Data Protection Policy
Appropriate Policy Document

Contents

Information Assurance & Data Protection
Last updated:

Document Control

Date	Version	Name	Role	Reason For Change
9 August 2019	0.1	Helen Findlay	Author	First draft
30 April 2020	1.0	Helen Findlay	Author	Final version 1
20 July 2021	2.0	Nicholas Reid	Edit	Update to legislation referenced, formatting.

1. Introduction

The UK General Data Protection Regulation (UKGDPR) and the Data Protection Act (DPA) 2018 impose obligations on the use of all personal data held by the Scottish Government, whether it relates to people and their families, employees, complainants, contractors or any other individual who comes into contact with the organisation, defined as data subjects.

This policy sets out how the Scottish Government meets its legal obligations and requirements under data protection law, and how it will protect special category and criminal convictions personal data, and processing for the purposes of law enforcement.

This policy will be reviewed annually, or as appropriate to take into account changes to legislation that may occur. Any breach of this policy may result in the Scottish Government being liable for the consequences of the breach.

2. Roles and responsibilities

The Permanent Secretary, as **Accountable Officer (AO),** has overall responsibility for data protection within the Scottish Government.

The Director General of Organisational Development and Operations is designated as the Scottish Government's **Senior Information Risk Owner (SIRO).**

The Data Protection Officer (DPO) is responsible for data protection assurance and compliance, and reports key findings and recommendations to the Executive Team.

Information Asset Owners (IAO) are responsible for maintaining, registering and safeguarding information assets. IAOs also have a responsibility to ensure compliance with data protection law within their business area.

Information Assurance and Data Protection Branch provide advice and guidance and training to the staff of the Scottish Government.

3. The data protection principles

Article 5 of the UK General Data Protection Regulation outlines the six data protection principles (detailed below) which must be adhered to when processing personal data

Article:	The Scottish Government will:
5(1)(a) – Lawfulness, fairness and transparency Processed lawfully, fairly and in a transparent manner in relation to individuals	• ensure that personal data is only processed where a lawful basis applies • process personal data fairly, and inform data subjects about the purposes of any processing. • ensure that data subjects receive full privacy information via a privacy notice, which will include the period for which personal data will be retained.
5(1)(b) – Purpose limitation Collected for specified, explicit and legitimate purposes and not further processed in a manner	• collect personal data for specified, explicit and legitimate purposes and inform data

Article:	The Scottish Government will:
that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes	subjects what those purposes are via a privacy notice • not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use data for a new purpose which is compatible, we will inform the data subject first.
5(1)(c) – data minimisation Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	• only collect the minimum personal data that we need for the purpose for which is it collected. We will make sure that the data we collect is accurate and relevant.
5(1)(d) – accuracy 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	• ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.
5(1)(e) – storage limitation 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals	• only keep personal data in an identifiable form as long as is necessary for the purposes for which it is collected, where we have a legal obligation to do so, or for archiving, scientific or historical research, or statistical purposes. Once we no longer need personal data it will be deleted, put beyond use or anonymized.
5(1)(f) – integrity and confidentiality (security) 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	• ensure that there are appropriate organisational and technical measures in place to protect personal data.
5(2) – accountability the controller shall be responsible for, and be able to demonstrate, compliance with the principles	• keep records of all personal data processing activities and provide these to the Information Commissioner on request • undertake a data protection impact assessment for all projects that involve personal data or privacy, with particular attention to high-risk processing activities • consult the Information Commissioner when preparing proposals for legislation which relates to processing of personal data.

To meet the overarching requirement of accountability we maintain adequate records of our data processing activities and keep evidence of how we comply with the data protection principles.

4. Law enforcement

The Scottish Government has some specialist reporting functions in respect of law enforcement for the following purposes:

- fisheries licensing and enforcement
- agriculture and rural enforcement.

When processing for law enforcement purposes, in addition to the above principles the Scottish Government will

- ensure our systems comply with the data logging requirements
- classify data subjects appropriately
- ensure appropriate safeguards are in place.

5. The legal bit

This policy meets the requirement Schedule 1 to the Data Protection Act 2018 that an appropriate policy document is in place where the processing of special category data is necessary for the purposes of performing obligations or rights in connection with employment, social security or social protection.

It meets the requirement at Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category data is necessary for reasons of substantial public interest. The conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018.

The Scottish Government (Scottish Ministers) is named as a competent authority for the purpose of Part 3 of the Data Protection Act 2018 which applies to the processing of personal data by such authorities for law enforcement purposes, these are described above.

6. Further information

For further information about the Scottish Government's compliance with data protection law, please contact:

Information Assurance and Data Protection Branch dpa@gov.scot

The Data Protection Officer dataprotectionofficer@gov.scot