Social Security Scotland
Tèarainteachd Shòisealta Alba

Social Security Scotland Data Protection Annual Assurance Report 2021-22

Dignity, fairness, respect.

1. Introduction

This is the first annual report providing the outcome of assurance activity carried out on Social Security Scotland's compliance with data protection legislation[1]. The report is derived from assurance and other activities carried out over the course of the year by Social Security Scotland's Data Protection and Information Governance branch. In support of our data protection assurance framework, it also includes an assessment provided by the Digital Risk and Security Team of information security compliance across the Agency.

The report is intended to be of use to stakeholders including the Agency Data Protection Officer, the Scottish Government Data Protection Officer, the Information Governance Group, the Data Governance Group, Information Asset Owners and the Audit and Assurance Committee among others. Owing to the nature of data protection requirements and the Agency's functions, it is difficult to provide a single statement on the state of the Agency's compliance with all aspects of data protection legislation. The report instead therefore seeks to provide commentary and highlight issues against the content of the data protection assurance framework in order to inform action to maintain or improve compliance in Social Security Scotland in 2022-23.

2. Data Protection Assurance in Social Security Scotland

A data protection assurance function was established in the Data Protection and Information Governance branch in March 2021 in order to implement Social Security Scotland's data protection assurance framework. The framework has been designed to assess compliance with legislation and support a culture of continuous improvement to support efforts to ensure we meet our obligations to protect and manage personal data appropriately. The framework has four elements:

- data protection requirements which set out the standards Social Security Scotland is required to meet;
- a tailored health check process for business units and processes;
- performance monitoring; and
- evidence-based reporting.

Activities in the year have focused on finalising and formalising the data protection requirements, designing, piloting and rolling out the health-check process and producing this report. Plans for further enhancement and implementation of the data protection assurance processes are set out below.

Internal Audit colleagues reviewed and provided advice on the assurance approach in early 2022. This was very helpful and their views will inform the development of the data protection assurance function.

[1] This term encompasses the UK General Data Protection Regulation, the Data Protection Act 2018 and associated regulations and the Privacy and Electronic Communication Regulations.

The Data Protection Team has become firmly established during the last year allowing an increasing range of data protection activities to be initiated. The findings from the assurance work has influenced the direction of activities for the team to ensure that identified issues are being addressed. These include the production and publication of data protection guidance together with delivering further training opportunities requested by the business areas that have undertaken the health checks. These further activities have contributed to the overall assurance on data protection compliance.

3. Data Protection Health Checks

The main data protection assurance activity is a consensual self-assessment health check questionnaire. This approach has been driven by the remote working restrictions in place. The questionnaire is completed by managers in the relevant business area to establish a baseline on their compliance with data protection.

The Agency Data Protection Officer agrees which business areas should be subject to a health check. Bespoke scenario-based questions are separately posed to a representative sample of colleagues within the business area and the findings are reviewed by the Data Protection Team to support or challenge (where appropriate) the responses received in the questionnaire. (See Annex 1, Table 1).

Using a continuous improvement approach within the business areas and support from the Data Protection Team, managers in business areas action any recommendation towards attaining full data protection compliance. Health check reports also seek to identify and promote areas of good practice.

Common issues have been identified from health checks:

- business areas are aware of data protection requirements but are at an early stage of maturity regarding how to fully implement the policies and controls required when handling personal data.

- business areas are creating and using tools, trackers and databases, which can hold significant volumes of personal data. There are a number of risks associated with this activity that Information Asset Owners may not be aware of and which are unlikely to have been assessed.

- there is often disparity between the self-assessment questionnaire and the results of the scenarios posed to the colleagues within the business area. The main areas requiring attention include how to correctly action a data subject request and report a potential data breach. This indicates a continuing requirement for guidance and training on such issues.

4. Assurance Framework

The Data Protection Framework Requirements is the reference document used to assess the extent to which the Agency is meeting the requirements of the data protection legislation. It consists of the following categories, with assurance findings set out on each and in section 5 for information security.

a) Data Protection Policy

Social Security Scotland follows the Scottish Government's data protection policy. This does not sufficiently reflect the Agency's specific functions in relation to:

- the personal data of our clients, and
- the processing of client data.

A dedicated Social Security Scotland data protection policy is in preparation and will be submitted for approval in Q1 of 2022/23.

b) Governance

The Scottish Government Data Protection Officer continues to fulfil the legal requirement for the appointment of a Data Protection Officer for Social Security Scotland as part of the legal entity of Scottish Ministers. The Agency has appointed a Data Protection Officer who acts in accordance with the Memorandum of Understanding (refreshed in January 2022) with the Scottish Government to carry out data protection responsibilities in the Agency. The Agency Data Protection Officer is [redacted] ([redacted] until May 2021).

The Data Governance Group and Information Governance Group have recently been established. These are the main mechanisms for the Agency Data Protection Officer to engage senior management (including the Senior Information Risk Owner and Information Asset Owners) in data protection matters. These will be fully established in the next reporting year and have an important role in monitoring compliance of the Agency moving forward.

c) Supporting Policies and Guidance

Bespoke guidance for the Agency has been produced on data breaches and managing data subject requests. Work is ongoing to ensure awareness and implementation of the guidance. The results of health checks indicate that further work is required more broadly across the Agency to ensure that policies and procedures on a wide range of issues across the Agency (for example human resource processes) take data protection requirements into account.

d) Record of Processing Activities

The Data Protection Team has focussed dedicated effort on creating a bespoke Record of Processing Activities in collaboration with business areas across the Agency capturing Agency personal data processes in accordance with the requirements of the data protection legislation which mandate this.

In conjunction with the Record of Processing Activities, an issues log has also been created to capture concerns with existing processes. Issues from both the Record of Processing Activities and issues log are fed into health check questionnaires to be raised with business areas undergoing assessment.

In the coming year, the focus will shift to maintaining and reviewing the Record of Processing Activities to ensure it remains up to date.

e) Privacy by Design

The Data Protection and Information Governance branch has supported the Agency in completing a number of Data Protection Impact Assessments on personal data processing initiatives in the Agency's corporate activities (until they formally transition to the Agency, responsibility for Data Protection Impact Assessments concerning benefits delivery remains with Programme).

During the last financial year the Data Protection and Information Governance branch has supported a number of business areas with Data Protection Impact Assessments. These included Volume Recruitment, user research, client panels and staff identity cards. The Agency Data Protection Officer is sighted on Data Protection Impact Assessments originating from both the Agency and Programme.

A new Data Protection Impact Assessment process and templates have been developed and implemented within the Agency. These are intended to further embed data protection compliance in the design of relevant projects and when business areas are introducing new processes or products involving personal data. The success of this will be measured through the health check process, as well as regular reviews of risks identified within Data Protection Impact Assessments, including seeking evidence that data protection risks are being integrated into the appropriate risk registers in Agency business areas.

Health checks have identified that not all business areas are sufficiently engaged in the Data Protection Impact Assessment process required to consider data protection aspects for any changes to the original design developed by the Programme. Projects involving data protection requirements sometimes only come to the attention of the Data Protection Team comparatively late in the delivery plan, risking insufficient time to assess data protection risks and design out non-compliant elements. Further work should take place to embed privacy by design as part of the Agency's normal processes. The Agency's new governance structures (e.g. for change management) will provide one opportunity for this, but further engagement across the Agency will be required to improve compliance in this area.

f) Third Party Risk

Third party risk concerns risk to Agency personal data processed by or shared with third parties. The Data Protection Team has worked with Procurement colleagues to ensure there is sight of all current and future Agency procurements. This is intended to the ensure data protection obligations are included in relevant contracts and:

- ensure contractual agreements that involve personal data processing reflect the requirement for appropriate data protection clauses; and
- that there are in-built reviews to ensure that supplier data protection obligations are being met in support of the Agency's own obligations.

A model for integration of data protection requirements into the procurement lifecycle has been developed and will be implemented to ensure data protection considerations are addressed throughout the procurement lifecycle and in a timely manner. This process continues to embed as some procurement requirements and contracts have being referred to the Data Protection Team by business areas at short notice or retrospectively, in an analogous way to Data Protection Impact Assessment requirements as noted above.

Future activities include ensuring the Agency has a centralised log of all its third party processors and Data Sharing Agreements. The Data Protection Team will use the health check process to identify any additional third party contracts and data sharing arrangements within the business areas under assessment.

Formal data sharing agreements are mainly required for the delivery of benefits and as such are managed by Programme until they formally transition to the Agency. The health check questionnaire includes content intended to identify any other third parties with whom it may be desirable to establish a formal data sharing agreement. The Data Protection and Information Governance branch is engaged in work overseen by the Data Governance Group for a formal process to assess requests to share Agency data with third parties, including the data protection considerations.

g) Training and Awareness

It is mandatory for all colleagues to complete the Scottish Government's Data Protection e-Learning package at induction and again on annual basis thereafter. The Data Protection Team monitors completion rates monthly and take the necessary steps to ensure staff take action if they do not attempt, fail to complete, fail to renew or fail to pass the e-Learning. This includes notifying the line manager and escalation to Deputy Directors if necessary. Management information on completion rates is shared regularly with the Data Governance and Information Governance Groups and compliance assessment is part of the health check process. At Agency level, management information shows the completion rates have remained at 90% or above during the past year.

In addition to mandatory e-Learning, the Data Protection Team delivers bespoke face to face training sessions to business areas. Specifically for new entrants in Client Service Delivery, there is a standard session which forms part of the formal induction plan. Ad hoc sessions have been delivered to meet actions identified by health checks or in response to data breaches.

The Data Protection Team has provided improved Saltire guidance on processes for managing personal data incidents and breaches and data subject rights. The team has also made recommendations on content in the Internal Knowledge Management hub including reviewing the guidance available for third party representatives, and has

published a series of articles raising data protection awareness to coincide with International Data Protection Day in January 2022.

h) Data Subject Rights

The Agency's requirement to notify data subjects of their rights under data protection legislation is delivered through privacy notices. The Social Security Programme is currently responsible for maintaining the client-facing privacy notice. Social Security Scotland relies on the Scottish Government's staff data privacy notice, but this appears not to have been updated for some time as it cites repealed data protection legislation and Social Security Scotland may therefore wish to develop its own version.

The Agency processed 11 data subject requests in 2021/22, with seven of these being requests for access and the remainder exercising other rights. All of the requests except for one were met within the prescribed period of one calendar month from date of receipt. There were some examples of data subject requests not being identified and forwarded to the Data Protection Team promptly or at all, including one where this oversight led to the Agency missing the statutory deadline to respond. The minimal volume of requests received were too low to identify any significant trends.

The Data Protection Team has provided communications, reminders and learning about data subject requests and the supporting processes. Evidence from the health checks has indicated additional activities are required to ensure the processes are fully embedded and the Agency is fulfilling its requirements in this area. Awareness of data subject rights other than the right of access in particular is low and awareness-raising is likely to continue to be required.

i) Personal Data Breaches

During 2021-22 the Data Protection Team has taken action to mature and embed the process for managing personal data breaches within Social Security Scotland. This has included revising and updating available guidance and delivering bespoke sessions to business areas identified as requiring support on breaches (business areas are identified as a result of trend analysis and findings from health checks).

Potential and actual personal data breaches are recorded in the Scottish Government's security incident reporting tool for investigation by the Agency's Data Protection Team. Each report is assessed to determine the severity of the breach.

[redacted]

The Data Protection Team provides feedback ensuring that a full summary, lessons learned and recommendations are shared appropriately within the Agency following every referral. Regular management information on data breaches is presented to the Data Governance and Information Governance Groups. Recommendations and management information also inform the health check process so that evidence-based reviews of data breaches are incorporated into follow-up assurance work.

The number of potential and actual personal data breaches reported to the Data Protection team has risen by approximately 60% compared to the year before. This may be attributed, in part, to the growth of the Agency, an increased volume of clients and staff as well as the complexity of the benefits we now deliver and related human error.

An increase has been identified in the number of breaches resulting from [redacted] Work is ongoing to co-ordinate the risk assessment of personal data breaches caused by [redacted]. There is a need to agree a process to investigate and assess the full scope and impact of [redacted] and ensure that data protection risks are considered alongside other priorities to achieve effective and timely resolution. This will also enable more accurate risk assessments and identification of appropriate next steps. Work continues to bring together the key stakeholders in managing these types of incidents.

It is anticipated that with the significant increase of staff required for the launch of Adult Disability Payment and further rise in client numbers that a further increase in the number of personal data breaches is likely to be reported in the coming year. The Data Protection Team will monitor this closely to intervene and mitigate the increase and consider what other actions we might take.

5. Information Security

Through the 2021-22 reporting year, Social Security Scotland (led by the Digital Risk and Security branch) has continued to develop the suite of information security policies which form a crucial part of the Social Security Scotland Security Governance documentation. 14 policies have been delivered to the Chief Digital Office Senior Management Team for review and approval and where appropriate a small portion have undergone further quality reviews and socialisation across Social Security Scotland and the Social Security Directorate.

A significant review and update of the Security Baseline Standard (SBS) was initiated and completed within the 2021-2022 reporting year. In support of Social Security Scotland Security policies and standards, the SBS details the cyber security requirements which must be met before a solution is accepted into the Social Security Scotland platform architecture. The Social Security Scotland SBS represents a baseline standard of security controls – it must be reviewed by applicable stakeholders involved in the introduction of new infrastructure or applications into the Social Security Scotland technology estate. The standard details the security controls which must be incorporated into solution designs and ensures adherence to ‘secure by design’ principles. Compliance with requirements is measured and reported through project engagement with the assigned Security Information Risk Advisor and this is reflected within the relevant security artefacts.

The Digital Risk and Security branch has continued to establish a security risk management framework through the 2021-2022 reporting year to support sufficient risk analysis of the organisation, information systems, services and business processes that process personal data. The Information Security Forum subscription provides access to a wide range of training and resources and access to the IRAM2 risk assessment methodology to enable where appropriate the delivery of robust and consistent risk

assessment outputs. Through the reporting year, the Digital Risk and Security branch has continued to refine the supporting risk assessment artefacts such as the Operation Readiness Statement and Statement of Assurance and their associated processes. An Information Security Risk Working Group has been established to provide governance and senior management oversight of risk treatment plans and ongoing assurance activities and deliverables.

A programme of IT Health Checks has continued to be executed at pace on new software and/or infrastructure being delivered as part of the Social Security Programme to gain external assurance that products are sufficiently hardened to minimise the likelihood of common digital attacks. Identified vulnerabilities are assessed, translated into risks utilising the IRAM2 methodology and documented within agreed risk treatment plans to enable risks to be managed appropriately.

The development of a Supplier Security Framework to manage information security risk throughout the lifecycle of contracts has continued with a primary focus on new suppliers. Where appropriate, the Cyber Security Procurement Support Tool is used to develop an initial supplier security risk profile. Requirements such as the National Cyber Security Centre Cloud Security Principles, data protection legislation and Information Commissioner's Office/National Cyber Security Centre UK General Data Protection Regulation Security Outcomes are posed to the Supplier and their responses are considered by the assigned Security Information Risk Advisor. Current assurance levels are assessed through the completion of a supplier assurance questionnaire contained within the Cyber Security Procurement Support Tool. Information risk related to services provided by a supplier is considered using the IRAM2 risk assessment methodology and the Digital Risk and Security team review and evaluate supplier security statements, plans, documentation and certifications. Supplier responses to security non-functional requirements as defined within the Security Baseline Standard are verified through verification that the design, processes and personnel involved within service delivery meet or exceed Social Security Scotland requirements.

A cyber resilience maturity assessment was initiated and completed within the last quarter of 2021-2022 and the results are under management review. The assessment aimed to assess maturity levels against each of the four security domains: Manage, Protect, Detect and Respond and Recover. This framework aims to provide a consistent way for Scottish public sector organisations to assess their cyber resilience arrangements, identify areas of strength and weakness, gain reasonable confidence that they are adhering to minimum cyber resilience requirements and taking informed decisions on how or whether to achieve higher levels of cyber resilience on a risk-based and proportionate basis.

6. Additional Assurance Activities

Additional assurance work was undertaken by the Data Protection and Information Governance branch on access to the Social Programme Management system by Programme and Chief Digital Office colleagues. This included ensuring legitimate business justification for access and where appropriate, modifying or removing access.

A review of options to mitigate risks associated with the ability to screen share using MS Teams was undertaken and options were presented for review by the Information Governance Group to inform decision-making on the appropriate approach.

The Data Protection Team received over 100 requests for data protection advice from across the Agency in 2021-22. This provides some indication that data protection issues are actively considered by colleagues across the Agency.

7. Data Protection Assurance Activities 2022-2023

There will be a number of data protection challenges in the forthcoming year including the introduction of new benefits and the ongoing maintenance of existing benefits transitioning from Programme to Agency, and related growth in the size of the Agency. The Agency will accordingly continue to embed awareness of and compliance with data protection legislation and practice as part of its culture and as it grows and matures.

Assurance activities will be further embedded and health checks will be extended to other business areas not assessed in 2021-22. There will also be activity to review the implementation of records in those business areas that were subject to a health check this year. This will be supported by a reporting mechanism being introduced which will include measuring progress on the recommendations identified from the health checks. The Data Protection Team will further expand the nature of assurance work it undertakes to assess compliance in thematic issues which affect multiple business areas across the Agency.

Author	[redacted]
Approved by	[redacted]
Date	June 2022
Distributed to	Data Protection and Information Governance Lead
	Scottish Government Data Protection Officer
	Information Governance Group
	Agency Leadership Team
	Executive Team
	Audit and Assurance Committee

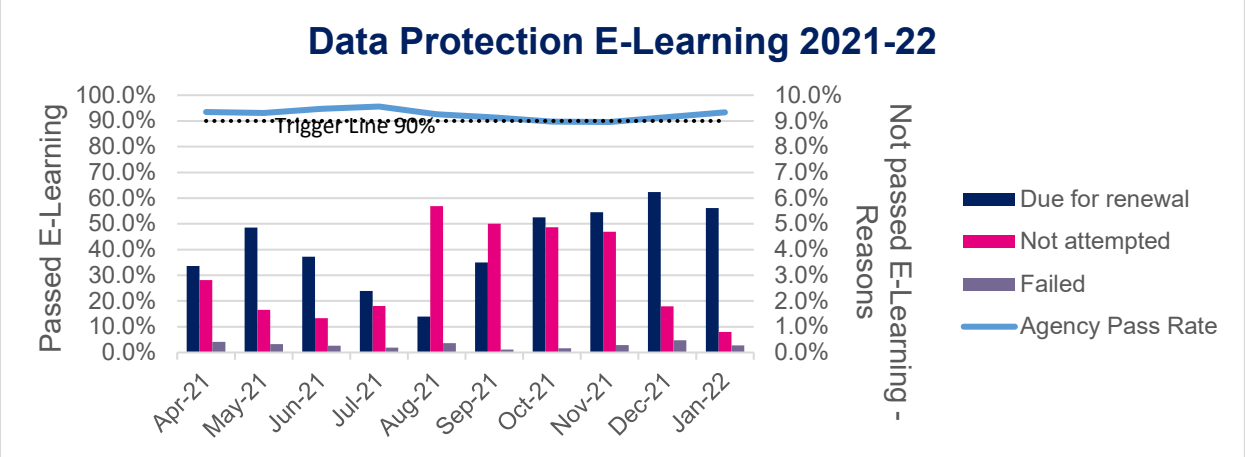
Annex 1

Table 1

Data Protection Health Checks

Number of Health Checks		Number of Recommendations			Number of Recommendations Accepted			Number of Recommendations Rejected		
Completed	Ongoing	High	Medium	Low	High	Medium	Low	High	Medium	Low
4	2	2	26	31	2	26	31	0	0	0

Table 2



*NB - the management information tool did not provide compliance data for February or March 2022.

Table 3

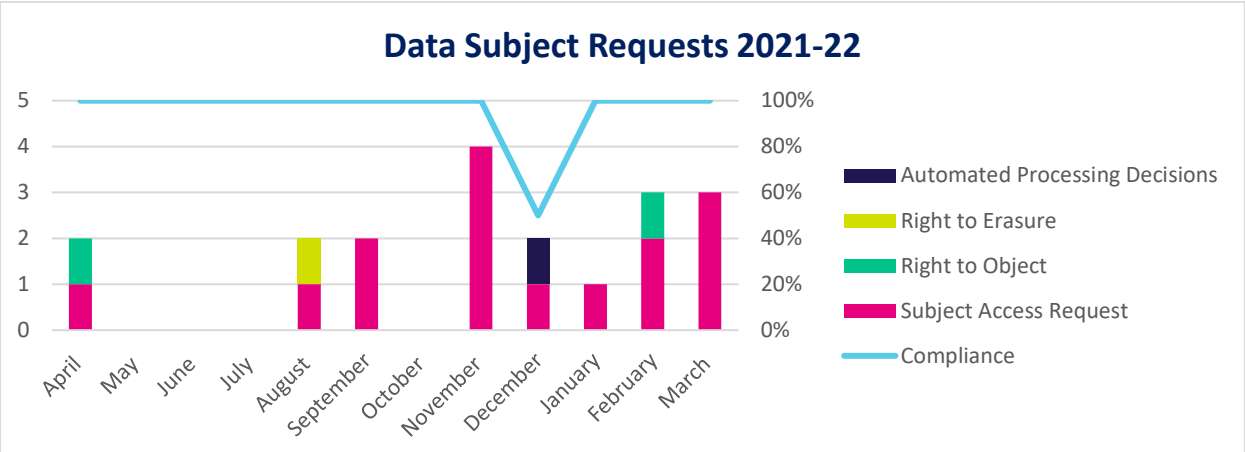


Table 4

[redacted]

Table 5

[redacted]