Social Security Scotland
Tèarainteachd Shòisealta Alba

Data Protection Policy

Classification: OFFICIAL

Dignity,
fairness,
respect.

Social Security Scotland – Data Protection Policy

1. Policy Overview

1.1 The purpose of this policy is to set out how Social Security Scotland will comply with its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR). Where appropriate, these pieces of legislation are referred to collectively in this policy as 'data protection legislation'.

1.2 The data protection legislation sets out responsibilities for the processing of personal data. Personal data is defined in the UK GDPR as:

'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

1.3 Personal data in Social Security Scotland includes information relating to our clients, current, former and prospective colleagues, as well as members of staff of stakeholder and partner organisations and other members of the public.

1.4 The UK GDPR prohibits processing of 'special category data' except in defined circumstances. Social Security Scotland may process special category data relating to its clients or colleagues. Unless stated otherwise, reference in this policy to personal data includes reference to special category data.

1.5 Special category data is personal data which reveal:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs, or
- trade union membership, and
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person;
- data concerning health or data concerning a natural person's sex life or sexual orientation.

1.6 Processing is defined in the UK GDPR as:

'operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

1.7 Social Security Scotland processes personal data through any use of it as described in the definition, including storage, and in any systems or applications, as well as in hard copy (for example in handwritten notes). Social Security Scotland can also engage suppliers and partners to process personal data on its behalf (see also paragraphs 5.7 and 5.9 below).

1.8 Personal data processed for Social Security Scotland's law enforcement functions including for example under Chapter 6 of the Social Security (Scotland) Act 2018 or the Management of Offenders etc. (Scotland) Act 2005 is governed by Part 3 of the DPA, rather than the UK GDPR. The provisions of Part 3 of the DPA are analogous to the provisions of the UK GDPR and this policy applies equally to processing for law enforcement purposes as it does to all of Social Security Scotland's other functions.

2. Governance

2.1 As an Executive Agency of the Scottish Government, Social Security Scotland acts on behalf of Scottish Ministers who are the controller for the personal data which Social Security Scotland processes. Social Security Scotland's data processing takes place within the terms of Scottish Ministers' data protection registration with the Information Commissioner's Office. Scottish Ministers and Social Security Scotland have agreed a memorandum of understanding which sets out the terms of an agreement between Scottish Ministers and Social Security Scotland on data protection responsibilities.

2.2 The Scottish Government's Data Protection Officer role satisfies the UK GDPR requirement for the appointment of a Data Protection Officer. The Data Protection and Information Governance Lead is the "Agency Data Protection Officer" as agreed with the Scottish Government's Data Protection Officer. References in this policy to the Data Protection Officer relate to Social Security Scotland's Data Protection Officer unless otherwise indicated.

2.3 The Data Protection and Information Governance team is responsible for supporting Social Security Scotland to comply with data protection legislation through provision of subject matter expertise and advice. The Data Protection and Information Governance team is also responsible for managing requests from individuals seeking to exercise their rights under the data protection legislation, investigating and managing suspected personal data breaches, providing assurance to Social Security Scotland on its compliance with the data protection legislation, and for maintaining necessary records of Social Security Scotland's data protection activities.

2.4 The Data Protection Officer and the Data Protection and Information Governance team provide advice on all aspects of data protection including on application of this policy and the implementation of data protection by design and default through Data Protection Impact Assessments. Colleagues seeking legal advice on data protection issues must contact the Data Protection Officer in the first instance before contacting any legal advisers.

2.5 The Information Commissioner's Office is the UK's data protection regulator. The Data Protection Officer must be consulted before any approach is made to the Information Commissioner's Office in connection with any of its functions.

2.6 Social Security Scotland commits to appointing and maintaining a Caldicott Guardian to ensure that it processes personal data relating to health and social care of clients in accordance with the Caldicott principles (a set of eight principles for the use of such data – see useful links below). The Chief Medical Advisor is Social Security Scotland's Caldicott Guardian.

3. Lawfulness of processing

3.1 Social Security Scotland will comply with the data protection principles in the UK GDPR (see section 4) in all its processing of personal data. Any Social Security Scotland's policies and procedures which concern the processing of personal data must be compatible with the requirements of the data protection legislation and this policy.

3.2 Social Security Scotland will only process personal data where a lawful basis for the processing applies. The UK GDPR provides the following six lawful bases:

- 'contract': the processing is necessary for a contract Social Security Scotland has with the individual, or because they have asked Social Security Scotland to take specific steps before entering into a contract;
- 'legal obligation': the processing is necessary for Social Security Scotland to comply with the law (not including contractual obligations);
- 'vital interests': the processing is necessary to protect someone's life;
- 'public task': the processing is necessary for Social Security Scotland to perform a task in the public interest or to carry out Social Security Scotland's official functions, and the task or function has a clear basis in law (for example Social Security (Scotland) Act 2018 or associated regulations);
- 'legitimate interests': the processing is necessary for Social Security Scotland's 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. This cannot apply when Social Security Scotland processing data to perform the its official tasks;
- 'consent': the individual has given clear consent for Social Security Scotland to process their personal data for a specific purpose.

3.3 Most of Social Security Scotland's data processing is likely to fall under the 'public task' lawful basis. Social Security Scotland will only rely on consent as a lawful basis where there are no other applicable bases to the processing as agreed by the Data Protection Officer or Data Protection and Information Governance team.

3.4 Social Security Scotland will only process special category data where a lawful basis exists under Article 6 and a condition set out in the Article 9 of the UK GDPR applies, or section 35 and schedule 8 of the DPA in the case of the processing for the its law enforcement purposes. Social Security Scotland maintains a policy document setting out the safeguards its applies to the processing of special category data as required by schedule 1 of the DPA. In most cases, Social Security Scotland's processing of special category data for clients and colleagues will rely on Article 9 (2) (b) (processing is necessary for the purposes of carrying out obligations in the field of employment or social security and social protection law).

4. Application of data protection principles

4.1 The UK GDPR sets out the a series of principles which require that personal data must be:

- processed lawfully, fairly and in a transparent manner (the 'lawfulness, fairness and transparency' principle);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those processes (the 'purpose limitation' principle);
- adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed (the 'data minimisation' principle);
- accurate and, where necessary, kept up to date (the 'accuracy' principle);
- kept for no longer than is necessary for the purposes for which it is processed (the 'storage limitation' principle);
- processed in a manner that ensures appropriate security of the personal data using appropriate technical or organisational measures (the 'integrity and confidentiality' principle).

4.2 Social Security Scotland will apply the data protection principles to its processing of personal data according to but not limited by the following general considerations. Social Security Scotland will pay particular attention to appropriate processing of personal data, and the protection of that data, when it relates to children.
4.3 Social Security Scotland will ensure it complies with the principle of lawful, fair and transparent processing by:

- only processing personal data where one of the legal bases in Article 6 of the UK GDPR applies; and
- ensuring adequate information is provided to the individuals whose data is processing, for example, through privacy information on its websites and intranet (for colleagues' personal data) and bespoke privacy information where appropriate in individual initiatives.

4.4 Social Security Scotland will ensure it complies with the purpose limitation principle by not processing personal data for a different purpose other than that for which it was originally collected where doing so would be incompatible with the original purpose.

4.5 Social Security Scotland will ensure it complies with the data minimisation principle by not processing personal data in excess of what is required for the activity for which it is processing personal data.

4.6 Social Security Scotland will ensure it complies with the accuracy principle by ensuring its processes and systems allow for the correction of inaccurate personal data.

4.7 Social Security Scotland will ensure it complies with the storage limitation principle by ensuring that it sets and operates retention and deletion schedules for all its personal data processing.

4.8 Social Security Scotland will ensure it complies with the integrity and confidentiality principle by maintaining appropriate technical and organisational measures, including limiting access to personal data to those with a business need only and by the application of security measures by the Chief Digital Office. Social Security Scotland colleagues must not process personal data in any system or application that has not been approved for that purpose by the Data Protection Officer and Chief Digital Office. This includes use of any devices, including personal devices and use of social media, including any similar online platforms.

4.9 Social Security Scotland will minimise the creation, use and storage of personal data in physical formats (hard copy) to essential business purposes only in view of the risks to compliance.

4.10 Social Security Scotland will pay special attention to protecting personal data relating to colleagues including access to such data.

4.11 All Social Security Scotland colleagues must undertake and pass e-learning on data protection on an annual basis. Colleagues with particular responsibilities for data protection must undergo appropriate supplementary learning and development relevant to their roles.

4.12 The data protection legislation provides some exemptions from some of these principles in particular circumstances. The Data Protection Officer or Data Protection and Information Governance team will provide advice on the application of exemptions before they are to be applied.

5. Data Protection by Design and Default (including Data Protection Impact Assessment)

5.1 Social Security Scotland will build in data protection considerations at the outset when planning its policies, processes, products, and research activities. This approach is known as 'data protection by design and default' and is intended to ensure that that data protection considerations, for example practical application of the data protection principles, are factored in at the beginning of any such activities.

5.2 Social Security Scotland will conduct a Data Protection Impact Assessment for any project, process, policy, system or research activity which involves processing personal data as determined by the Data Protection and Information Governance team The Data Protection Officer will require Information Asset Owners to take responsibility for managing risks in Data Protection Impact Assessments as necessary.

5.3 Colleagues responsible for the implementation of any such activities which are subject to a Data Protection Impact Assessment must ensure that any data protection risks identified are actively managed through an appropriate risk register.

5.4 Social Security Scotland will ensure that its governance and project management processes capture the need to complete a Data Protection Impact Assessment at the outset of any activity and that assessments are conducted on appropriate activities and continue to be assessed through the lifecycle of the activity, from design to delivery and termination.

5.5 Owners must review Data Protection Impact Assessments regularly to ensure their content and risk assessments remain up to date, relevant and accurate.

5.6 Social Security Scotland will not grant access to personal data relating to clients to any person outside Social Security Scotland (including the Social Security Programme) unless the processing has been subject to a Data Protection Impact Assessment, or as agreed by the Data Protection Officer or the Data Protection and Information Governance team, or is being made available to appropriate legal advisers for the purposes of obtaining legal advice.

5.7 Social Security Scotland will not process or arrange or permit the processing of personal data for which it is responsible outside the United Kingdom (including by any third parties contracted to provide services to Social Security Scotland) without the prior agreement of the Data Protection Officer. Colleagues proposing to arrange or permit processing of personal data must discuss any proposals with the Data Protection Officer.

5.8 Social Security Scotland will enter into formal data sharing agreements with third parties where the sharing of personal data with those parties is to be regular or high risk. Social Security Scotland will keep such agreements under regular review to ensure they remain accurate and up to date and the arrangements described are functioning as intended and comply with any legislative changes.

5.9 Social Security Scotland will ensure that any contracts and agreements it engages in with third parties contain appropriate provisions on personal data processing in accordance with the nature of any personal data processing described in such arrangements. The Data Protection and Information Governance team will provide advice on any such arrangements to ensure they meet the requirements of data protection legislation before any data processing takes place.

5.10 Social Security Scotland will ensure it retains logs of activities in relation to the processing of personal data in its core systems, including as required by Part 3 of the Data Protection Act in relation to personal data processed for law enforcement purposes.

6. Data Subject Requests

6.1 The data protection legislation provides various rights to individuals over the processing of their personal data. The rights are not absolute and exemptions may be required to their application. All data subject requests must therefore be considered individually on a case by case basis. The rights are:

- the right to be informed about the collection and the use of their personal data (this right is usually achieved through the provision of privacy information as described in 3.2 above);
- the right to access personal data and supplementary information (this right is often referred to as a Subject Access Request or SAR);
- the right to have inaccurate personal data rectified, or completed if it is incomplete;
- the right to erasure (to be forgotten) in certain circumstances;
- the right to restrict processing in certain circumstances;
- the right to data portability, which allows individuals to obtain and reuse their personal data for their own purposes across different services in certain circumstances;
- the right to object to processing in certain circumstances;
- rights in relation to automated decision making and profiling;
- the right to withdraw consent to processing at any time (where relevant);
- the right to complain to the Information Commissioner.

6.2 Any individual can make a request to exercise these rights. They can do so verbally or in writing and they do not have to cite the legislation or any particular terms for a request to be valid. In most cases, there is a one month statutory deadline for responding to such requests. Any such requests, or suspected requests, must therefore be referred to the Data Protection and Information Governance team as soon as they are received. The Data Protection and Information Governance team will manage all such requests. Colleagues must assist the Data Protection and Information Governance team with any requirements necessary to fulfil Social Security Scotland's responsibilities in processing data subject requests.

6.3 Requests by an individual (typically a client or member of staff) to correct personal data held about them in a live benefit claim (for example, a change of address) and which are unproblematic, can be processed without reference to the Data Protection and Information Governance team unless the colleague processing the request considers it should be rejected or a request is for information to be deleted, in which case the request should be referred to the Data Protection and Information Governance team.

6.4 Colleagues must refer any complaints or concerns received from any individual regarding the processing of their personal data to the Data Protection Officer before a response is made to any such individual.

7. Personal Data Breaches

7.1 The UK GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

7.2 Colleagues must refer any suspected personal data breach incident to the Data Protection and Information Governance team. Colleagues must not take action on any suspected incident without first discussing the matter with the Data Protection and Information Governance team or the Data Protection Officer.

7.3 Colleagues must assist the Data Protection and Information Governance team with any requirements necessary to fulfil Social Security Scotland's responsibilities in managing personal data breaches and incidents.

7.4 The Data Protection Officer is responsible for deciding on whether a personal data breach requires to be notified to the Information Commissioner's Office or communicated to a data subject.

8. Assurance

8.1 The Data Protection and Information Governance team is responsible for the implementation of a data protection assurance process in order to provide information to the Data Protection Officer, the Audit and Risk Committee and senior managers on Social Security Scotland's compliance with data protection legislation. All business areas in Social Security Scotland must engage with the data protection assurance process, including consideration of its findings, in order to ensure that Social Security Scotland can obtain assurance on its compliance with the requirements of the data protection legislation.

9. Cookies and Electronic Marketing

9.1 The Privacy and Electronic Communications Regulations (PECR) set out legal requirements for application of cookies and other tracking technology on websites, and on restrictions for unsolicited marketing by phone, fax, email, text or other electronic message.

9.2 All external websites operated by or on behalf of Social Security Scotland must conform to the PECR requirements by:

- ensuring all non-essential cookies and tracking technologies are disabled by default;
- providing accurate, easily accessible and comprehensive information on the use of such technologies to website users; and
- requiring users to opt in to any non-essential cookies or tracking or analytical technologies before they are activated on website users' equipment.

9.3 Colleagues must agree any proposals for electronic marketing within the terms of PECR with the Data Protection Officer before any such marketing takes place.

10. Roles and responsibilities

Data Protection and Information Governance lead	Owns, approves and monitors compliance with the policy.
Data Protection and Information Governance team	Carries out activities as described in the policy and keeps the policy under review.
Information Asset Owner	Approves relevant Data Protection Impact Assessments following review by the Data Protection Officer, and manages risks to information assets they are responsible, assigns an individual in their business area to keep Data Protection Impact Assessments under review and schedule reviews of it when circumstances change.
Chief Information Security Officer	Provides technical and organisation security measures to protect personal data.
All colleagues	Report personal data breaches and suspected personal data breaches, and receipt of data subject requests to the Data Protection and Information Governance team for further action, and complete annual data protection e-learning and any other required data protection training.

Useful links

Data protection guidance: Data Protection (sharepoint.com)

Caldicott principles: Eight Caldicott Principles 08.12.20.pdf (publishing.service.gov.uk)

Document Control

Doc Ref	Classification	Circulation	Status	Author	Contact
A40063445	Official	All colleagues	Final	[redacted]	dataprotectionofficer@socialsecurity.gov.scot

Version Control

Date	Updated By	Version	Reason for Change
01/10/2021	[redacted]	0.1	First draft
02/11/2021	[redacted]	0.2	Second draft
09/06/2022	[redacted]	0.3	Third draft
15/06/2022	[redacted]	0.4	Fourth draft
25/07/2022	[redacted]	0.5	Feedback from Information Governance Group
08/08/2022	[redacted]	1.0	Final version
31/08/2023	[redacted]	1.1	Annual review

Distribution and Approval

Role	Approval Decision	Date
Data Protection and Information Governance lead	Approved	31/12/2021
Chief Data Officer	Approved	14/06/2022
Information Governance Group	Approved	07/07/2022

Policy Owner

Role	Purpose
Data Protection and Information Governance lead	Owner

Review

Date Approved	Effective Date	Date of Next Review
07/09/2023	07/09/2023	September 2024