An Bord Pleanála

General Data Protection Regulations (GDPR) Policy

May 2018

1.0 Contents

2.0 Purpose of the Policy

This policy is a statement of An Bord Pleanála's commitment to protect the rights and privacy of individuals in accordance with the General Data Protection Regulation 2016. An Bord Pleanála must process (store or use) certain personal data about staff, Board members and stakeholders in order to fulfil its purpose and to meet its legal obligations.

An Bord Pleanála is a data controller and is responsible for the implementation of the legislation in respect of the personal data it holds. 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.

This data can be held on paper or electronically or other media and will be maintained in accordance with the obligations of the Regulations as outlined below.

3.0 Data protection principles

An Bord Pleanála will perform its responsibilities under the GDPR in accordance with the following 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').

4.0 Lawfulness of processing

Processing of personal data by An Bord Pleanála shall be lawful only if and to the extent that at least one of the following applies:

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

(b) processing is necessary for the 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 the controller 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 in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller 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, in particular where the data subject is a child.
(g) Point (f) shall not apply to processing carried out by public authorities in the performance of their tasks.

5.0 Conditions for consent

1. Where processing is based on consent, An Bord Pleanála shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Conditions applicable to child's consent in relation to information society services

1. In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
2. An Bord Pleanála shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

6.0 Personal information supplied to An Bord Pleanála

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 Bord Pleanála, the Board must receive the name and address of any party, observer, objector or other person who correspond with An Bord Pleanála in relation to a case that is or has been subject to processing by An Bord Pleanála.

Staff and Board members

Throughout an employee's duration of employment, he/she is required to provide details as outlined below in paragraph 7 for Human Resources, Finance and Pension purposes and where appropriate complete a declaration of interest form annually during his/her term of office/employment.

Consultants

Consultants to An Bord Pleanála are required to provide personal contact details, complete a declaration of interest form annually during his/her term of office.

Contractors

An Bord 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.

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 Bord Pleanála for:

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

7.0 Description of data collected

Casework

Names and addresses of parties and agents, the proposed development description and address involved in case work under the provisions of the applicable legislation. These details are processed using a case management system. The names of parties are published on our website.

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 certs.

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.

Finance Section

Name, postal and email addresses, telephone, union membership, PPS numbers, bank details, mandates for financial payovers, 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.

Email system

- Individual An Bord Pleanála email accounts.
- Email addresses of correspondents.
- Such material as may be included in the bodies of emails received and sent.

Flexi Clock system

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

Door access control system

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

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 your personal safety. Access to the recorded material is strictly limited to authorised personnel.

Phone monitoring system

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

8.0 Protecting the rights of data subject

Transparent information and communication with the data subject

An Bord Pleanála shall provide a data subject a response to any data request in clear plain language within a maximum period of one month. If An Bord Pleanála is unable to deal with the request fully within a calendar month due to the complexity or the number of requests, the period may be extended by a further two calendar months and if so doing will explain the reasons for the delay.

If the request is made electronically, An Bord Pleanála shall provide the information electronically, where possible. An Bord 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.

Right of access to one's personal data

A data subject has the right of access to personal data which has been collected concerning him or her by An Bord Pleanála and may exercise that right easily and at reasonable intervals, in order to be aware of and verify, the lawfulness of any processing that is being carried out. Every data subject has the right to know;

(a) The contact details for An Bord Pleanála and its designated Data Protection Officer
(b) The purposes for which the personal data is processed
(c) The time period for which the data is processed
(d) The right to request access to and rectify personal data or restrict processing
(e) Any recipients of the personal data
(f) If the processing of the personal data is statutory or contractual
(g) If automated or profiling is involved, the consequences of such processing

Data controllers are required where possible to provide remote access to a secure system which the data subject can have direct access to his or her own personal data.

An Bord Pleanála is currently not in a position to provide remote access to facilitate a data subject.

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 Bord 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
(c) The data subject objects to the processing
(d) The data has been unlawfully processed
(e) The data has to be erased for compliance with a legal obligation
(f) The data was collected from a child under 16 years of age.

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 Bord Pleanála is subject
(c) For a task carried out in the public interest or official authority or public health

Right to restriction of processing

The data subject can request that the processing of their personal data by An Bord 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 Bord Pleanála no longer needs the data for the purposes of the processing
(d) The data subject has objected to processing

Right to object

A data subject is entitled to object to the processing of their personal data based on his or her particular situation.

Right to data portability

The data subject is entitled to receive a copy of the personal data which he or she has provided to An Bord Pleanála in a structured, commonly used, machine readable and interoperable format. An Bord Pleanála will transmit the data at the data subject's request, to another data controller.

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 Bord Pleanála does not process personal data for profiling.

No personal data obtained by An Bord Pleanála is processed for the purposes of direct marketing.

9.0 Security of data

Disclosure of information

In line with An Bord Pleanála's Code of Conduct for Board members, employees and certain other persons, members of the Board, staff and consultants are obliged not to disclose any information obtained while performing, or as a result of performing, any activities on behalf of An Bord Pleanála. The disclosure of information to government ministers, regulatory authorities, other agencies with which An Bord 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).

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

An Bord 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 Bord Pleanála has an appropriate level of security in order to protect personally identifiable data and information from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. In particular, An Bord Pleanála endeavours to ensure 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 Bord Pleanála 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.

Encryption features to protect personal data

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.

All laptops and hybrid device disks are deployed with full disk encryption. It is not the practice to encrypt desktop PC's are they are within the main An Bord Pleanála office and are immobile.

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

All external hard drives and removable disks are fully encrypted.

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

Electronic Communications

An Bord 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.

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.

10.0 Data breach

1. In the case of a personal data breach, An Bord Pleanála 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. Where the notification to the Commission is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify An Bord Pleanála without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by An Bord Pleanála to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. An Bord Pleanála shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, An Bord Pleanála shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) above.
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
   (a) An Bord 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 Bord 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.
4. If An Bord Pleanála has not already communicated the personal data breach to the data subject, the Commission, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met**.**

11.0 Data protection impact assessment

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 Bord Pleanála shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. An Bord Pleanála shall seek the advice of the data protection officer and the Commission when carrying out a data protection impact assessment.
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.

12.0 Transfer of data outside the state

Should it become necessary that in the course of business An Bord Pleanála has to transfer personal data to other third party service provider organisations outside of Ireland which do not have comparable data protection laws to Ireland, if and when this is necessary, the third party company will provide assurances to An Bord Pleanála that the data has the same level of protection as it does inside the State. An Bord Pleanála will only transmit to companies that agree to guarantee this level of protection. For more information, please contact the Data Controller.

13.0 Roles

Data Controller:	An Bord Pleanála, 64 Marlborough Street, Dublin 1 Tel: 01 8588100 Email: dataprotection@pleanala.ie
Data Protection Officer:	Ellen Morrin, Senior Administrative Officer Email: dataprotection@pleanala.ie
Compliance Officer:	Chief Officer

Data Protection begins at management level and the overall responsibility for an effective policy for data protection rests with the Chief Officer. Day to day management of data protection is with Senior Management. Staff share a responsibility with management in ensuring that the principles of data protection are abided.

14.0 Review

This policy will be reviewed as required having regard to any legislative or other relevant developments relating to data protection.

Appendix 1: Definitions and References

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;

References:

- General Data Protection Regulation 2016
- An Bord Pleanála Code of Conduct for Board members and employees
- An Bord Pleanála CCTV/Swipe Card Policy
- An Bord Pleanála Telephone Software Policy
- An Bord Pleanála Human Resources Retention Policy
- An Bord Pleanála ICT Acceptable Use Policy
- An Bord Pleanála Technology Usage Policy
- An Bord Pleanála Access Control Policy