Northern Ireland Assembly

DATA PROTECTION POLICY

May 2018

CONTENTS

1. Introduction

1.1 The Northern Ireland Assembly Commission (the Assembly Commission) is fully committed to complying with Data Protection legislation[1] including the General Data Protection Regulation ('GDPR') which has applied from 25th May 2018. We will follow procedures to ensure that all employees, contractors, agents, consultants and other parties who have access to any personal data held by, or on behalf of, the Assembly Commission are fully aware of, and abide by, their duties and responsibilities.

2. Statement of Policy

2.1 We need to collect and use information about people with whom we work in order to carry out our business and provide our services. These may include Members of the Assembly, members of the public, current, past and prospective employees, clients, customers and suppliers. In addition, we may be required by law to collect and use information. All personal data must be handled and dealt with properly, however it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means.

2.2 This policy should be read in conjunction with the following Assembly Commission policies and procedures:

i. Assembly Commission Information Assurance Policy;
ii. Policy for the use of IT Resources by Secretariat Staff;
iii. Flexible Working Policy;
iv. Records and Email Management Policy;
v. Social Media Policy;
vi. Retention Policy;
vii. Data Breach Management Plan; and
viii. IS Password Policy.

3. Management and Responsibilities

3.1 The Assembly Commission has overall responsibility for compliance with the GDPR within the organisation. The implementation of, and compliance with, this policy is delegated to the Data Protection and Information Standards Officer and Information Asset Owners. The Director of Legal, Governance and Research Services is designated as the Senior Information Risk Owner ('SIRO') for the organisation for the purposes of the Data Breach Management Plan.

3.2 The Data Protection and Information Standards Officer is responsible for ensuring this policy is communicated to all staff. Information Asset Owners ('IAO') are responsible for ensuring this policy is further communicated and implemented within their area of responsibility. They are responsible for the quality, security and management of personal data in use within their business area. Advice or assistance regarding this policy or the GDPR is available from the Data Protection and Information Standards Officer.

[1] Data Protection legislation means the GPR, the Data Protection Act 2018 and regulations relating thereto.

3.3 Requests for personal data are dealt with by the Data Protection and Information Standards Officer and business areas will be consulted accordingly.

3.4 Information sharing agreements, in line with the ICO code of practice, will be signed on behalf of the Assembly Commission by the Head of Business, or as delegated by the Head of Business within each business area.

3.5 All Data Protection and information related incidents must be reported and properly investigated according to the Assembly Commission Data Breach Management Plan.

3.6 All correspondence with the Information Commissioner's Office ('ICO') on Data Protection matters will be dealt with by the Data Protection and Information Standards Officer.

3.7 This policy will be reviewed annually, and when appropriate, to take into account changes to legislation that may occur, and / or guidance from the Information Commissioner. Appendices outlining the Assembly Commission's policy on specific Data Protection-related projects and issues will be added when required.

4. Principles relating to processing of personal data

4.1 The Assembly Commission fully supports and complies with the principles relating to processing of personal data set out at Article 5 of the GDPR which require that personal data shall be:

i. processed lawfully, fairly and in a transparent manner in relation to individuals;

ii. 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;

iii. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

iv. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

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

5. Registration with the Information Commissioner's Office

5.1 Data Protection legislation requires every data controller who is processing personal data to register with the ICO, unless they are exempt. The Assembly Commission holds a valid registration with the ICO and renews this annually as required. The current registration can be found here.

5.2 The Assembly Commission has conducted an audit of the personal data processed throughout the organisation and produced a register of the processing carried out. IAOs will be required to review the Data Protection register on a quarterly basis to ensure it remains accurate and appropriate at all times. This review will include an update of any required changes or amendments, or altering or removing information as necessary, on a quarterly basis.

5.4 The Assembly Commission record of processing activities under its responsibility, as set out at Article 30 of the GDPR, will replace the previous notification with the ICO.

6. Data Processors

6.1 Where the Assembly Commission uses a contractor to process personal data on its behalf, the contractor must sign a data processing agreement, which ensures that they are taking adequate steps to comply with the Data Protection legislation and act only on the instruction of the Assembly Commission as agreed. The Assembly Commission and the data processor are responsible for their actions in processing personal data.

7. Individuals' Rights

7.1 Under the Data Protection legislation, individuals have the following rights:

i. the right to be informed;
ii. the right of access;
iii. the right to rectification;
iv. the right to erasure;
v. the right to restrict processing;
vi. the right to data portability;
the right to object; and
vii. rights in relation to automated decision making and profiling.

7.2 All requests to facilitate the exercise of data subject rights, under Articles 15-22 of the GDPR, will be facilitated through the Data Protection and Information Standards Officer. Further guidance and instruction will be available on AssISt.

8. Disclosure of Personal Data

8.1 Strict conditions apply to the passing of personal data both internally and externally. The Assembly Commission will not disclose personal data to any third party unless we believe it is lawful to do so. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:

i. we have the statutory power or are required by law to do so; or
ii. the information is clearly not intrusive in nature; or
iii. the member of staff has consented to the disclosure; or
iv. the information is in a form that does not identify individual employees.

8.2 Concerns about providing information should be referred to the Data Protection and Information Standards Officer for advice, for example, if the information includes personal data about a third party. In all cases, the Data Protection and Information Standards Officer should be advised that a request has been received and details for the request recorded.

9. Handling of Personal Data

9.1 All secretariat staff will, through appropriate training and responsible management:

i. fully observe conditions regarding the fair collection and use of personal data;
ii. meet our legal obligations to specify the purposes for which personal information is used;
iii. collect and process appropriate personal data only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;
iv. ensure the quality of personal data used;
v. apply strict checks to determine the length of time personal data is held;
vi. ensure that the rights of people about whom information is held can be fully exercised under the Data Protection legislation;
vii. take appropriate technical and organisational security measures to safeguard personal data;
viii. ensure personal data is secured to prevent access by unauthorised individuals and that all information is kept in adequate storage in line with the information assurance policy;
ix. ensure personal data is not transferred outside the European Economic Area (‘EEA’) without adequate safeguards;
x. ensure Privacy by Design is considered and implemented as necessary in all new policies, procedures, systems, projects, etc.;

xi. ensure Data Protection Impact Assessments ('DPIAs') are carried out where data processing is likely to result in high risk to individuals, for example:
    a. where a new technology is being deployed;
    b. where a profiling operation is likely to significantly affect individuals; or
    c. where there is processing on a large scale of the special categories of data; and
xii. inform the Data Protection and Information Standards Officer where a DPIA indicates that the data processing is high risk which the cannot be sufficiently addressed. The Data Protection and Information Standards Officer will therefore be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

10. Compliance

10.1 The Assembly Commission will ensure that:

i. there is someone with specific responsibility for Data Protection in the organisation;
ii. all staff receive annual awareness of Data Protection legislation;
iii. everyone managing and handling personal data understands that they are directly and personally responsible for following good Data Protection practice;
iv. only staff who need access to personal data as part of their duties are authorised to do so;
v. everyone managing and handling personal data is appropriately trained to do so;
vi. everyone managing and handling personal data is appropriately supervised;
vii. anyone wanting to make enquiries about handling personal data knows what to do;
viii. queries about handling personal data are promptly and courteously dealt with;
ix. methods of processing personal data are clearly described. This is usually done through a privacy notice. The privacy notice will also detail the purpose of processing the personal data; the legal basis for processing; data retention periods; individuals' rights, including the rights to complain to the ICO if they think there is a problem with the way their data is being handled;
x. an information audit of personal data held across the organisation is conducted on an annual basis. This documents what personal data is held, where it came from and who it is shared with. This will include an assessment and evaluation to ensure that all personal data held is accurate and up to date and that adequate controls are in place to ensure information is managed and stored appropriately. This will help the organisation to comply with the Data Protection legislation and demonstrate accountability;
xi. 'Data Protection by design' is implemented as necessary in all new policies, procedures, systems, projects etc.;
xii. DPIAs are carried out as necessary; and

xiii. if a DPIA indicates that the data processing is high risk, and the risk cannot be sufficiently addressed, the ICO will be consulted to seek its opinion as to whether the processing operation complies with the GDPR.

10.2 To assist in achieving compliance, we have:

i. appointed a Data Protection and Information Standards Officer who has overall responsibility for Data Protection within the organisation;
ii. created guidance on the Assembly's Commission's Data Protection procedures in accordance with the Data Protection legislation;
iii. appointed dedicated Information Asset Owners to ensure staff compliance with the Data Protection principles and adherence to the business area procedures;
iv. created monitoring procedures to ensure business area compliance with the Information Assurance Policy (bi-annually);
v. created a register of the personal data processed throughout the organisation; and
vi. created policies and procedures to ensure personal data remains complete, accurate and up to date and managed in line with the Principles.

11. Staff Responsibilities

11.1 All staff have a responsibility to protect the personal data held by the Assembly Commission. Staff must follow policy and procedures to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

i. staff participate in training regarding the handling of personal data;
ii. paper files and other records or documents containing personal / sensitive data are kept in a secure environment in accordance with the Information Assurance Policy;
iii. personal data held on computers and computer systems is stored securely in the shared drive or relevant database, as required; and access control is managed in accordance with the Information Assurance Policy;
iv. individual passwords are not easily compromised and are in accordance with the IS Office Password Policy; and
v. all personal data which staff provide to the Assembly Commission is accurate and up to date and the Assembly Commission is informed of any errors, corrections or changes.

11.2 If and when, as part of their responsibilities, staff collect information about other people, they must comply with the policy and business area procedures. No one should process personal data outside this guidance or use personal data held on others for their own purposes.

12. Third Party Users of Personal Data

12.1 Any third parties who are users of personal data supplied by the Assembly

Commission will be required to confirm and demonstrate that they will abide by the requirements of the Data Protection legislation. Audits may be carried out, as necessary, by the Assembly Commission to ensure compliance.

13. Policy Awareness

13.1 A copy of this policy statement will be given to all new members of Assembly Commission staff and relevant third parties, such as Agency staff and secondees. Existing Commission staff and any relevant third parties will be advised of the policy which will be posted on the Commission website and AssISt, as will any subsequent revisions. All staff and relevant third parties are to be familiar with and comply with this policy at all times.

13.2 Training

The Assembly Commission has a mandatory training programme which includes maintaining awareness of managing information effectively, information assurance and Data Protection issues in accordance with Data Protection legislation. This is carried out by annual training sessions covering the following subjects:

i. Personal responsibilities;
ii. Handling of information in line with the Information Assurance Policy;
iii. Compliance with the Data Protection Principles;
iv. Upholding Individual rights;
v. Adherence to the Records and email management policy; and
vi. General good practice guidelines covering security and information assurance

13.4 Induction

All new starts will receive information governance training as part of the Assembly Commission induction process. Extra training in these areas will be given to those who require it due to the nature of their job. A register will be maintained of all Commission staff attendance at training sessions.

13.5 Contracts of Employment

All contracts of employment include a Data Protection clause. Agency and contract staff are subject to the same rules.