Northern Ireland Assembly

DATA PROTECTION POLICY

Revised September 2026

Contents

1. Introduction 1
2. Data protection policy statement 1
3. Responsibilities 2
4. Role of the Information Standards Office 2
5. Lawfulness, fairness and transparency 3
6. Sharing personal data 4
7. Privacy notices 4
8. Storage limitation 5
9. Security of personal data 5
10. Privacy by design and data protection impact assessments 6
11. Personal data breaches 6
12. Data subject rights 6
13. Data subject complaints 7
14. The data protection register 7
15. Policy Awareness 8
16. Accountability 8

1. Introduction

1.1 When supporting the Assembly in the discharge of its legislative, scrutiny and representative functions the Northern Ireland Assembly Commission (the Assembly Commission) may as part of its day-to-day operations obtain, use and retain personal information (personal data).

1.2 The UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Data Use and Access Act 2025 (collectively 'the data protection legislation') are the principal enactments which address how the Assembly Commission, as a data controller, should obtain, use and retain personal data.

1.3 The Assembly Commission is committed to complying with its legal and regulatory obligations to manage personal data in an appropriate manner, to being clear and transparent about how it obtains and uses personal information, and to communicating how (and when) that information is deleted when it is no longer required.

1.4 This Data Protection Policy (the Policy) sets out the responsibilities of all Assembly Commission employees, contractors, agency workers and consultants (collectively 'Assembly Commission personnel') in that regard. This Policy will help to ensure that Assembly Commission personnel understand and comply with the various data protection requirements to which they are subject in the course of their work.

1.5 The Policy applies to all personal data whether it is on paper or stored electronically and whether it is in writing or stored as verbal or video files. It applies whether the personal data is stored on the Assembly Commission network, on individual desktop or laptop computers, on mobile devices, phones or tablets, in filing cabinets or in any other way.

1.6 The Policy will be reviewed and updated at least **biennially** to ensure that the Assembly Commission continues to comply with obligations under the data protection legislation. Revised versions of the Policy will be published as necessary.

2. Data protection policy statement

2.1 The Assembly Commission complies with all relevant legislative and regulatory provisions governing the management and storage of personal data in electronic and paper formats. The Assembly Commission is registered with the Information Commissioner's Office (ICO) under the data protection legislation.[1]

[1] The current registration can be found here.

2.2 The Assembly Commission complies with the data protection principles set out at Article 5 of the UK GDPR. These require that personal data is—

- processed in a fair, lawful and transparent manner,
- processed for specified, clear and legitimate purposes,
- adequate, relevant and not excessive,
- accurate and up-to-date,
- not kept longer than necessary,
- processed in accordance with the data subject's rights,
- protected securely using appropriate technical and organisational measures, and
- not transferred to non-approved countries without adequate protection.

3. Responsibilities

3.1 The **Assembly Commission** has overall responsibility for compliance with the data protection legislation.

3.2 The **Director of Legal, Governance and Research Services** is the Senior Information Risk Owner (SIRO) for the purposes of the Data Breach Management Plan.

3.3 The **Data Protection and Governance Officer** (DPGO) is responsible for overseeing this Policy and advising Information Asset Owners.

3.4 The DPGO is supported by the **Information Standards Office** (ISO). The contact details for the DPGO and ISO are in Appendix 3.

3.5 **Information Asset Owners** (IAOs) are responsible for ensuring this Policy is communicated and implemented within their business area.

3.6 **Directors, line managers and contract managers**, supported by IAOs, must ensure all Assembly Commission personnel comply with this Policy and implement appropriate controls and training in their business area to maintain compliance.

4. Role of the Information Standards Office

4.1 The ISO provides specialised, tailored advice on processing of personal data, the retention and disposal of personal data, personal data breaches and subject access requests. The ISO **must** be contacted if—

- you are unsure of the legal basis on which you are relying to process personal data (see **paragraph 5** and **Appendix 1**),
- you propose to transfer personal data outside the UK – if for example you are concluding a contract with a corporate body based outside the UK (see **paragraph 6**),

- you intend to draft or revise a privacy notice (see **paragraph 7**),
- you are unsure about the retention period for the processing of personal data, or you propose to change a retention period (see **paragraph 8)**,
- you are unsure about the security measures you should implement to protect personal data, or particular classes of personal data (see **paragraph 9)**,
- you are engaging in a significant new, or change in, processing activity which is likely to require a DPIA (see **paragraph 10**),
- you think there has been a personal data breach (see **paragraph 11**),
- you receive a subject access request (SAR) from an individual concerning the use of their personal data (see **paragraph 12**),
- you receive a complaint from an individual concerning the use of their personal data (see **paragraph 13**), or
- you have any concerns that this Policy is not being followed.

5. Lawfulness, fairness and transparency

5.1 Under the data protection legislation, the lawful processing of personal data requires that the Assembly Commission demonstrate a condition for processing under Article 6(1) of the UK GDPR, and that the processing is a necessary (fair) means of satisfying that condition.

5.2 The usual basis for the processing of personal data by the Assembly Commission is Article 6(1)(e) of the UK GDPR (performance of a task in the public interest) read with section 8(c) and (d) of the DPA.[2] The use of another condition (such as consent) will rarely be appropriate, and if a business area proposes to rely on a basis for processing other than the performance of a task in the public interest, they should discuss this with the ISO.

5.3 The processing of **special category** data (which includes information about an identifiable individual likely to reveal their racial or ethnic origin, political opinions, religious beliefs, and data about their health or sexual orientation) is unlawful unless a condition under Article 6(1) UK GDPR and an additional condition under Article 9 UK GDPR is satisfied. If a business area intends to collect or process special category data (for example, should it be necessary to collect such data as part of a consultation), advice on the processing of this data should be sought from the ISO.

[2] (c) 'the exercise of a function conferred on a person by an enactment or rule of law'; (d) 'the exercise of a function of a government department' (pursuant to Article 9(2) of the Northern Ireland Assembly Commission (Crown Status) Order 1999, the Assembly Commission is treated as a government department for the purposes of section 8(d) of the DPA).

6. Sharing personal data

6.1 Assembly Commission personnel should not share personal data with third parties unless appropriate safeguards and contractual arrangements are in place.

6.2 This paragraph does not affect the sharing of personal data required by any enactment or rule of law (see further Appendix 1).

6.3 Assembly Commission personnel may only share the personal data held by the organisation with third parties, such as contractors, if—

- the third party has a need to know the information for the purposes of providing the contracted services,
- sharing the personal data complies with the privacy notice provided to the data subject,
- the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place,
- the transfer complies with any applicable cross-border transfer restrictions, and
- a written contract that contains UK GDPR-compliant third party clauses has been obtained (the Assembly Commission Standard Terms and Conditions is such a contract).

6.4 The UK GDPR restricts personal data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. If you are managing a contract under which personal data may be transferred outside the UK, you must ensure adequate contractual protections for the transfer of data are in place and consult the ISO if in any doubt.

7. Privacy notices

7.1 The UK GDPR requires the Assembly Commission, as a data controller, to provide specific information to data subjects on the collection and processing of their personal data. This information is set out by relevant business areas in a **privacy notice**.

7.2 A privacy notice must be concise, easily accessible, and in clear and plain language so that it is readily understood by the data subject. A privacy notice will identify the Assembly Commission as a data controller and set out how the organisation will use, process, disclose, protect and retain that personal data.

7.3 The privacy notice should set out the period for which personal data is stored or refer the reader to the appropriate provisions of the Assembly Commission Retention and Disposal Schedule (the R&D Schedule). In considering whether retention of any personal data is necessary, business areas must be particularly aware of the storage limitation requirement in the UK GDPR.

7.4 To facilitate complaints under the UK GDPR all Assembly Commission privacy notices must—

- make clear that the data subject may complain to the Assembly Commission as regards the use of their personal data,
- include an e-mail address to which complaints may be sent, and
- make clear that the data subject can complain to the ICO.

7.5 Most Assembly Commission business areas which collect and process personal data will already have a bespoke privacy notice. If a business area proposes to revise that notice, or if a business area which has not previously collected or processed personal data now has a business need to do so, it must develop and publish a privacy notice. The ISO can assist in this regard.

8. Storage limitation

8.1 Under Article 5 of the UK GDPR, personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. The R&D Schedule sets out retention periods for the disposal of personal data. Any proposed changes to periods set out in the R&D Schedule should be discussed with the ISO.

8.2 The R&D Schedule allows the retention of personal data for the legitimate business purposes for which that data was originally collected by the Assembly Commission and to satisfy legal, accounting and reporting requirements. Under the R&D Schedule, some personal data collected by the Assembly Commission is permanently preserved.

8.3 After the retention period applicable to personal data has expired, each business area must take all reasonable steps to destroy or erase that data. This includes (where applicable) requiring third parties to delete that data.

9. Security of personal data

9.1 The UK GDPR requires that personal data held by the Assembly Commission must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. Particular care is required in protecting special category personal data and criminal conviction data from loss and unauthorised use or disclosure.

9.2 Assembly Commission personnel must follow all procedures and comply with physical and technological measures put in place to maintain the security of personal data from the point of collection to the point of destruction. A failure to follow these procedures may lead to a personal data breach (see paragraph 11).

9.3 Further information on maintaining the security of personal data held by the Assembly Commission is set out in the Records Management Handbook.*

10. Privacy by design and data protection impact assessments

10.1 The UK GDPR requires data controllers to implement **privacy by design** measures when processing personal data by implementing appropriate technical and organisational measures (such as anonymisation and pseudonymization) to ensure compliance with the data protection principles.

10.2 In addition, the Assembly Commission must conduct data protection impact assessments (DPIAs) as regards certain higher-risk processing. DPIAs are required when implementing major system or business change programs involving the processing of personal data including—

- use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes),
- large-scale processing of special categories of personal data or criminal convictions data, and
- large-scale, systematic monitoring of a publicly accessible area.

10.3 Further information on the conduct of DPIAs is published in the Data Protection Handbook. *

11. Personal data breaches

11.1 A personal data breach is a breach of physical or technical security measures leading to the accidental or unlawful destruction, loss, alteration, or disclosure of personal data.

11.2 The Assembly Commission has in place procedures to deal with personal data breaches, and to notify, as necessary, the ICO and any data subject affected. Relevant procedures are set out in the Data Breach Management Policy.

11.3 If you know or suspect that a personal data breach has occurred, refer the matter to the ISO **immediately** in accordance with the procedures set out in the Data Breach Management Policy. You should preserve all evidence related to the suspected breach.

12. Data subject rights

12.1 A data subject has various rights concerning the processing of their personal data. Data subjects may request information held by the Assembly Commission about their personal data and may complain about the collection and processing of their personal data. Data subjects may request—

- information about the Assembly Commission's processing activities,
- access to personal data about them held by the Assembly Commission (including receiving a copy of their personal data),
- restrictions on processing (in specific circumstances),

- a copy of any agreement under which their personal data is transferred outside the UK by the Assembly Commission,
- in limited circumstances, for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

With the exception of requests to Human Resources made by Assembly Commission employees and dealt with in the usual course of business, all subject access requests or other requests concerning the processing of personal data must sent to the ISO, which will manage the request and the response with the relevant IAO.

12.2 Further guidance and instruction on subject access requests is available at Appendix 2 and in the Data Protection Handbook. *

13. Data subject complaints

13.1 Under the data protection legislation, a data subject may make a complaint to the Assembly Commission if he or she considers that there has been an infringement by the Assembly Commission of the UK GDPR as it affected their personal data.

13.2 Data subjects may complain in any way they choose: they may use the e-mail address set out in the relevant privacy notice (see paragraph 7) but may also contact Assembly Commission personnel with whom they have previously interacted, or use Assembly Commission social media channels.

13.3 All complaints by data subjects concerning the UK GDPR and identified as such must be referred to the ISO.

13.4 The ISO will—

- acknowledge receipt of the complaint,
- take appropriate steps to respond to the complaint,
- inform the data subject of the outcome of the complaint, and
- maintain records of complaints received under this paragraph.

14. The data protection register

14.1 The UK GDPR requires the Assembly Commission to keep records of its data processing activities. The Assembly Commission maintains a data protection register for this purpose.

14.2 IAOs must review the data protection register entry for their business area every three months to ensure the continuing accuracy of corporate records concerning the processing of personal data including (if relevant) records of data subjects' consents and procedures for obtaining consents.

15. Policy Awareness

15.1 A copy of this Policy is provided to all new Assembly Commission personnel. The Policy is published on the Assembly Commission website and AssISt. Familiarity with the Policy forms part of mandatory data protection training completed by all relevant Assembly Commission personnel each year.

16. Accountability

16.1 Under the UK GDPR, The Assembly Commission is responsible for, and must be able to demonstrate, compliance with the data protection principles, including the accountability principle.

16.2 Pursuant to the accountability principle, the Assembly Commission will—

(a) Ensure there is someone with specific responsibility for compliance with the data protection legislation

(b) implement privacy by design when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of data subjects,

(c) integrate data protection into internal documents,

(d) regularly train Assembly Commission personnel on the data protection legislation, including data subject rights, legal basis, personal data breaches and maintaining a record of such training, and

(e) conduct periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

---

* Documents marked with an asterisk will be published by 30 November 2026. Until that date, information on these matters may be obtained by contacting the ISO.