



An  
Bord  
Pleanála

**An Bord Pleanála**

## **CCTV Data Protection Policy**



## Table of Contents

<b>1.0</b>	<b>Introduction .....</b>	<b>3</b>
<b>2.0</b>	<b>Purpose of Policy .....</b>	<b>3</b>
<b>3.0</b>	<b>Lawfulness.....</b>	<b>3</b>
<b>4.0</b>	<b>Necessity and Proportionality .....</b>	<b>4</b>
<b>5.0</b>	<b>Security of Personal Data .....</b>	<b>5</b>
<b>6.0</b>	<b>Storage, Retention and Deletion .....</b>	<b>5</b>
<b>7.0</b>	<b>Transparency .....</b>	<b>6</b>
<b>8.0</b>	<b>Data Processors .....</b>	<b>6</b>
<b>9.0</b>	<b>Access Request by Data Subjects .....</b>	<b>7</b>
<b>10.0</b>	<b>Data of CCTV Footage to Third Parties .....</b>	<b>8</b>
<b>11.0</b>	<b>Policy Review .....</b>	<b>9</b>
	<b>Chronology of Review and Amendment Cycle .....</b>	<b>9</b>

## **1.0 Introduction**

- 1.1 A Closed Circuit Television System (CCTV) is installed in An Bord Pleanála at 64 Marlborough Street, Dublin 1.
- 1.2 This policy is in accordance with the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act 2018.
- 1.3 This policy takes into consideration the current guidance (November 2023) on the use of CCTV by the Data Protection Commission (DPC).

## **2.0 Purpose of Policy**

- 2.1 The principles of data protection require that personal data shall be “*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*”.
- 2.1 The purpose of this policy is to regulate the use of CCTV and its associated technology in the monitoring of both the internal and external environs of the office building of An Bord Pleanála.
- 2.3 Any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy, for example CCTV will not be used for monitoring staff performance.

## **3.0 Lawfulness**

The use of a CCTV system by An Bord Pleanála is in accordance with Article 6,1(f) of the GDPR as processing is necessary for the purposes of its legitimate interests in protecting its property and assets and maintaining the safety of Board members, staff and persons using the office building.

## **4.0 Necessity and Proportionality**

4.1 A CCTV system is installed to externally monitor the perimeter of the office building for security purposes and installed internally on the ground floor and fifth floor external balcony for the purpose of enhancing security and protect the health and safety of Board members, staff and persons using the office building.

4.2 CCTV surveillance at the office is intended for the purposes of:

- protecting the building and assets, both during and after office hours;
- promoting the health and safety of Board members, staff and customers;
- monitoring issues relating to public access to documents.

4.3 Externally, cameras are installed and positioned in six locations:

- One on Marlborough Street
- Two on Findlater Place
- Two on Strong's Court
- One on fifth floor external balcony

Internally, nine cameras are installed and positioned on the ground floor:

- Four in Reception
- One in the Maoilbhríde Room,
- One in the three meeting rooms (Parnell Room, Séan McDermott Room and Cathal Brugha Room).
- One in the hallway to Parnell Room

Basement Level - four cameras positioned in the basement/carpark entrance.

## 5.0 Security of Personal Data

- 5.1 The CCTV system monitoring and storing the CCTV footage is encrypted and password protected.
- 5.2 The CCTV system is situated in the security area on the ground floor and operated by Security Personnel under the Facilities Management Contract.
- 5.3 Only authorised personnel have access to and may view the CCTV footage. Authorised personnel are the Security Personnel and the Data Protection Officer/Deputy Data Protection Officer.  
Only the Data Protection Officer/Deputy Data Protection Officer is authorised to give access to a data subject to view or release CCTV footage following a request.  
Access requests to view or receive a recording of the CCTV footage are entered in a CCTV Access Log by the Security Personnel in the security area.
- 5.4 Supervising the maintenance of the CCTV System is the responsibility of the SAO in Facilities and Environmental Management under the Facilities Management Contract.

## 6.0 Storage, Retention and Deletion

- 6.1 Article 5.1(e) of the GDPR states that data shall be *“kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are published.”* The CCTV recording system has a default retention period of **30 days**, the maximum acceptable period under Data Protection Commission Guidance.
- 6.2 Where footage has been identified that relates to a specific incident, a longer period may be justifiable for the particular section of footage concerned, such as in the investigation of a workplace accident or where footage may be used as evidence in criminal proceedings. This footage is isolated from the general

recordings onto a USB key and is kept securely for the purpose that has arisen.

- 6.3 Footage on a USB key retained beyond the retention period for a specific purpose shall be deleted once the issue is settled. The Data Protection Officer/Deputy Data Protection Officer shall keep a record of deletion.

## **7.0 Transparency**

- 7.1 A copy of the CCTV Data Protection Policy is available to staff and Board members on the GDPR SharePoint site and at reception for contractors and visitors to the office. The policy is also available on An Bord Pleanála's website: [www.pleanala.ie](http://www.pleanala.ie)
- 7.2 Signage is placed at each location in which a CCTV camera is sited to indicate that CCTV is in operation. Signage includes the name and contact details of the data controller, An Bord Pleanála.

## **8.0 Data Processors**

- 8.1 Article 32 of the GDPR places a number of obligations on Data Processors. These include having appropriate security measures in place to prevent the destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, in particular where the processing involves the transmission of data over a network and against all unlawful forms of processing.
- 8.2 The CCTV system is operated by a security company sub-contracted through the Facilities Management Contractor. The Contractor has a written contract with the security company in place which details the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply.

The written contract states that the security company will give An Bord Pleanála all reasonable assistance to deal with any subject access request made under Article 15 of the GDPR which may be received by An Bord Pleanála within the statutory timeframe (generally one calendar month).

Staff of the security company have been made aware of their obligations relating to the security of data.

## **9.0 Access Request by Data Subjects**

- 9.1 Data protection law provides individuals with a right of access to their personal data. This right of access applies to any individual whose identifiable image has been recorded by a CCTV system. When An Bord Pleanála receives a request from an individual to access CCTV data, it will normally respond within **one month**.
- 9.2 To facilitate the processing of the request, An Bord Pleanála will ask the individual to give a reasonable indication of the date and time of the footage they are looking for. If the recording has already been deleted on the date on which the request is received, the defined retention period having expired, the individual will be informed that the footage no longer exists. If an access request has been received, the footage will not be deleted until the request has been fulfilled.
- 9.3 In giving an individual a copy of their data, An Bord Pleanála may provide a still/series of still pictures or a USB key with the relevant footage. Where necessary, measures may be taken to pixelate or otherwise de-identify the images of other identifiable parties before supplying a copy of the footage to the requester. Alternatively, An Bord Pleanála may seek the consent of those other parties, where possible, whose images appear in the footage to release an unedited copy containing their images to the requester.

9.4 Access requests can be made to the Data Protection Officer or Deputy Data Protection Officer, An Bord Pleanála, 64 Marlborough Street, Dublin 1, D01 V902 or email: [dataprotection@pleanala.ie](mailto:dataprotection@pleanala.ie) or [dpo@pleanala.ie](mailto:dpo@pleanala.ie)

9.5 If a data subject is unsatisfied with a response received to a data subject request, the data subject has the right to lodge a complaint with the Data Protection Commission online at [www.dataprotection.ie](http://www.dataprotection.ie)

## **10.0 Data of CCTV Footage to Third Parties**

10.1 On occasion, An Bord Pleanála may be asked to disclose CCTV recordings to third parties for a purpose other than that for which they were originally obtained. This may arise, for example, where a request is received from An Garda Síochána (or another law enforcement body) to provide footage to assist in the investigation of a criminal offence.

10.2 Requests from An Garda Síochána (or another law enforcement body) for copies of CCTV footage should only be acceded to where a formal written request is provided to An Bord Pleanála stating that it is investigating a criminal matter.

10.3 For practical purposes, and to expedite a request speedily in urgent situations, a verbal request to the Data Protection Officer/Deputy Data Protection Officer may be sufficient to allow for the release of the footage sought. However, any such verbal request should be followed up with a formal written request.

**Note:** Access requests by third parties to view or obtain a recording of CCTV footage from the CCTV system will only be authorised by the Data Protection Officer/Deputy Data Protection Officer and will be recorded in the CCTV Access Log at the Security Desk.



10.4 An Bord Pleanála may be requested to provide CCTV footage to a third party to investigate an incident. In such cases, the same assessment procedure as applied for the original purpose should be applied to the new purpose to determine if it can be justified in the pursuit of a genuinely legitimate interest of An Bord Pleanála or another party. Such eventualities will be assessed on a case-by-case basis to ensure that the principles of data protection are adhered to, and the rights of individuals are not prejudiced.

## **11.0 Policy Review**

11.1 This policy will be assessed on at least an annual basis to determine whether it needs to be amended to take account of any changes in the relevant legislative, legal or central guidance environments or based on practical experience of the operation of the policy and related procedures in the workplace. A full substantive review of the policy will take place at least every **three** years.

### **Chronology of Review and Amendment Cycle**

First Adopted by Board	May 2018
Minor Amendment by DPO	October 2021
Review and amendment by DPO	April 2025