other questions which it's relevant to ask in the circumstances, and it will be for the UK GDPR Working Party and/or the HOCS/BST to identify these. For example, for technical services such as the appeal portal or email mailing systems, we should ask what

[49] Found at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts-and-liabilities-between-controllers-and-processors-multi/, relevant section at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/

back-ups are kept in case of a need to restore lost personal data, what access controls are in place and how are these audited.

341. Our pre-contract questionnaire is a template in VC. When using this template you should note:

    (a) We need to know that the processor has sufficient technical expertise to assist us in meeting our UK GDPR requirements. When available, adherence to an approved code of conduct or certification mechanism may be used as an element by which to demonstrate compliance on these points. Have regard to the particular risks presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data being processed.

    (b) Sometimes it will be sufficient for the processor to advise us that they have a privacy policy, record management policy, information security policy, disaster recovery plan / business continuity plan, other times we will need to see copies and check the terms of those policies. Whether we need to have sight of this documentation will depend on the personal data being processed, and the type of processing.

Follow up questions

342. Depending on the nature of the processing and any risks posed to a data subject, we may also wish to ask the data processor additional questions in light of the identified data protection risks related to the work to be done by the contractor. Advice on these can be sought from the BST or (as appropriate) HOE on a case-by-case basis, depending on the processing and the related risks.

Appendix 5 Data Protection Impact Assessments

Guidance when considering whether a full DPIA is needed

343. A Data Protection Impact Assessment (DPIA) will be required where the processing is likely to result in a high risk to the rights and freedoms of individuals. In particular, a DPIA is required in the case of:

    (a) a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect the individual;

    (b) processing on a large scale of special categories of personal information, or of personal information relating to criminal convictions and offences; or

    (c) a systematic monitoring of a publicly accessible area on a large scale.

344. Other circumstances which might give rise to high risk include circumstances such as:

    (a) where the processing might give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal information protected by professional secrecy[50], unauthorised reversal of de-identification, or any other significant economic or social disadvantage;

    (b) where individuals might be deprived of their rights and freedoms or prevented from exercising control over their personal information;

    (c) where special categories of personal information or information relating to criminal convictions and offences or related security measures are processed;

    (d) where personal aspects are evaluated, such as profiling;

    (e) where personal information of vulnerable natural persons, in particular of children, is processed; or

    (f) where processing involves a large amount of personal information and affects a large number of data subjects.

345. In order to determine whether a DPIA is required there is a pre DPIA checklist which should be completed and signed off by the Head of the Department which is undertaking the project. The HOE can provide advice and guidance on pre-DPIA checklists

346. The pre-DPIA checklist is a template in VC. When using this template it should be noted:

[50] See Recital (75) to the GDPR (no longer directly applicable in the UK). The term 'professional secrecy' is not defined in the UK GDPR. However, see Art 14(5)(d) – "…where the personal data must remain confidential subject to an obligation of professional secrecy regulated by domestic (UK) law, including a statutory obligation of secrecy".

(a) If the work involves using innovative technological solutions and is done in combination with any of the criteria in the European guidelines it's likely a DPIA will be needed.

(b) If you are not able to identify the risks, potential consequences of the risks occurring or the likelihood of the risk occurring, you may need to revert to the person who completed the form and ask for more information.

347. For further guidance, please see the ICO guidance on DPIAs[51]and the Article 29 Working Party's Guidelines[52].

348. The matrix set out below should be used to give an overall indication of the assessment of the risks posed by the project to personal information, based on the answers given in the pre-DPIA checklist.

349. For illustration purposes, this table provides that an overall score of 0-3 is low risk and does not require a DPIA to be carried out (unless there is a contractual or other legal obligation to carry out a DPIA). Scores of 4 and above would require a DPIA and scores of 8 or above would flag high risk projects that require a DPIA and may also need to be notified to supervisory authorities such as the ICO under Art 36.1 in the event that the risks cannot be adequately mitigated.

	Severity of Risk					
Likelihood of Risk	**0**	**1**	**2**	**3**	**4**	**5**
0	0	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**2**	**3**	**4**	**5**
2	**2**	**3**	**4**	**5**	**6**	**7**
3	**3**	**4**	**5**	**6**	**7**	**8**
4	**4**	**5**	**6**	**7**	**8**	**9**
5	**5**	**6**	**7**	**8**	**9**	**10**

Full DPIA required

350. Where it is clear from the information provided in the pre DPIA checklist that a DPIA is needed, the staff member who completed the checklist should complete the DPIA (see the template in VC) and consult the GDPR Working Party on the draft DPIA. A DPIA will help us to identify and minimise the data protection risks of a project.

351. A DPIA must be carried out for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. It is also good practice to carry

[51] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/

[52] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

out a DPIA for any other major project which requires the processing of personal data and involves significant changes in that processing from existing practice.

352. The DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

353. The DPO must also be consulted on all draft DPIAs and the HOE will arrange the consultation with the DPO. Where appropriate, it may also be necessary to consult relevant individuals, experts and processors.

354. If, having carried out a DPIA, we identify that there is a high risk which we cannot mitigate, we must consult the ICO before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the ICO may issue a formal warning not to process the data, or ban the processing altogether.

355. If the DPIA involves processing for law-enforcement purposes, we need to consider the ICO's guidance Guide to Law Enforcement Processing.

356. The Commissioner will publish all DPIAs where possible.

Appendix 6 Breaches of personal data and data incidents

357. A personal data breach is any data incident that affects the confidentiality, integrity or availability of personal data. A breach will include situations where personal data is:

- lost or corrupted;
- altered, destroyed, accessed or disclosed without proper authority;
- made unavailable, for example by encrypted ransomware.

358. A personal data breach can happen for a number of reasons, both accidental and deliberate:

- loss or theft of data or equipment on which data is stored
- inappropriate access controls allowing unauthorised access
- equipment failure
- human error
- unforeseen circumstances such as fire or flood
- hacking attack
- “blagging” offences where information is obtained by deception.

359. Our policies and procedures are designed to minimise the risk of personal data breaches occurring.

360. If a data incident occurs, the FAM (in consultation with the HOE, as required) has overall responsibility for coordinating the DIMP and reporting to and seeking the views of the SMT (as required) on any DIMP.

361. In the event that a personal data breach or potential data breach occurs**, it must be reported immediately to the FAM.**

362. If the data incident is likely to be a significant data incident, the FAM must notify the HOE (in whose absence, another member of the SMT).

363. A DIMP must be prepared for all data incidents using the template in “Data Incident Management Plan” in VC. The FAM (in consultation with the HOE, as required) will provide guidance on who should prepare the draft DIMP and will provide the data incident reference number.

364. Data incidents do not have to be referred to the DPO (or, by extension, the ICO or the data subject) where a breach does not pose a risk to the individual(s) affected and where no harm to them is likely as a result of a breach. A prime example is where routine elements of an applicant’s personal data are shared with the wrong public authority in the course of an appeal. For such cases, the template “Data Incident Management Plan Minor” should be used: this should be prepared on the basis that no further referral/ notification will be required, but should still be submitted to the HOE (for comment/consideration of whether the SMT needs to be informed) and otherwise dealt with in accordance with this procedure.

365. The relevant section of the ICO's Guide to the UK GDPR should be followed in relation to notifying the ICO and data subjects about a breach: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UK GDPR/personal-data-breaches/

366. Where a processor (e.g. a contractor processing personal data on our behalf) detects a personal data breach in relation to our data, the processor should report that breach to the FAM as soon as possible.

367. The FAM will coordinate the DIMP, which comprises four steps:

- containment and recovery
- assessment of ongoing risk
- notification of breach
- evaluation and response

368. Each data incident will be distinct in nature and require a different response. It is therefore not possible to be prescriptive about the detailed response to each occurrence. However, applying the ICO's guidance will ensure that our response to an occurrence is appropriate.

369. In all cases, we must bear in mind the need to consider whether the personal data breach needs to be notified to:

- The ICO: we must do this for every breach, unless we're satisfied that the breach is unlikely to result in a risk to anyone's rights and freedoms (consideration of this needs to be documented, in the "Assessing the risks" section of the DIMP) and in the Data Incident Log which is held in VC. The FAM will complete the Data Incident Log. In every case where we do need to notify, we must do so within 72 hours of becoming aware of the breach. For ICO contact arrangements, see https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/
- The data subject(s): we must do this where a breach is likely to result in a high risk to the rights and freedoms of the individual(s) concerned. This means the "Assessing the risks" section of the DIMP also needs to consider the severity of any potential impact and the likelihood of it occurring. Where a high risk is identified, we need to inform the affected individuals as soon as possible, unless we're satisfied that we've either –
    - applied appropriate measures (e.g. encryption) to protect the affected personal data and render them unintelligible to unauthorised persons, or
    - taken measures following the breach to ensure that the high risk is no longer likely to materialise.

370. The FAM/HOE can contact the DPO for advice and guidance on a DIMP and must record the advice given by the DPO. If necessary, the FAM/HOE may also contact the ICO's helpline for advice prior to any formal notification to the ICO.

371. The FAM will send the draft DIMP to the SMT for decision on the proposed course of action, except in cases where a DIMP Minor has been prepared and the HOE decides this is not required).

372. If the data incident requires to be notified to the ICO, the notification will be made by the HOE (in whose absence, another member of the SMT) and must include details of:

- the nature of the breach, including (where possible) the categories and approximate number of affected –
    - data subjects and
    - personal data records;
- the name and contact details of the DPO or other contact point where the ICO can obtain more information;
- the likely consequences of the breach;
- the measures we are taking or propose to address the breach, including any measures to mitigate its possible adverse effects.

373. Where we are aware of a breach and we are unable to provide all of the above within the 72 hours, we will provide what we can – with an explanation of the delay – and follow it up with the rest as soon as possible.

374. Notification to data subjects must include, in clear and plain language:

- a description of the nature of the breach, and
- the information set out in 10(ii), (iii) and (iv) above.

375. Where we conclude that identifying, locating and contacting the affected individuals would involve disproportionate effort, we should make a public communication with the above information.

376. Given the relatively short timescale for notifying the ICO, it's important that consideration is given as soon as possible to whether we need the DPO's assistance in handling the breach. When notifying the ICO, we need to give contact details for the DPO or another appropriate point of contact, to allow the ICO to obtain more information on the breach – if the DPO is to be the contact, they must be fully informed about the breach before notification. The DPO contact details are:

    Email: dataprotection@parliament.scot

    Telephone: 0131 348 5281

377. The data incident must be recorded in the Data Incident Log.

378. The DIMP and the actions (with records of any relevant SMT decision(s)/HOE comments and of the implementation of any relevant actions/decisions) must be retained as a formal record of the data incident.

379. The FAM (in consultation with the HOE, as appropriate) will be responsible for ensuring that any follow up actions take place.

380. The FAM will include the relevant details of any data incidents in the quarterly report to the SMT.

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and Status.	C5 Data Protection Policy and Handbook v03 CURRENT ISSUE
VC File Id	200302
Type	Policy & Procedure
Approver	SMT
Responsible Manager	HOE
Date of next planned review	January 2028
Approval & Publication	
Approval Date (major version)	10/01/2024
For publication *(Y/N)*	Y
Date published	26/11/2025
Name of document in website file library	DataProtectionPolicyandHandbook
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	19/06/2026

Summary of changes to document

Date	Action by *(initials)*	Version updated *(e.g. 01.25-36)*	New version number *(e.g. 01.27, or 02.03)*	Brief description (*e.g. updated paras 1-8, updated HOPI to HOCS, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding*)
10.01.2024	SL	03.00	03.01	New document created, DCS updated
25.01.2024	SL	03.01	03.02	DCS updated with publication date
04/04/2024	LB	03.02	03.03	Link to DPO MOU in para 70 updated (original link wasn't working)
29/10/2024	LB	03.03	03.04	Para 382 – changed 'must' to 'can'
21/11/2024	LB	03.04	03.05	Small changes to reflect referral to the DPO, front page updated, URL's checked and updated
20/02/2025	EM	03.05	03.06	Updates
04/03/2025	LB	03.06	03.07	Changes accepted after approval by SMT
25/11/2025	EM	03.07	03.08	Updates to reflect current practice and for D (U & A) Act 2025
26/11/2025	LB	03.13	03.14	DCS updated and published
19/06/2026	EM	03.14	03.15	Changes to reflect D (U & A) provisions on complaints (as approved by SMT)

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

t 01334 464610
enquiries@foi.scot
www.foi.scot

© Scottish Information Commissioner 2024

You may use and re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence v3.0. To view this licence, visit http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/