Data Protection Impact Assessment (DPIA)

1. Introduction

The purpose of this document is to assess privacy risks relating to the operational activity of the Internal Audit Division (IA)

2. Document metadata

3.

3.1 Name of Project: Review of Privacy Risk in Internal Audit

3.2 Author of report: **[REDACTED]**

3.3 Date of report: July 2020

3.4 Name of Information Asset Owner (IAO) of relevant business unit: Jennifer Inglis-Jones

3.5 Date for review of DPIA: July 2021

Review date	Details of update	Completion date	Approval Date
March 2021	Review on operational experience		
Annual – April	Part of activity planning		

4. Description of the project

4.1 Description of the work:

Internal Audit (IA provide audit services to the whole of the Scottish Government and over twenty other public sector bodies (such as the Scottish Public Pensions Agency, Revenue Scotland and Transport Scotland). As well as carrying out verification, compliance and audit work on EU funds.

IA provides independent assurance that proper and effective arrangements exist for financial and management control, primarily on behalf of Accountable Officers. We look at the procedures used to control the key activities across the SG to assess how well they are operating and examine whether the systems in use give best value for money. Our role is in addition to, not in place of, programme managers in the control and monitoring of spending. IA is also a source of advice and is often brought in when systems or procedures are being developed.

A DPIA is needed because:

The Division has not been assessed against the new privacy regulations and laws introduced in 2018. It is also likely that personal information will be processed as part of the Division activity and some of this information may be sensitive or lead to criminal proceedings.

4.2 Personal data to be processed.

Variable	Data Source
Names and business e-mails addresses of staff being audited	Audits, Assurance and Investigations
Names, business and personal e-mail addresses and living and working addresses of persons being investigated	Counter Fraud Investigations
Personal statements	Investigations

4.3 Describe how this data will be processed:

Some information may be stored with the SCOTS outlook on a temporary basis, and in accordance with the SG Internal Audit manual, data is stored in eRDM for the corporate record. The eRDM area is restricted to IA, and where files may contain sensitive information, these files are restricted to only include those who require access to it.

Personal information will be disposed of once the purpose for which it was obtained has been fulfilled.

Internal Audit stores documents electronically within the SCOTS network. The Galileo system is hosted on the SG network and is therefore protected by the overall SG network security system. In addition to this, each user is allocated a unique username and password that is used to grant access the system.

5. Stakeholder analysis and consultation

5.1 List all the groups involved in the project, and state their interest.

Group	Interest
IA	Controller and or processor
SG business areas	Controllers and processors
Non-SG business areas	Controllers
Areas or persons being investigated	Data subjects
Audit Scotland	Assurance
Ernst & Young	Sub-Processor
Local Authority Partners	Controller and or processor
Cabinet Office	Sub-Processor

5.2 Method used to consult with these groups when making the DPIA.

Stakeholders that are provided an Internal Audit service are done so through a Memorandum of Understanding agreement, that outlines how their data will be processed.

Stakeholders which are non-SG are provided with Data Privacy Notice, option for SG Data Sharing Agreement (template), MoUs.

Where Stakeholders are processing data on behalf of DIAA, this will be done in line with the “Data Protection” section in the contract.

5.3 Method used to communicate the outcomes of the DPIA .

The DPIA is published on the Scottish Government website.
The DPIA is shared with all data providers directly.

6. Questions to identify privacy issues

6.1 Involvement of multiple organisations

In addition to the Scottish Government, Internal Audit will be processing to data of 21 other public body clients. The full list of organisations currently comprises:

Scottish Government
Accountant in Bankruptcy
Community Justice Scotland
Crown Office and Procurator Fiscal Service
Disclosure Scotland
Education Scotland
Food Standards Scotland
Forestry and Land Scotland
National Records of Scotland
Office of the Scottish Charity Regulator
Official Feed and Food Controls
Registers of Scotland
Revenue Scotland
Scottish Courts and Tribunal Service
Scottish Fiscal Commission
Scottish Forestry
Scottish Housing Regulator
Scottish Public Pensions Agency
Social Security Agency
Student Award Agency Scotland
Transport Scotland

Processing is lawful as it meets the following conditions for processing Personal Data under:

- Article 6(1) of the GDPR:

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

Internal Audit processes personal information under the lawful basis of public task. This is underpinned by the Finance arrangements in the Scotland Act in section 64 to 72 and specifically section 70 that relates to Financial Control, Accounts and Audit.

In addition to this general legal basis, it is likely that some organisations being audited will have a statutory requirement of their own and where this is appropriate, this will be identified in the audit approach document agreed with eh client.

6.2 Anonymity and pseudonymity

There is no intention to anonymise personal information as the nature of audit and assurance activity demands that individuals are known, this will be reviewed in 2021, in line with a recommendation from Audit Scotland. Sensitivity will be shown where required and names will be avoided or redacted as necessary. The use of pseudonymity methods may be applicable to statements during investigations and this will be reviewed at the first DPIA review in 2021.

6.3 Technology

SCOTS is the primary platform for processing information. This includes Galileo, eRDM, Outlook, hard drives and terminal devices such as laptops and smart phones. SCOTS is accredited to Cyber Essentials Plus and is subject to regular security health checks. Role based access management is in place as is system monitoring and staff training. The SCOTS platform and operational processes is subject to regular audit.

Where information is being passed to other organisations, suitable measures will be taken to ensure appropriate privacy is in place and that information is not passed across the clear internet. SG cyber security team will be consulted on a case by case basis and techniques such as PDF encryption or secure winzip or eRDM connect will be used.

SCOTS enjoys a secure connection with the PNN and CJSM networks and information can be passed to Crown Office and Police through those channels.

6.4 Identification methods

It is anticipated that in most cases full names will be used. Where pseudonymity techniques have been used, as per section 6.2 above, then only staff in the immediate investigation team will have access to the linking files.

6.5 Sensitive/Special Category personal data

IA does not set out to collect sensitive or special category information but recognised that it may need to processed as part of a fraud or other investigation.

In such a case, this work meets the conditions of GDPR Article 9(2)(g) - processing is necessary for reasons of substantial public interest, on the basis of Union or Members State law which will 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.

This work also is in line with the Data Protection Act 2018 Schedule 1 Part 1.

Where special category or sensitive information has to be processed, additional safeguards will be put in place as follows:

A restricted eRDM folder will be set up to control access to sensitive information;
eRDM Connect will be used to share information with relevant external bodies in a secure manner.

It is feasible that an investigation may lead to criminal charges. In such cases, IA will rely on GDPR Article 10 and conditions for law enforcement processing set out in DPA 2018 Part 3 section 42 (safeguards), the Scottish Government have an appropriate policy as required by DPA 2018.

6.6 Changes to data handling procedures

The IA privacy notice will be updated and lodged in the audit handbook. The requirement to make this available at point of collection will be met by including the notice in the audit approach document agreed with clients before work commences.

6.7 Statutory exemptions/protection

The audit function and counter fraud activities will call upon exceptions to subject access rights under GDPR Articles 13 to 21 and 34 where evidence of criminal activity or malpractice in public office is suspected. These are justified under DPA 2018 Schedule 1 Part 2 in relation to protect members of the public against dishonesty, malpractice, seriously improper conduct, unfitness or incompetence.

6.8 Justification

This project is required to support the delivery of audit services to the Scottish Government, and other bodies that IA provide an internal audit service for.

6.9 Other risks

None. Internal Audit does not involve regular systematic processing of high risk personal information. Sensitive, special category or information concerning prosecution will be handled by exception under the legal bases described above and to the safeguards set out in the appropriate policy document.

7. General Data Protection Regulation (GDPR) Principles

Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.1 Principle 1 – fair and lawful, and meeting the conditions for processing	Yes	Data processing is lawful and in line with the GDPR. Article 6(1) (e) of the GDPR: The processing is necessary in order to perform a task in the public interest. In such a case, this work meets the conditions of GDPR Article 9(2)(g) - processing is necessary for reasons of substantial public interest, on the basis of Union or Members State law which will 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.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.2 Principle 2 – purpose limitation	**Yes**	The data collected will only be used for the purposes of conducting audits. A MoU sets out how information will be used.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.3 Principle 3 – adequacy, relevance and data minimisation	**Yes**	The approach taken to audit and assurance reviews will be agreed with the client before work begins. No more information is collected than is needed to provide assurance. In the case of counter fraud activity, statutory exemptions will be employed.

Principle	Compliant – Yes/No	Description of how you have complied
6.4 Principle 4 – accurate, kept up to date, deletion	**Yes**	All audit and assurance reviews are shared with the client before publication.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.5 Principle 5 – kept for no longer than necessary, anonymization	**Yes**	Information will be retained and disposed of in line with IA records management plan
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.6 GDPR Articles 12-22 – data subject rights	**Yes**	The information processing tools on SCOTS support searching and identification of subjects information. Subject access rights will be complied with unless a statutory exception applies.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.7 Principle 6 - security	**Yes**	The SCOTS IT system is demonstrably secure and encryption safeguards will be employed when moving data out of this environment.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.8 GDPR Article 24 - Personal data shall not be transferred to a country or territory outside the European Economic Area.	**Yes**	No personal information will be transferred outside of the EU.

8. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result
Data is Breached by IA	1	• Data is stored within eRDM or Galileo, these systems are administered by Scottish Government iTechs colleagues in line with SG policy, therefore risk of data breach is minimal. If a data breach is discovered, for example an erroneously sent email, this will be handled in line with SG data breach guidelines, and the appropriate actions taken. In addition all IA staff undertake mandatory Annual SG training on data handling.	Reduced

Data is Breached by Sub-Processor	2	• Sub Processors will only process data on behalf of Internal Audit after signing a contract/MoU to do so. These documents contain clauses outlining the data security standards.	Reduced
Data is Lost	3	• All data is stored within eRDM or Galileo. These systems are subject to regular backups by iTechs colleagues in line with Scottish Government policy. Therefore the risk of data loss is minimal.	Reduced

9. Data Protection Officer (DPO)

The DPO may give additional advice, please indicate how this has been actioned.

Advice from DPO	Action

10. Authorisation and publication

The DPIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the DPIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the DPIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "DPIA report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a DPIA has been conducted.

I confirm that the impact of (undertaking the project/applying the policy – add appropriate wording) has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	**Date each version authorised**
Jennifer Inglis-Jones Deputy Director Internal Audit and Assurance	**July 2020**