Data Protection Policy

Author	Data Protection Officer		
Reviewed	Head of Risk and Information Governance		
Cleared	Corporate Director		
Approval	IAG	Approval Date	December 2020
Policy Version	3.0		
Review Responsibility	IAG	Review Date	December 2022
Suitable for Publication	Y		
Contact:	dataprotection@ros.gov.uk		

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 General Data Protection Regulation (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 in the course of its functions and activities.

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 GDPR sets out principles for the processing of personal data. These are that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- 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

2.3 Further obligations include:

- Upholding individuals' rights
- Demonstrating accountability by evidencing compliance with the data protection principles
- Appropriately safeguarding any transfer of personal data outside the UK

3. Lawfulness, fairness and transparency

3.1 The GDPR sets out the lawful purposes for which personal data may be processed. These are that:

a. The data subject has given his or her consent
b. The processing is necessary for the performance of a contract with the data subject
c. The processing is necessary to fulfil a legal obligation on RoS
d. The processing is necessary to protect the data subjects' vital interests
e. The processing is necessary for the public interest
f. The processing is necessary for the legitimate interests of RoS or a third party

3.2 RoS will process all personal data in line with a lawful purpose and record this purpose in its record of processing.

3.3 RoS will meet its obligations to fair and transparent processing using communications such as the privacy statement on the RoS website and other information provided to individuals at or after the point of data collection. RoS seeks to help individuals understand how it processes their personal data.

4. Special category data

4.1 Data protection legislation defines categories of personal data which require additional conditions to be met in order 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.

4.2 The RoS record of processing will detail any processing of special category data alongside the purpose and lawful basis (including the relevant condition from Schedule 1 Parts 1-3 of the DPA), and the applicable retention and erasure policy which will be applied. It will be available for inspection by the Information Commissioner's Office (ICO) upon request.

5. Purpose limitation

5.1 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 and in particular that it is fair and lawful. Such processing will be detailed in the RoS record of processing.

6. Data minimisation

6.1 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.

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

7. Accuracy

7.1 RoS will process personal data which it understands to be accurate, complete, up-to-date and relevant to its purpose. Where personal data is found to be inaccurate, that inaccuracy 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.

8. Storage limitation

8.1 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 (as set out in our corporate retention schedule). Destruction of personal data will be carried out securely.

8.2 Where retention beyond these rules is necessary, the reasons for this will be recorded, and steps taken to ensure that personal data is removed or obscured using techniques such as anonymisation or pseudonymisation.

9. Security and data breaches

9.1 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.

9.2 RoS will continually develop and implement safeguards to protect personal data, apply these consistently, and regularly review their effectiveness. Such safeguards will be proportionate and appropriate to risk, considering sensitivity and volume of data, and potential for damage or distress to data subjects which might result from unauthorised or unlawful processing.

9.3 Safeguards will be designed and implemented having account for the current state of technology and the evolving nature of threats to personal data in the digital environment.

9.4 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).

9.5 RoS will operate appropriate procedures for managing any information security incident which may constitute a personal data breach. Notification of personal data breaches to the ICO and data subjects is legally mandated in certain circumstances. Assessment of data breaches and, where appropriate reporting, is the responsibility of the Data Protection Officer (DPO).

10. **Individuals' Rights**

10.1 RoS will fulfil its obligations to uphold individuals' rights:

a. To be informed
b. To access personal data
c. To rectification of inaccurate personal data
d. To erasure of personal data
e. To restrict processing of personal data
f. To data portability
g. To object to processing of personal data
h. To protection from automated decision making, including profiling

10.2 RoS will operate procedures to appropriately manage requests received from individuals to exercise their rights; these will be managed by the DPO.

10.3 Information relating to these rights, and the procedures in place to manage rights requests, will be communicated to all staff through training and communications.

11. Accountability

11.1 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 the appointment of a DPO, the implementation of privacy by design and Data Privacy Impact Assessments (DPIAs), the maintenance of detailed records of processing activities, maintenance of appropriate consent and contract documentation, regular training of staff and contractors, and regular testing and review of its controls to privacy.

11.2 Records of processing activities will be kept up to date and will be reviewed every six months in respect of the processing of special category data.

12. International transfers of personal data

12.1 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 controls in place, thereby providing an appropriate level of protection for personal data. Such transfers will be risk assessed and recorded in our record of processing.

13. Data sharing and disclosure to third parties

13.1 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.

14. Privacy by design

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

14.2 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.

14.3 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.

15. Training and awareness

15.1 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.

15.2 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.

16. Roles and responsibilities

16.1 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.

16.2 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.

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

16.4 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.

16.5 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.

16.6 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.

17. Approval and Review

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

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 data protection legislation. DPOs are responsible for overseeing data protection strategy and implementation to ensure compliance with data protection legislation.

Data sharing - The sharing of data, usually personal data, between data controllers, typically on a repeated or regular basis.

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

Disclosure - The sharing or publication of personal information with any organisation or individual. It can also be used to describe the sharing of personal information *within* an organisation, in a way which would not normally be expected.

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

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 in 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 in order 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