National Records of Scotland

Data Protection Policy

May 2020

1. Introduction

1.1 At National Records of Scotland (NRS) we take our customers' trust and right to privacy seriously. We are committed to ensuring that whenever we process personal data we do so fairly, lawfully and in a transparent manner, and in compliance with data protection and privacy laws, including the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the Data Protection Act 2018 (DPA 2018).

1.2 The GDPR, which came into effect on 25 May 2018, has introduced a new framework of rights and duties for the protection of personal data. The Regulation harmonises data privacy laws across Europe and strengthens and extends individuals' rights and protections.

1.3 The DPA 2018 ensures that the standards set out in the GDPR have effect in the UK, strengthens or provides exceptions from some of the requirements of the GDPR, extends data protection laws to areas which are outside the scope of the GDPR, and implements the EU Law Enforcement Directive.

1.4 NRS is committed to ensuring that all of our employees comply with their obligations under the GDPR and the DPA 2018 and to safeguarding the integrity and confidentiality of any personal data held or processed by us.

1.5 Our priority will always be to ensure that the rights and freedoms of individuals are protected before we carry out any processing of personal data. Employees should be aware that failure to comply with data protection laws not only risks infringing the rights of individuals, but may also result in loss of reputation, loss of public and stakeholder trust, substantial fines and criminal proceedings against the organisation and individuals.

2. Purpose and Scope

2.1 The purpose of this policy is to set out our obligations under data protection laws, demonstrate our commitment to compliance with these, and explain the measures we have put in place in order to achieve this.

2.2 The policy aims to fulfil the requirement for the fair, lawful and transparent processing of all personal data, both in the records which NRS creates and receives in the course of carrying out its functions and administering its own business, and also in the records of organisations and private individuals deposited with NRS for historical purposes.

2.3 The policy relates to all staff and applies to all records regardless of format or medium, including paper, electronic, audio, visual, microform and photographic.

3. Data Protection Principles

3.1 Article 5 of the GDPR sets out six principles relating to the processing of personal data which NRS must be able to demonstrate compliance with. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner 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;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) 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;

(e) 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;

(f) 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.

4. Definitions of Personal Data

4.1 Personal data are information that relates to an identified or identifiable individual.

4.3 The GDPR definition of what constitutes personal data is more detailed and has been expanded to include a wide range of personal identifiers, reflecting changes in technology and the way organisations collect information about people. For example, online identifiers like IP addresses can be personal data.

"Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more

factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

4.4 The GDPR replaces the term 'sensitive personal data' with processing of special categories of personal data:

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

5. Personal data processed by NRS

5.1 NRS processes personal data in order to:

- administer public and government services
- maintain accounts and records
- support and manage our staff
- enumerate the census
- produce statistics
- carry out and facilitate research
- manage archives
- administer civil registration
- provide a health administration service
- promote our goods and services
- administer membership records
- assist crime prevention and prosecution of offenders (including CCTV)
- administer information and databanks
- provide consultancy and advisory services

5.2 NRS processes the following categories of personal data:

- personal details – e.g. name, address, etc
- family, lifestyle and social circumstances
- financial details
- employment details
- education and training details
- personal identifiers – e.g. identification numbers, online identifiers

5.3 NRS processes the following special categories of personal data:

- criminal proceedings, outcomes and sentences
- offences (including alleged offences)
- physical or mental health
- political opinions
- racial or ethnic origin
- religious beliefs

- sexual life
- trade union membership

5.4 NRS processes personal data about following categories of individuals:

- business contacts
- customers and clients
- individuals featured in archival records
- persons enumerated in Scotland
- suppliers
- members of the public who use our services
- offenders and suspected offenders
- patients
- staff, including volunteers, agents, temporary and casual workers
- students and pupils

6. Policy Statement and Commitment

6.1 In order to fulfil our obligations under data protection law NRS is committed to:

- making data subjects aware of when we collect personal data about them, and explaining the ways in which that information will be used;
- making data subjects aware of their rights and how they can exercise them;
- ensuring that there is a lawful basis for any processing;
- ensuring that processing is fair and will not be unduly detrimental, unexpected or misleading to individuals;
- processing personal data which are adequate, relevant and limited to what is necessary for the intended purposes;
- ensuring that personal data are accurate and kept updated;
- retaining personal data only for as long as they are needed;
- taking appropriate technical and organisational measures to safeguard the integrity and confidentiality of personal data;
- ensuring that personal data are not transferred outside the EEA without appropriate safeguards;
- maintaining records of processing activities and organisational compliance.

With exemptions, where appropriate, for personal data which are processed only for public interest archiving, statistical purposes, or historical research purposes.

6.2 This is achieved through:

- use of privacy notices and privacy information to inform data subjects wherever the collection and processing of personal data takes place, outlining the purposes for which the data will be used, who it will be shared with, how it will be securely retained, and how individuals may access it;

- quick and efficient handling of subject access requests and other information rights requests;
- identification of a Data Protection Officer, at director level, with specific operational responsibility for data protection in NRS;
- training all NRS staff in data protection and information management in order to ensure that they understand their obligations;
- operation and regular review of comprehensive procedures for the management and security of all NRS information, regardless of media or format;
- maintenance of an information asset register and records of processing activities;
- regular monitoring, review and audit of the way in which personal data are collected, stored and used by NRS
- active use of retention and disposal schedules to ensure that information is only retained for as long as it is required;
- ensuring individuals are aware of their obligations when being given access to personal data for research purposes;
- sharing information lawfully and in accordance with the Information Commissioner's Office Data Sharing Code of Practice; entering into data sharing agreements with third parties, which clearly state the terms under which information will be shared;
- entering into data processing agreements whenever NRS processes personal data on behalf of another data controller, or where NRS contracts data processing services;
- carrying out data protection impact assessments before we begin any processing of personal data which is likely to result in a high risk to individuals;
- carrying out privacy compliance checks to assess compliance with the data protection laws;
- engaging and consulting with the Information Commissioner's Office directly on policy and process discussions touching on privacy, data sharing and other data protection issues;
- notifying the Information Commissioner's Office of any reportable personal data breaches within 72 hours of becoming and notifying individuals where there is a high risk to their rights and freedoms.

7. Roles and Responsibilities

7.1 All staff within NRS must comply with the principles set out in this policy. Breaches of this policy and therefore data protection laws may lead to disciplinary action, in line with Scottish Government's 'Civil Service Code' and associated disciplinary procedures. Colleagues must familiarise themselves with, and follow this policy and the supporting codes of practice, ensure that procedures for the collection and use of personal data are complied with in their area, and familiarise themselves with the implications of data protection for their role.

7.2 The Registrar General for Scotland / Keeper of the Records of Scotland as data controller for NRS has primary responsibility for ensuring that all collection and processing of personal data within the organisation complies with the data protection laws and principles.

7.3 The NRS Data Protection Officer, supported by the NRS Information Governance Team, has responsibility for identifying and publicising responsibilities for data protection within NRS, in accordance with this policy.

7.4 Senior management regard the lawful and correct treatment of personal data as of vital importance to the success of our business operations, and to maintaining the confidence of our stakeholders. Senior management will make provision for a regular review of this policy and investigate modifications when necessary.

7.5 The Information Governance Team will ensure that this policy and other internal policies relating to data protection are kept up to date, provide advice, guidance, training and support to staff to help ensure that they comply with their obligations under the data protection laws, maintain the information asset register and records of processing activities, monitor and report on the effective operation of data protection systems.

7.6 Line managers must ensure that all of their staff actively consider their data protection obligations when performing their duties and undertake mandatory data protection training annually.

8. Legislative Framework

8.1 Compliance with this policy will help facilitate compliance with the following legislation, regulations and standards.

- Census Act 1920
- Data Protection Act 2018
- Equality Act 2010
- General Data Protection Regulation (Regulation (EU) 2016/679)
- Freedom of Information (Scotland) Act 2002
- Human Rights Act 1998
- Local Electoral Administration and Registration Services (Scotland) Act 2006
- Public Records (Scotland) Act 2011
- Statistics and Registration Service Act 2007
- UK Statistics Authority – Code of Practice for Official Statistics 2009

8.2 NRS operates in accordance with HMG Security Policy Framework, HMG Information Assurance (IA) standards and their associated Good Practice Guides / Supplements / IA Notices.

8.3 NRS also aims to operate in accordance with the following best practice standards for security and recordkeeping:

- BS ISO 27001:2013 – Information Technology – Security Techniques Information security management systems – Requirements
- BS EN 15713:2009 – Secure Destruction of Confidential Material
- BS ISO 15489-1:2016 – Information and Documentation – Records Management (Parts 1 & 2)

9. Monitoring and Review

9.1 Compliance with this policy and related standards and guidance will be monitored by the NRS Data Protection Officer and Information Governance Team, in consultation with the Registrar General / Keeper of the Records of Scotland. The policy will be reviewed at least every two years in order to take account of any new or changed legislation, regulations or business practices.