

Data Protection Policy

1. Purpose and scope

1.1 This policy sets out the commitment of the Keeper of the Registers of Scotland (RoS) to exercise best practice when processing personal data, to comply with data protection law (including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA)), and to uphold the rights of individuals to privacy.

1.2 This policy applies to all processing of personal data by RoS.

1.3 Definition of key terms is included at [Annex A](#).

2. Data protection law and principles

2.1 Data protection law governs the processing of personal data by a data controller, or by a data processor on their behalf. It sets out obligations for organisations processing personal data, and rights for individual data subjects. RoS acts as both a data controller and a data processor in the course of its activities.

2.2 The UK GDPR sets out seven key principles for the processing of personal data, these are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

3. Lawfulness, fairness and transparency

3.1 RoS will process all personal data in line with a lawful purpose, as set out in UK GDPR, and will record this purpose in its record of processing.

3.2 RoS seeks to help individuals understand how it processes their personal data through clear, transparent communications such as the privacy statement on the RoS website and other information provided to individuals at or after the point of data collection.

4. Purpose limitation

4.1 RoS will process personal data for specified, explicit and limited purposes, and will not further process that data for incompatible purposes. Processing of personal data beyond the purpose for which it was originally collected will be risk assessed to ensure that it complies with the data protection principles.

5. Data minimisation

5.1 RoS will process personal data which is adequate, relevant and limited to what is necessary for its purpose. Data collection and use will be risk assessed to ensure that excessive or unnecessary data is not processed.

5.2 Anonymisation and pseudonymisation of data will be considered and applied where appropriate to ensure that individuals are identified only where necessary.

6. Accuracy

6.1 RoS will process personal data which it understands to be accurate, complete, up-to-date, and relevant to its purpose. Where inaccuracies are found, these will be addressed prior to further processing, or the data deleted. RoS will take all reasonable steps to ensure that personal data remains accurate over time.

7. Storage limitation

7.1 RoS will retain personal data only for as long as is necessary to its purpose and will apply clearly defined rules governing the retention and disposal of data, in line with the RoS Retention Framework. Destruction of personal data will be carried out securely and in line with the RoS Disposal Standard.

7.2 Where exceptions to these rules are necessary, reasons for this will be recorded, and steps taken to ensure that personal data adequately protected.

7.3 RoS will continually develop and implement safeguards to protect personal data, ensuring these remain in line with developments in technology and the threat landscape, applying them consistently and proportionately based on risk. Regular reviews of safeguard effectiveness will also be carried out.

8. Security and data breaches

8.1 RoS will implement appropriate organisational and technical measures to protect personal data against unauthorised or unlawful processing, and against accidental loss, destruction or damage. Such measures will protect the confidentiality, availability and integrity of personal data at all times.

8.2 RoS will implement policy and procedure for the encryption of data, the application of controls to data access, and the transfer of data beyond RoS (including internationally).

8.3 RoS will operate appropriate procedures for managing any information security incident that constitutes a personal data breach, including notification to the ICO if required. Assessment of data breaches and, where appropriate reporting, is the responsibility of the Data Protection Officer (DPO).

9. Accountability

9.1 RoS will put adequate resources and controls in place to ensure, and evidence, compliance with the data protection principles and data protection law. These will include:

- Appointment of a DPO
- Implementation of privacy by design and Data Privacy Impact Assessments (DPIAs)
- Maintenance of detailed records of processing activities
- Maintenance of appropriate consent and contract documentation
- Regular training and awareness activities for staff and contractors
- Regular testing and review of its controls to privacy

9.2 Records of processing activities will be kept up to date and will be made available for inspection by the Information Commissioner's Office (ICO) upon request.

10. Special category and criminal offence data

10.1 Data protection legislation defines categories of personal data which require additional conditions to be met for their processing to be fair and lawful. RoS will process such data in accordance with the data protection principles, and in accordance with this policy.

10.2 The RoS record of processing will detail any processing of special category or criminal offence data alongside the purpose and lawful basis (including the relevant condition from Schedule 1 Parts 1-3 of the DPA), and this information will be reviewed biannually.

11. Individuals' Rights

11.1 RoS will fulfil its obligations to uphold individuals' rights and will operate procedures to appropriately manage requests received from individuals to exercise their rights. These requests will be managed by the DPO.

12. Data sharing and disclosure to third parties (including beyond the UK)

12.1 Personal data will be disclosed to third parties appropriately and governed by data sharing agreements and data processor contracts which will provide for appropriate safeguards. Disclosure will be in line with a specific and lawful purpose which will be identified prior to disclosure.

12.2 Where RoS transfers personal data beyond the UK, including to its data processors, it will do so in line with a relevant condition as set out in data protection legislation, and with any required contractual clauses in place, thereby providing an appropriate level of protection for personal data. Such transfers will be risk assessed and the relevant condition recorded in our record of processing.

13. Privacy by design

13.1 Privacy by design is a series of best practice principles which embed privacy considerations in the culture of the organisation.

13.2 RoS is committed to privacy by design and to the consistent use of risk assessments and Data Protection Impact Assessments (DPIAs), which are

mandatory in certain circumstances, to improve the early identification and mitigation of privacy risk and to ensure we meet our obligations in respect of data protection law.

13.3 DPIAs will be considered wherever there is significant a change to the way personal data is processed. The DPO will advise as to whether a DPIA is required, including whether a statutory requirement to conduct a DPIA exists. The DPO will notify the ICO of a DPIA in circumstances where data protection law requires it.

14. Training and awareness

14.1 RoS will ensure that all its staff and contractors understand their responsibilities in relation to data protection and privacy by providing regular training opportunities, including specialised training for those working in areas, or undertaking roles, with higher privacy risk.

14.2 Where customers and stakeholders have a role in helping to fulfil this policy, RoS will communicate appropriately with them to help them understand and meet its expectations.

15. Roles and responsibilities

15.1 All RoS staff and contractors have responsibilities for data protection and privacy, are bound by the commitments of this policy, and are required to effectively operate the various operational procedures which facilitate its fulfilment in practice.

15.2 The RoS DPO has operational responsibility for data protection and privacy within RoS. Their role is mandated and governed by data protection legislation and is an impartial advisory role to the organisation's highest level of management. They must act as the RoS point of contact with the ICO and are responsible for ensuring that the procedures and training which support the fulfilment of this policy are operated effectively and kept up to date.

15.3 The RoS Senior Information Risk Owner (SIRO) has strategic oversight and overall accountability for data protection and privacy within RoS.

15.4 The RoS Executive Management Team is responsible for ensuring that the commitments given in this policy are met, and that the privacy function is appropriately resourced and accounted for within the wider governance of RoS.

15.5 The RoS Board is responsible for ensuring that the DPO is able to fulfil their role impartially and without conflict of interest and can operate according to the requirements set out in data protection legislation.

15.6 RoS expects its Data Processors and Data Sharing Partners to assist in meeting the commitments given in this policy, to uphold the agreements made in data processing contracts and data sharing agreements, and to fulfil their own statutory obligations in respect of data protection.

16. Review

16.1 This policy will be reviewed and approved by the RoS Information Assurance Group at two-year intervals, unless earlier review is appropriate.

Author	Head of Information Governance		
Reviewed	Head of Risk and Information Governance		
Cleared	Corporate Director		
Approval	IAG	Approval Date	January 2023
Policy Version	4.0		
Review Responsibility	IAG	Review Date	January 2025
Suitable for Publication	Y		
Contact:	dataprotection@ros.gov.uk		

Annex A_– Definitions of Key Terms

Anonymisation – The process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

Criminal conviction data - Personal data relating to an individual’s criminal convictions, or the alleged prosecution of offences, is covered by additional safeguards and cannot be processed unless under official authority or where authorised by law.

Data controller - An organisation processing personal data, and which determines the purposes and means of processing that personal data

Data processor – An organisation processing personal data on behalf of a data controller, acting on their instruction.

Data Protection Impact Assessment (DPIA) – Also known as privacy impact assessments. A form of risk assessment that can help identify privacy risk at an early stage in the change cycle to allow that risk to be controlled appropriately.

Data Protection Officer – The Data Protection Officer (DPO) is a role required for certain organisations under the GDPR. DPOs are responsible for overseeing data protection strategy and implementation to ensure compliance with data protection legislation.

Data subject – The ‘natural person’ to whom the personal data relates and who is identifiable from that data.

Data subjects’ rights – Data protection legislation sets out the following rights for data subjects:

- To be informed
- To access personal data
- To rectification of inaccurate personal data
- To erasure of personal data
- To restrict processing of personal data
- To data portability
- To object to processing of personal data
- To protection from automated decision making, including profiling

Encryption – The process of encoding information or data so that only authorised parties can access it.

Lawful purpose - Data subjects’ rights – Data protection legislation sets out the following rights for data subjects:

- To be informed
- To access personal data

- To rectification of inaccurate personal data
- To erasure of personal data
- To restrict processing of personal data
- To data portability
- To object to processing of personal data
- To protection from automated decision making, including profiling

Personal data - Information relating to an identifiable person who can be directly or indirectly identified. Includes names, staff number, location data, online identifier (eg IP address) and pseudonymised data

Processing - The use of personal data in any way – this includes collecting, creating, analysing, copying, storing, transferring, sharing, disclosing, publishing and disposing of personal data.

Pseudonymisation – De-identifying data so that a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without that individual being identified directly. Legally, this data remains personal data.

Record of Processing – A record of the activities an organisation undertakes that involve the processing of personal data. This is a legal requirement and must contain certain information in relation to each processing activity.

Special category personal data – types of personal data which require additional safeguards and conditions to be met for processing to be fair and lawful. Categories are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data
- Sex life or sexual orientation