DATA PROTECTION POLICY

Implementation date: 1 February 2019
Review date: 1 February 2021

Data Protection Policy

1. Purpose

1.1. The purpose of this document is to set out how, as a data controller, the Attorney General for Northern Ireland (AGNI) protects personal data.

2. Introduction

2.1. As a data controller, the AGNI is fully committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

2.2. Within the Office of the Attorney General for Northern Ireland (OAGNI) we collect and use personal data in order to carry out our business. Our data subjects include members of the public, other NI Departments, clients, customers, suppliers, and current, past and prospective employees. All personal information will be processed with care, however it is collected, recorded and used, and whether it is within manual files, held electronically or recorded by any other means.

2.3. The OAGNI has governance and accountability measure in place to ensure that all employees and other parties who have access to personal information (including special categories of personal data) held by or on behalf of the OAGNI are fully aware of and abide by their duties and responsibilities under the legislation.

3. Data Protection Principles

3.1. OAGNI fully supports and complies with the six principles of the GDPR. In summary, this means that personal information will be:

I. processed lawfully, fairly and in a transparent manner;

II. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes:

III. adequate, relevant and limited to what is necessary;

IV. accurate, and where necessary, kept up to date;

V. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed; and

VI. 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. Governance Structure

4.1. The OAGNI has a strong commitment at senior management level to the safeguarding of personal data.

4.2. The Senior Management Team takes overall ownership of the organisation's information risk policy and is responsible for ensuring that information risk is managed appropriately.

4.3. A Data Protection Officer is appointed to monitor internal compliance and inform and advice on data protection obligations.

5. Processing of Personal Information

5.1. The OAGNI will, through appropriate training and responsible management:

- take a privacy by design approach to all work to incorporate data protection compliance at an early stage;
- fully observe conditions regarding the fair collection and use of personal information and special category data;
- maintain appropriate documentation on processing activities;
- provide clear, easily accessible privacy information to inform data subjects about the collection and use of their personal data;
- collect and process personal information only to the extent that it is needed to fulfil operational needs, or to comply with legal requirements;
- ensure the quality and accuracy of personal information used;

- apply strict checks and appropriate data retention schedules to determine the length of time personal information is held;
- ensure that data subjects can fully exercise their rights under the data protection legislation;
- respond to subject access requests promptly and within one month of receipt;
- put in place appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without adequate safeguards; and
- ensure all personal data is held in line with information assurance, information management and records management policy.

6. Compliance

6.1. The Data Protection Officer will ensure that:

- only staff who need access to personal information as part of their duties are authorised to do so;
- all staff processing personal information are appropriately trained and supervised; and
- procedures for handling personal information are clearly understood, available and regularly reviewed.

7. Staff Responsibilities

7.1. All staff managing and processing personal information are directly and personally responsible for following good data protection and records management practice.

7.2. They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss, disclosure or destruction, and in particular will ensure that:

- they complete annual training in the handling of personal information;

- they have a specific data protection objective in personal performance agreements;
- all records and documents containing personal / special category data are processed securely;
- personal data held electronically is protected by use of secure passwords; and
- individual passwords are not easily compromised.

7.3. When staff process information about other people, they must comply with this policy and OAGNI data handling procedures. Staff must not disclose personal information outside this guidance or use data held on others for their own purposes.

8. Data Breach Management

8.1. In the event of a data breach, staff must follow procedures set out within the OAGNI Data Breach Management Policy. The purpose of this is to ensure that a consistent and effective approach is applied to handling data incidents.

8.2. The policy sets out arrangements for the management of incidents and sets out the roles of staff in reporting and investigating breaches.

9. Data Sharing

9.1. Data sharing means the disclosure of information from the OAGNI to a third party organisation or organisations.

9.2. Before disclosing personal information to another organisation, staff will ensure all sharing is lawful, fair, transparent and in line with the rights and expectations of data subjects.

9.3. If the OAGNI engages a data processor, a written contract will be put in place to ensure both parties understand their obligations, responsibilities and liabilities. Any suppliers who are users of personal information supplied by the OAGNI will be required to confirm and demonstrate that they will abide by the requirements of the legislation and the terms and conditions of the contract.

9.4. Where personal data is shared with another public authority, a data sharing agreement is required to define a common set of rules to be adopted by all parties subject to the data sharing operation.

9.5. Data sharing agreements and contracts will be drawn up in line with Department of Finance guidance on Data Sharing.

10. Policy Awareness

10.1. A copy of this policy will be given to all new members of staff and interested third parties. Existing staff and any relevant third parties will be advised of the policy which will be posted on our website. It can be made available in other formats on request to the Data Protection Officer.

10.2. All staff and relevant third parties must be familiar and comply with this policy at all times. The policy will be reviewed every two years.

11. Contact

11.1. In the event that a data subject has a concern or complaint in relation to the OAGNI's handling of personal data or wishes to exercise their rights under the legislation, they can contact the Data Protection Officer. Data subjects can also complain to the OAGNI if they are dissatisfied with our response to a subject access request. We aim to respond to complaints or queries within 20 working days of receipt of correspondence.

11.2. The Data Protection Officer can be contacted as follows:

Data Protection Officer
OAGNI
PO Box 1272
Belfast
BT1 9LU
Email: contact@attorneygeneralni.gov.uk

11.3. Data subjects also have the right to lodge a complaint directly with the Information Commissioner at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Email: casework@ico.org.uk
Website: ico.org.uk/concerns/handling