An Coimisiún Pleanála

General Data Protection Regulations (GDPR) Policy

Contents

1.0 Purpose of the Policy

1.1 This policy is a statement of An Coimisiún Pleanála's commitment to protect the rights and privacy of individuals in accordance with the General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018 (referred to together as "Data Protection Law") and related regulatory guidance. An Coimisiún Pleanála must process (use or store) certain personal data about staff, Planning Commissioners and stakeholders in order to fulfil its purpose and to meet its legal obligations.

1.2 An Coimisiún Pleanála is a data controller and is responsible for compliance with the legislation in respect of the personal data it processes. 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. It covers any information that relates to an identifiable, living individual. Even if the individual's "real-world" identity (for example, their name) is not known, they still can be considered identifiable if they can be singled out using the available information.

This data can be held on paper (in a structured form) or electronically and must be processed in accordance with An Coimisiún Pleanála's obligations under Data Protection Law, as outlined below.

2.0 Data Protection Principles

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency').**

(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 **('purpose limitation');**

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

(d) 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 **('accuracy');**

(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 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 this Regulation in order to safeguard the rights and freedoms of the data subject **('storage limitation');**

(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 **('integrity and confidentiality').**

(g) The controller shall be responsible for and be able to demonstrate compliance **('accountability').**

Further Guidance on the Principles of Data Protection can be found at this link.

3.0 Lawfulness of Processing

3.1 To ensure that processing of personal data by An Coimisiún Pleanála is lawful, personal data shall be processed only if and to the extent that one of the following legal bases applies to An Coimisiún Pleanála's processing:

(a) the data subject has given An Coimisiún Pleanála valid consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for An Coimisiún Pleanála's performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which An Coimisiún Pleanála is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out by An Coimisiún Pleanála in the public interest or in the exercise of official authority vested in An Coimisiún Pleanála, for example, processing of personal data by An Coimisiún Pleanála in the context of determination of appeals and certain other matters under the Planning and Development Act 2000, as amended, and associated legislation;

(f) processing is necessary for the purposes of the legitimate interests pursued by An Coimisiún Pleanála or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data;

(g) Point (f) shall not apply to processing carried out by An Coimisiún Pleanála in the performance of its tasks.

Link to Privacy Statement: Privacy and the General Data Protection Regulations (GDPR) 2018 | An Coimisiún Pleanála –

4.0 Conditions for Consent

4.1 Where processing is based on consent, An Coimisiún Pleanála must be able to demonstrate that the data subject has consented to processing of his or her personal data.

4.2 There are a number of conditions that An Coimisiún Pleanála must satisfy to ensure that consent is valid, (for example, consent must be freely given, specific (for example, related to specific data and purpose(s) of processing), informed, unambiguous, documented, and withdrawable. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be clearly distinguished from and not linked to the other matters and must be clear and written in plain language.

4.3 The data subject has the right to withdraw his or her consent at any time and An Coimisiún Pleanála must ensure that individuals can withdraw consent as easily as they gave it. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal thereof.

5.0 Personal Information supplied to An Coimisiún Pleanála

5.1 Parties to Case Work

By the powers of the Planning and Development Act 2000 as amended, and all other associated legislation covering the statutory functions of An Coimisiún Pleanála, the Commission must receive the name and address of any party, observer, objector or other person who correspond with An Coimisiún Pleanála in relation to a case that is or has been subject to processing by An Coimisiún Pleanála.

5.2 <u>Planning Commissioners and staff of the Commission</u>

Throughout an employee's duration of employment, he/she is required to provide details for purposes as outlined below in 6.2 Human Resources, 6.3 Finance and 6.4 Pension and where appropriate, complete a declaration of interest form annually during his/her term of office/employment.

5.3 Consultants

Consultants to An Coimisiún Pleanála are required to provide personal contact details.

5.4 Contractors

An Coimisiún Pleanála contractors are required to provide the organisation with tax clearance certificates, company and contract manager/personnel contacts for example; names, addresses, emails, websites, PPS/VAT numbers and bank details for Electronic Fund Transfer payment.

5.5 Member of the Public

A member of the public may on occasion supply the organisation with personal information through the website, by post, by e-mail or over the phone. All information supplied is used exclusively by An Coimisiún Pleanála for:

- the purposes for which it is provided,
- verification purposes, statistical analysis, archival purposes and
- administrative purposes.

6.0 Description of Data Collected

6.1 Casework

Names and addresses of parties and agents, the proposed development description and address involved in case work under the provisions of the applicable planning legislation. These details are processed using a case management system. Documentation submitted to An Coimisiún Pleanála is published in full on its website. For full details, please follow this link to the privacy statement:

Privacy and the General Data Protection Regulations (GDPR) 2018 | An Coimisiún Pleanála

6.2 Human Resources

Name, address, contact details, telephone numbers and email address, PPS number, birth certificate, educational certificates, employment histories, Garda clearance reports, job applications, medical and VDU eyesight reports, leave details, appraisal information and Performance Management through Development and Support, disciplinary issues, details of training needs/records, emergency contact person details, medical and Social Welfare Certificates.

6.3 Finance Section

Name, postal and email addresses, telephone number, union membership, PPS numbers, bank details, mandates for financial pay overs, travel and subsistence records, car type and registration number, company/individual names, addresses, PPS/VAT numbers and tax clearance certificates, date of birth for payroll only where no PPS is provided or when there is an early retirement.

6.4 Pension

Employment commencement date, dependant details, information of previous time worked in the public service and name of previous public service employer organisation if applicable.

6.5 Email System

- Individual email accounts of the Governing Board, Planning Commissioners and staff of An Coimisiún Pleanála.

- Email addresses of Consultants / Suppliers and Service Providers / other correspondents.

- Such email details and material as may be included in the bodies of emails received and sent.

6.6 Flexi Clock System

Staff name, date and times of clocking in and out on the time management system.

6.7 Door Access Control System

Card holders name, date and times of entry and exit through controlled doors.

6.8 CCTV

Cameras are in operation for security purposes. The organisation has closed circuit television cameras located at entry and exit doors, at reception, in the ground floor conference and meeting rooms, on the fifth floor balcony and in the car park. Images are being recorded for the purpose of crime prevention and personal safety. Access to the recorded material is strictly limited to authorised personnel.

Link to the CCTV Policy here: CCTV-Data-Protection-Policy.pdf

6.9 Phone Monitoring System

Staff members name, extension number, date, time, duration, phone number of all incoming and outgoing calls.

7.0 Protecting the Rights of Data Subject

7.1 Transparent information and communication with the Data Subject.

An Coimisiún Pleanála shall provide a data subject with a response to any data request in clear plain language, without delay and within a maximum period of one month. If An Coimisiún Pleanála is unable to deal with the request fully within a calendar month, taking into account the complexity and the number of requests, the period may be extended by a further two calendar months and if so doing An Coimisiún Pleanála must explain the reasons for the delay to the relevant individual.

If the request is made electronically, An Coimisiún Pleanála shall provide the information electronically, where possible. An Coimisiún Pleanála will inform the data subject without delay if it is not taking action on the request and on the right to complain to the Data Protection Commission.

An Coimisiún Pleanála shall consider and respond without delay to complaints from individuals about its processing of their personal data. For complaints from individuals about An Coimisiún Pleanála's processing of their personal data, please refer the complaint as soon as possible to the Data Protection Officer at dataprotectection@pleanala.ie

7.2 Right of access to personal data by Data Subject

A data subject has the right of access to their personal data processed by An Coimisiún Pleanála. An Coimisiún Pleanála will provide a copy of the personal data undergoing processing (usually in a commonly used electronic form, unless otherwise requested by a data subject), unless it can withhold certain personal data in reliance on certain exceptions set out in Data Protection Law (for example if a claim of legal privilege could be made with respect to the relevant personal data). In addition to providing a copy of the requested data, An Coimisiún Pleanála must also provide additional information related to the processing.

Every data subject has the right to know;

- The contact details for An Coimisiún Pleanála and its designated Data Protection Officer.
- The purposes for which the personal data is processed
- The time period for which the data is processed
- The right to request access to and rectify personal data or restrict processing
- Any recipients of the personal data
- If the processing of the personal data is statutory or contractual
- If automated or profiling is involved, the consequences of such processing

Link to Further Information on Data Subject Rights: The Right of Access | Data Protection Commission

7. 3 Right to be Forgotten

The data subject has the right to obtain the erasure of personal data concerning him or her without undue delay and An Coimisiún Pleanála is obliged to erase personal data where one of the following grounds applies;

(a) The personal data is no longer necessary.

(b) The data subject withdraws consent and there is no other legal basis for the processing.

(c) The data subject objects to the processing (where such objection is allowed under Data Protection Law) and An Coimisiún Pleanála cannot demonstrate an overriding compelling legitimate interest to continue to process the personal data.

(d) The data has been unlawfully processed.

(e) The data has to be erased for compliance with a legal obligation.

Even where the data subject requests the erasure or removal of data, certain circumstances may require retention for example;

(a) Exercising the right of freedom of expression and information.

(b) For compliance with a legal obligation to which An Commisiún Pleanála is subject.

(c) For a task carried out in the public interest or the exercise of official authority vested in An Coimisiún Pleanála or for reasons of public interest in the area of public health.

7.4 Right to Restriction of Processing

The data subject can request that the processing of their personal data by An Coimisiún Pleanála should be restricted for a period of time, or until the underlying issue is resolved.

Restriction on the processing of personal data may arise where;

(a) The accuracy of the data is contested

(b) The processing is unlawful

(c) An Coimisiún Pleanála no longer needs the data for the purposes of the processing

(d) The data subject has objected to processing

7.5 Rights in relation to Profiling and Automated Decision Making

Profiling is automated data processing which can be used to evaluate and predict certain individual behaviours and preferences. An Coimisiún Pleanála does not process personal data for profiling and does not engage in automated decision-making.

8.0 Security of Data

8.1 Disclosure of Information

In line with An Coimisiún Pleanála's Code of Conduct, the Governing Board, Planning Commissioners, staff of the Commission and certain other persons, are obliged not to disclose any information obtained while performing, or as a result of performing, any activities on behalf of An Coimisiún Pleanála. The disclosure of information to Government Ministers, Regulatory Authorities, other agencies with which An Coimisiún Pleanála has appropriate reciprocal confidentiality agreements, or to parties with whom there is a legitimate requirement to share information, is permitted in the circumstances provided under EU Directive 95/46 (as amended).

Further details on data sharing in the Public Sector can be found here.

As part of the terms of a contract of employment/engagement, Planning Commissioners, staff of the Commission and consultants sign a confidentiality undertaking as a condition of appointment.

An Coimisiún Pleanála has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons, including -

a) The pseudonymisation and encryption of personal data,

b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,

c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,

d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

An Coimisiún Pleanála has an appropriate level of security in order to protect personal data it processes from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access. In particular, An Coimisiún Pleanála ensures that all appropriate confidentiality obligations and technical and organisational security measures are in place to prevent any unauthorised or unlawful disclosure or processing of such information and data, and the accidental loss or destruction of, or damage to, such information and data. Only authorised An Coimisiún Pleanála Planning Commissioners and staff are provided access to personally identifiable information and these employees are required to maintain the confidentiality of any data to which they have access.

Further Information on Data Security: Guidance for Controllers on Data Security | Data Protection Commission

8.2 Encryption Features to Protect Personal Data

a) Sensitive/personal data files are protected by assigning different permission levels based on section grouping within the Active Directory. Restricted members of the Human Resources team have access to files and folders of personal data relating to staff.

b) All laptops and hybrid device are deployed with full encryption. It is not the practice to encrypt desktop PC's are they are within the main An Coimisiún Pleanála office and are immobile. All laptops and workstations are secured with a password-protected screensaver with the automatic activation feature set at a maximum of 15 minutes, or by locking or logging-off when the system is unattended.

c) Email encryption is configured within Microsoft Office 365 and each individual email may be encrypted by the end user before delivery to the recipient.

d) Information considered sensitive is encrypted (for example on USB, via e-mail, backup tapes).

e) All network and cloud related data is encrypted at rest and in transit.

8.3 Electronic Communications

An Coimisiún Pleanála provides email, internet and intranet facilities. In order to protect against the dangers associated with email and internet use, screening software is in place to monitor email and web usage.

8.4 ICT Access

Authorised users are only granted access to information systems, services and networks which are necessary to carry out the responsibilities of their role or function. Each user must respect and protect the privacy and confidentiality of the information systems and network they access, and the personal data processed by those systems or networks. Access is denied to users to systems relating to their previous roles when their role and responsibility changes within the organisation.

9.0 Data Breach

9.1 In the case of a personal data breach, it should be reported immediately to the Data Protection Officer at dataprotection@pleanala.ie.

9.2 When a Planning Commissioner or staff member recognises that a hard copy data loss or a data breach has occurred, it must be declared immediately to the CEO, in the case of a Planning Commissioner and a Line Manager in the case of a staff member.

9.3 The CEO/Line Manager must then declare, through appropriately recorded channels, details of any data breach to the internal Data Protection Officer.

9.4 The Data Protection Officer shall where feasible, and not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Commission unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Such notification should be made without undue delay and, where the notification to the Commission is not made within 72 hours, it should be accompanied by reasons for the delay.

Link to information on Breach Notification | Data Protection Commission

9.5 The Data Protection Officer shall document/record internally any personal data breaches (whether notifiable or not), comprising the facts relating to the personal data breach, its effects, risk assessment, the remedial action taken, and lessons learned.

10.0 Communication of a personal Data Breach to the Data Subject

10.1 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, An Coimisiún Pleanála will communicate the personal data breach to the affected data subjects without undue delay, unless any of the following conditions are met:

(a) An Coimisiún Pleanála has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, such as encryption;

(b) An Coimisiún Pleanála has taken subsequent measures which ensure that the high risk is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar whereby the data subjects are informed in an equally effective manner.

11.0 Data Protection Impact Assessment (DPIA)

11.1 Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, An Coimisiún Pleanála shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (Data Protection Impact Assessment).

11.2 Senior Management shall seek the advice of the Data Protection Officer when carrying out a data protection impact assessment.

11.3 A data protection impact assessment shall be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data;

(c) a systematic monitoring of a publicly accessible area on a large scale.

Guide to Data Protection Impact Assessments | Data Protection Commission

12.0 Transfer of data outside the State

An Coimisiún Pleanála shall not transfer personal data outside of Ireland (which includes access from outside of Ireland), unless the transfer is:

(1) To a country approved by the European Commission as having adequate data protection laws to protect the personal data; or

(2) To an organisation that has entered into a data transfer agreement with us (based on European Commission Standard Contractual Clauses).

13.0 Roles and Responsibilities

Data Protection Officer

The Data Protection Officer's role is to advise the data controller (An Coimisiún Pleanála) on data protection compliance, respond to data subject requests, record and respond to data breaches and report to Senior Management and relevant committees where required. The Data Protection Officer reviews and monitors any data protection impact assessments that are carried out by Senior Management.

CEO and Senior Management

Overall responsibility for an effective policy for data protection rests with the Chief Executive Officer (CEO).

Data Protection begins at management level and the day to day management of data protection is with Senior Management. Planning Commissioners and all staff of the Commission share a responsibility with management in ensuring that the principles of data protection form part of their work.

Data Controller	An Coimisiún Pleanála, 64 Marlborough Street, Dublin 1 Tel: 01 858 8100. Email: dataprotection@pleanala.ie
Data Protection Officer	Data Protection Officer Deputy Data Protection Officer Email: dataprotection@pleanala.ie
Compliance Officer	Chief Executive Officer

14.0 Review

This policy will be reviewed by the Data Protection Officer every three years or as required having regard to any legislative or other relevant guidance relating to data protection.

15.0 Version Control

First Adopted by Board	May 2018
Minor Amendment by DPO	June 2022
Full Review and amendment by DPO	September 2025

16.0 References

- General Data Protection Regulation 2016
- An Coimisiún Pleanála Code of Conduct for Board members and employees
- An Coimisiún Pleanála CCTV Policy
- An Coimisiún Pleanála Human Resources Retention Policy
- An Coimisiún Pleanála ICT Acceptable Use Policy
- An Coimisiún Pleanála Access Control Policy
- An Coimisiún Pleanála Policy on Transporting Hard Copy Data
- An Coimisiún Pleanála Information Security Policy
- An Coimisiún Pleanála Clean Desk Policy

Appendix 1: Definitions

biometric data	means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
consent	of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
data concerning health	means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
genetic data	means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
filing system	means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

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;
personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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;
profiling	means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
pseudonymisation	means 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 such 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;

restriction of processing	means the marking of stored personal data with the aim of limiting their processing in the future;
processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
recipient	means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;