Houses of the Oireachtas Commission/ Houses of the Oireachtas Service

Data Protection Policy

Table of Contents

1. Introduction

The Houses of the Oireachtas Commission is a corporate body established under the Houses of the Oireachtas Commission Act 2003 as amended. It is the governing body of the Houses of the Oireachtas Service. The Houses of the Oireachtas Service is the public service body that administers the National Parliament of Ireland (the Houses of the Oireachtas) on behalf of the Houses of the Oireachtas Commission. In this Policy, the two are generally referred to as the **Service**.

This Policy outlines how the Houses of the Oireachtas Service seeks to ensure that it complies with its data protection duties, especially under the General Data Protection Regulation (EU) 2016/679 (the GDPR) and the Data Protection Act 2018.

The mission of the Service is to provide a high-performing Parliamentary Service that enables the Houses of the Oireachtas to discharge their constitutional functions; supports members as representatives of the people, and promotes an open and accessible Parliament.

The primary functions of the Service are to provide advice and support services to —

- the Houses of the Oireachtas Commission
- the Houses of the Oireachtas and their Committees
- Members of the Houses of the Oireachtas[1].

This policy should be read in conjunction with the Service's Records Management Policy, Personal Data Breach Management procedures, Disposal of Records Procedures, Information Security Policy, and CCTV Policy, and the Service's Privacy Notices that apply to particular activities, for example its Website Privacy Notice.

A glossary of terms key to understanding data protection principles is set out in the Appendix to this Policy.

2. How the Service complies with its data protection duties

The Service is responsible for—

1) Data protection governance.

The Service takes its duty to comply with the GDPR and the Data Protection Act 2018 with the utmost seriousness. It has set in place governance procedures to oversee, monitor, and ensure compliance with data protection legislation. Data protection forms part of the overall governance framework of the Service and the relevant governance principles are set out in Office Notice X of 2019.

[1] The two Houses of the Oireachtas (National Parliament) are the Dáil and the Seanad (Senate). Members of the Dáil are known as TDs or Deputies. Members of the Seanad (Senate) are known as Senators. Together they are in this Policy referred to as "Members".

2) Data protection by design and by default. Technical and organisational measures.

Implementation of data protection by design and by default means that data protection principles (see section 5 below) will be embedded into ICT systems or other relevant processes at the earliest stage possible. The Service will ensure that data protection by design and default is built into existing ICT project management guidelines. This addresses matters such as setting up a system so that users cannot gain automatic access across the board to personal data in a database. The Service has established and implemented technical and organisational measures to secure data against unauthorised access, internal or external. These include, for example, an Acceptable Usage Policy and security policies. These measures are continuously reviewed and, where appropriate, upgraded.

3) Record of processing.

As noted under **Accountability** in section 5 "**Data processing principles"** below, the Service maintains a record of processing activities with the particulars prescribed by the GDPR. This will be comprehensively reviewed at least annually.

4) Third party relationships – joint controller/data sharing.

If the Service decides jointly with another data controller (including a Government Department or other public body) on processing personal data, the Service and the other data controller(s) will formally set out their arrangements for complying with their data protection responsibilities and duties except so far as the subject matter is governed by legislation. These arrangements will be transparent. The arrangements may take the form of contracts or memoranda of understanding or bilateral agreements with the relevant third parties with whom or which personal data is shared. The arrangements will specify why the data are shared, security requirements, and provide for how the arrangement is to come to an end, and what is then to happen to the data (usually return or deletion). The Service's privacy notices will describe the effect of these arrangements. Where necessary, the essence of data sharing arrangements will be made available to the relevant data subjects. The arrangements will not restrict the data subject's rights against the Service and the other controller(s).

5) Third party relationships – data processor.

The Service will only engage a third party data processor to process data on its behalf where the processor sufficiently guarantees that it will implement technical and organisational measures so as to ensure that the GDPR is complied with and the rights of data subjects are protected. A third party will not process data on behalf of the Service unless it does so pursuant to a contract or equivalent legally binding instrument in force between the third party and the Service. The contract will clearly set out the respective duties and liabilities of the Service and the processor, and the minimum terms it will include are those set out in the GDPR. In particular, the contract will limit processing by reference to the Service's instructions. It will require the data processor to take technical and organisational measures to implement appropriate levels of security and it will expressly provide, subject to any independent legal obligation to which the processor is subject, for the verified return or deletion of data being processed when it ceases to have effect.

6) Data protection impact assessment (DPIA).

The Service will conduct DPIAs where required before commencing a data processing project, in particular where the project is likely to involve a high risk to privacy and other personal rights. The Service will seek the advice of the Data Protection Officer ("DPO") about the conduct of the DPIA. If the DPIA shows that the high risks cannot be mitigated, the Service will contact the Data Protection Commission before any processing begins.

Members of staff are encouraged to contact the DPO if they are in doubt whether a DPIA is necessary, or where they think one may be appropriate although it is not necessary, or in any other instance where they believe that a particular class of personal data processing may significantly affect a data subject's rights and freedoms.

7) Pseudonymisation and anonymisation.

Where personal data are not immediately required for consultation or use, information may be extracted from those data and stored separately so that the remainder is no longer attributable to a particular person. This is known as pseudonymisation. Alternatively the means of identification may be eliminated entirely, in which instance it is anonymised. Pseudonymisation will be considered by the Service where appropriate as means of ensuring data protection by design and by default, and as a general security measure. Data will be pseudonymised or anonymised where data are processed for archival, historical research or statistical purposes unless to do so would frustrate the purpose in question.

8) Transfer outside the EEA.

If it is necessary to transfer third party data out of the European Economic Area (currently the EU, Iceland, Liechtenstein, and Norway) then the Service will ensure that all the necessary protections and appropriate safeguards are in place.

9) Data breach procedures.

A **personal data breach** includes a **breach of security** leading to **unauthorised disclosure, alteration, loss or destruction of personal data** in any form. A specific set of procedures for **Personal Data Breach Management** and a reporting form are maintained by the Service. It is the duty of a member of staff to comply with these procedures when (s)he believes a breach or potential breach has occurred, principally by reporting the matter to the DPO in accordance with the procedures.

The DPO will comply with his or her duty to report a breach to the Data Protection Commission in accordance with the time limits specified by the GDPR, and will, having assessed the gravity of the breach and any mitigating circumstances in accordance with Article 34 of the GDPR, ensure that the Service informs affected data subjects of the breach as required by that Article.

10) Training.

The Service provides regular staff training with regard to data protection duties. Targeted training is provided where appropriate as a "*suitable and specific measure*" for dealing with special category data as contemplated by section 36 of the Data Protection Act 2018.

3. Scope

This policy applies to all personal data collected, processed and stored by the Service in respect of all individuals, (for example, Members, Members' staff, Service employees, third party service providers, members of the public) by whatever means including paper and electronic records[2].

4. Service as data controller and data processor

The Service is most likely to process personal data as a data controller. The purpose of this Policy is to provide guidance about how the Service deals with personal data as controller.

The Service also processes personal data as **data processor** on behalf of Members in connection with their parliamentary duties. The Member is then the data controller. The personal data are processed by the Service only on the basis of the Member's authorisation and instructions. The same high level of security is applied to the data as to the data the Service keeps or otherwise processes on its own behalf. The Service provides a data processing agreement for Members to sign to comply with their duties on retaining a data processor.

5. Data protection principles

Article 5 of the GDPR establishes 6 principles that all data controllers, including the Service, must observe. That is, personal data must be:

1. **Processed lawfully, fairly, and transparently**

   Lawfulness

   There must be a legal basis for every act of processing. Article 6 of the GDPR specifies six legal grounds for processing personal data. These are where it is necessary for:

   — performing a contract or entry into one, the data subject being (an intended) party

   — compliance with a legal obligation to which the Service is subject

   — protecting a person's vital interests

   — performing a task in the public interest or exercising official authority

[2] Core parliamentary functions are conferred on the Oireachtas by the Constitution or by statute and are broadly in line with the scope of parliamentary privilege. Parliamentary privilege also extends to the work of the Service where this is inextricably linked with the performance by the Houses, their Committees, or Members of core parliamentary functions. If personal data are processed in connection with a core parliamentary function, the GDPR and the Data Protection Act 2018 do not regulate the processing so as to limit parliamentary privilege. This is recognised by section 60(3)(a)(i) of the 2018 Act. Therefore, to the extent that that regulation of processing of personal data would be inconsistent with parliamentary privilege, this Policy does not apply.

— Advancing the Service's legitimate interests, but only if the Service is not performing its public functions (e.g. is acting as employer), and if, on balance, the data subject's rights should not take precedence (e.g. because of prejudice or surprise).

The other ground is that:

— the data subject has given consent.

Usually, the legal basis the Service relies on for processing personal data is the **public interest** or the exercise of **official authority**. The GDPR requires this to be defined in (in this instance) Irish law. Section 38 of the Data Protection Act 2018 permits the processing of data that is "*necessary and proportionate for…the performance of a function of a controller conferred by or under an enactment* [this is defined to include Regulations] *or by the Constitution*."

Article 9 of the GDPR sets out 10 categories of additional justification, at least one of which is required for processing **special category data** (see the Appendix below). So, special category data may not be processed merely for performance of a contract, but may be processed where processing is necessary in the field of **employment law**, for example. **Section 49** of the Data Protection Act 2018 permits the processing of special category data on grounds similar to section 38, but it requires a higher level of justification and additional safeguards. Another ground that applies from time to time to special category data processed in the political context is that the data have been **manifestly made public** by the data subject

The Service acknowledges that processing of personal data relating to **criminal convictions and offences (including allegations)**, and **related security measures**, is subject to special rules under Article 10 of the GDPR and section 55 of the Data Protection Act 2018 and complies with these rules.

Fairness and transparency

The duty to process data **fairly and transparently** means there should be no surprises about how personal data are processed. Under Articles 13 and 14 of the GDPR the Service:

- gives data subjects ready access to Privacy Notices in plain language describing how their personal data are processed;
- if it has obtained the personal data from someone else, must usually let the data subject know within a month at most;
- must also let him or her know from what source it obtained the personal data.

The Service's **Privacy Notices** set out the legal basis for collecting and otherwise processing data for particular classes of data subjects.

2. Collected for specified, explicit, and legitimate purposes.

Personal data must **only be processed** in a way that is **compatible** (consistent) with the purposes it was collected for. This is known as the principle of **purpose limitation**. The Service will not collect and process a person's personal data for one reason, and use it for a

quite different purpose. Further use of personal data will only be allowed where it is compatible with the original purpose or where appropriate by way of a formal Data Protection Impact Assessment (see above). Service staff will be trained to have regard for this principle.

3. **Adequate, relevant, and limited to what is necessary.**

   This is known as **data minimisation**. The Service will only gather and process information about the data subject that is immediately needed for a particular purpose. The Service will follow the principle of data protection **by design and by default**, one aspect of which is that access to data will be limited on a "*need to know*" basis.

4. **Accurate and, where necessary, kept up to date.**

   The Service will take all reasonable steps to keep personal data accurate and up to date. One objective of data protection by design is that personal data once updated at one point of contact is captured and harmonised throughout the Service's systems. Care will be taken to eliminate stale or inconsistent data. The accuracy of personal data processed is obviously vital to the Service's effective performance of its functions, quite apart from its data protection duties. Some further consequences of this duty are addressed in the context of the data subject's right to **rectification** and/or **erasure** below: in particular, if the Service has to correct data it will normally inform persons who have received data that are wrong or no longer accurate of the correction.

5. **Storage limitation**

   The Service will not keep personal data longer than is needed for why they are processed. The Service has accordingly adopted a Records Retention Policy. Data retained for archive, historical research, or statistical purposes will be anonymised or pseudonymised where this would not frustrate the purpose of the processing.

6. **Kept secure and where appropriate confidential.**

   This involves taking appropriate technical and organisational measures. Organisational measures the Service has introduced include restricting dissemination and access. Service staff have been appropriately trained in their data protection duties, and this training is repeated and updated at regular intervals. The Service employs various technical measures including encryption to ensure its systems are secure and has an IT Security Policy. The Service uses measures combining technical and organisational elements include pseudonymisation (to impede identification of the data subject where the data are not in immediate use) and logging.

There are exceptions to the principles. Sometimes, giving notice of a type of processing might require disproportionate effort. Or it might prejudice an investigation, or a medical or legal confidence. Or personal data might need to be used in a court case or for a Garda investigation. All these exceptions are grounded in the GDPR or Irish law implementing it, and they need to be specially justified. More detail appears in the Service's **Privacy Notices**.

Accountability

This is sometimes treated as a 7th data protection principle. A data controller such as the Service must also take **responsibility** for and be able to **demonstrate compliance** with the previous six principles. Consequently, the Service keeps a record of data processing activities which contains details of:

- The data controller
- All categories of personal data processed
- Purposes of the processing
- Categories of data subjects
- Lawful basis for the processing of personal data
- Recipients of personal data
- Source of the personal data
- Retention period
- Safeguards and security measures
- Details of any data transfers
- Details of data processors
- Details of any joint controllers

6. Data subject rights

Before complying with any data rights request, the Service will take all necessary steps to confirm the identity of the individual making the request, whether on his or her own behalf or on another's behalf, and, where applicable, the requester's entitlement to act on behalf of the other person.

Again, just like with the six data protection principles, the following data rights are subject to any relevant qualifications or exemptions provided for by the GDPR or by Irish law (such as in section 60 of the Data Protection Act 2018) in conformity with it.

1) Right to access and information

A data subject has a right to information about his or her personal data that the Service processes, such as the purposes of the processing, any categories of recipients to whom the data have been or will be disclosed, particulars of his or her other rights in respect of the data, and the source of the data if it is not the data subject. Much of this information will already be available to the data subject from the Privacy Notices published by the Service.

Furthermore, a data subject has a right to obtain a copy of any personal data about him or her held by the Service.

The Service will respond to a data subject's access request within one month of receiving it unless this interval may exceptionally be extended as provided in the GDPR.

2) Right to rectification

A data subject has the right to have data rectified where an inaccuracy has been identified and the right to have data completed where it is incomplete. This can include the right to provide a supplementary statement.

3) Right to erasure ("be forgotten")

A data subject has a right to erasure of personal data, for example, where the processing is no longer necessary, where the data subject has withdrawn the consent that was the legal basis of the processing, where (s)he successfully exercises the right of objection (sub-heading 7 below), or the erasure is consistent with a legal duty (including where data are being unlawfully processed).

This right in particular is subject to a **number of qualifications**. It does not apply, for instance,

- where ongoing processing is required by a legal obligation,
- where such processing is justified by law in the public interest or in the exercise of official authority,
- where such processing is justified by legitimate objectives of public information or freedom of expression, or
- where the processing relates to legal claims and litigation, or
- is being carried out for archiving, historical research, or statistical purposes.

4) Right to Restrict

A data subject may ask the Service to restrict dealing with his or her personal data where:

(a) the accuracy of the personal data is contested by the data subject, and for as long as is necessary for the Service to verify that accuracy,
(b) the processing is unlawful but the data subject does not want the personal data deleted,
(c) the Service no longer needs the personal data but they are needed by the data subject for the establishment, exercise, or defence of a legal claim, or
(d) the data subject has used his or her right to object and the Service is still assessing whether there are compelling grounds for continued processing that override the rights of the data subject[3].

5) Right to data portability

A data subject has a right to data portability where the data are processed on the basis of consent or contract and the processing is carried out by automated means. If requested and technically feasible this right allows personal data to be transmitted directly from one data controller to another.

6) Right to Object

A data subject may object to the ongoing processing of his or her personal data where the legal bases for processing are that it is necessary for the performance by the Service of a task carried out in the public interest or in the exercise of official authority or where the processing is necessary for the advancement of the Service's legitimate interests. The data controller must cease processing unless the data controller can demonstrate compelling legitimate interests which override the interests of the data subject, or the processing is needed for the establishment, exercise, or defence or legal claims.

---

[3] Where a data subject exercises his or her rights under sub-headings 2), 3) or 4), the Service will, unless it proves impossible or would entail disproportionate effort, communicate the rectification, erasure, or restriction to any person who had previously received the personal data from the Service. Also, the data subject may ask the Service to inform him or her about those recipients.

7) Right to Complain

The Service aims to address any concerns that data subjects may have in relation to data protection in a clear, open and prompt manner. A data subject who believes that his or her personal data are not being processed by the Service lawfully, or that his or her rights in respect of the data as set out at 1) to 7) above are not being respected, should contact the Service's Data Protection Officer at dataprotection@oireachtas.ie. The Data Protection Officer will seek to resolve the complaint in a manner satisfactory to both parties.

A data subject has the right (whether as an alternative or subsequently) to lodge a complaint with the Data Protection Commission. The contact details of the Commission are:

Telephone	+353 57 8684800 +353 (0)761 104 800 1890 252 231 (Lo Call Number)
Fax	+353 57 868 4757
Email	info@dataprotection.ie

Postal Addresses

Laois Office	**Dublin Office**
Data Protection Commission	Data Protection Commission
Canal House	21 Fitzwilliam Square
Station Road	Dublin 2
Portarlington	D02 RD28
R32 AP23 Co. Laois	Ireland.

7. Data protection officer

A Data Protection Officer (DPO) has, in accordance with the GDPR, been designated by the Service, and answers only to the highest level of management. The Service will ensure that the DPO is involved, properly and in a timely manner, in all issues that relate to the protection of personal data – for example with regard to DPIAs and other assessments of risk posed by current or intended processing to data subjects, and in responding to potential personal data breaches. The Service will support the DPO in his or her tasks as contemplated by the GDPR.

The DPO under the GDPR Article 39(1)(b) among other matters (without limiting duties specified elsewhere in this Policy):

- informs and advises the Service, and the employees of the Service who carry out processing, of their obligations under Irish and EU law that relates to the protection of personal data
- monitors the compliance of the Service with Irish and EU law that relates to the protection of personal data
- monitors the compliance of the Service with the Service's policies in relation to the protection of personal data, including the assignment of responsibilities, the raising of awareness and the training of staff involved in processing operations, and any audit activity related to the protection of personal data
- provides advice, where requested to do so, in relation to the carrying out of a data protection impact assessment, and monitors any steps taken on foot of that assessment

- acts as the contact point for data subjects with regard to all issues related to the processing of their personal data and to the exercise of their rights
- cooperates with the Data Protection Commission and acts as a contact point for the Commission for issues related to processing carried out by the Service, including consultation by the Service with the Commission
- promotes a data protection risk based approach across the Service.

The Service's Data Protection Officer can be contacted on +353 1 618 4712 or dataprotection@oireachtas.ie. The postal address of the Service is Houses of the Oireachtas Service, Leinster House, Kildare Street, Dublin 2, D02 XR20

.

Glossary

(data) controller	A "**controller**" or "**data controller**" is the person or body who determines the how and why of the processing of personal data (contrast "**processor**")
data subject	An identifiable natural person is the "**data subject**" of a particular piece of personal data about them
GDPR	General Data Protection Regulation
identifiable natural person	A living person who can be identified, directly or indirectly; in particular a person can be identified by reference to an identifier such as a name, an identification number, location data, or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person
personal data	Any information relating to an identified or identifiable living person
Processing	Any act performed on personal data; examples include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
(data) processor	A "**processor**" or "**data processor**" is a person or body who processes data on behalf of a controller
pseudonymis-ation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
special category data	Personal data revealing • racial or ethnic origin, • political opinions, • religious or philosophical beliefs, • trade-union membership and also • genetic data, • biometric data where processed for the purpose of uniquely identifying a living person and also • data concerning health • data concerning a natural person's sex life or sexual orientation.