GREYHOUND RACING IRELAND

CLOSED CIRCUIT CCTV

DATA PROTECTION POLICY & PROCEDURE

Contents

Purpose	3
Policy	3-4
Scope	4
References	4
Definitions	4
Risk Management	5
Lawful Basis for Using CCTV	5
Camera Locations	6
Notification & Signage	6
Covert Surveillance	6
Managing Data Processors	6
Remote Monitoring	7
Event Security – Body Cameras	7
Data Retention	7-8
Data Subject Access Requests	8
Roles and Responsibilities	9
Policy Review and Update	9

Purpose

The purpose of this policy is to enable Rásaíocht Con Éireann/Greyhound Racing Ireland (GRI) comply with its legal obligations as set out in the General Data Protection Regulation (EU) 2016/679 and the Data Protection Acts 1988-2018 and other associated laws.

GRI is committed to regulating its use of CCTV and associated technologies when monitoring and recording the internal and external environs of GRI premises in a manner consistent with data protection law. GRI has installed CCTV internally and externally to enhance security associated with its assets and operations, including monitoring compliance with greyhound racing and gambling regulations and associated protocols. CCTV creates awareness among employees and visitors that security surveillance is in operation during daylight and night hours on an ongoing basis. CCTV surveillance at head office and greyhound stadia is provided:

- to protect buildings, assets and operations, during and after operational hours,
- to monitor and protect the safety, health and welfare of employees and visitors during operations, within the premises, car parks and the environs of the stadia grounds,
- to investigate accidents and/or incidents occurring on the premises or within the environs of stadia grounds,
- to monitor and protect the integrity of greyhound racing, sales and trial sessions against regulatory non-compliance within the environs of greyhound stadia grounds,
- to protect betting operations against regulatory non-compliance, fraud, and/or criminal activity,
- to prevent bullying, pranks and/or horseplay likely to endanger safety,
- to reduce and where necessary investigate incidence of crime and anti-social behaviour (including theft, fraud or vandalism),
- to support the Gardaí in a bid to deter, detect and investigate crime,
- to assist in identifying, apprehend and prosecute offenders regarding criminal matters,

Policy

Rásaíocht Con Éireann/Greyhound Racing Ireland has responsibility to safeguard its employees, visitors, and assets. GRI recognise its common law and statutory duty of care owed to employees and visitors, including the requirements of the Safety, Health and Welfare at Work Act 2005, the Occupiers Liability Act 1995, as amended by the Courts and Civil Law (Miscellaneous Provisions) Act 2023.
To meet these obligations, GRI use Closed Circuit Television Systems (CCTV) to enhance its security profile and maintain security standards.

GRI also use CCTV to enhance and safeguard the integrity of greyhound racing operations within a safe environment as provided by the Greyhound Racing Act 2019 and to support its compliance obligations under the Gambling Regulation Act 2024 and associated protocols. GRI is committed to operating its CCTV systems in a lawful and ethical manner. Any use of CCTV in a manner contrary to law is prohibited by this policy.

This policy prohibits CCTV monitoring based on the characteristics and classifications contained in equality legislation related to gender, marital status, family status, age, disability, sexual orientation, race, religion, and being a membership of the Traveller community. It prohibits monitoring that violates the organisations Equality & Diversity Policy, Dignity at Work Policy, Codes of Practice related to Bullying & Harassment and Sexual Harassment, Child Safeguarding, and other related policies and laws.

CCTV will not be used for day-to-day monitoring of employee performance e.g., timekeeping and attendance. The use of CCTV for monitoring employment activities related to safety, security, racing regulation and duties, gambling regulatory compliance and associated employment activities is limited to uses that do not violate an individual's reasonable expectation to privacy based on their fundamental rights and freedoms. GRI recognise that images captured by CCTV are personal data and subject to the provisions of the General Data Protection Regulation EU 2016/679 and the Data Protection Act 2018. It is GRI policy to comply with these laws.

Scope

This policy and associated procedures relate directly to all CCTV situated and used on GRI sites. It applies to all activities related to the use of CCTV including maintenance, management, monitoring, processing, recording, access, storage, security, retention, reviewing, downloading, copying, transferring, dissemination, and subsequent use of recorded material and its ultimate destruction. It applies to all external monitoring conducted by GRI's service providers that externally monitor GRI locations for security purposes. It applies to board members, employees, students on work experience, trainees, volunteers, contractors, and any other person/s performing any role or function in, or on behalf of Greyhound Racing Ireland. It applies to all GRI operations including racing, trials, and greyhound sales, wagering activities, food, and beverage service and attendance at greyhound stadia.

References

- General Data Protection Regulation (EU) 2016/679
- Data Protection Act 2018
- Law Enforcement Directive - Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, thus repealing Council Framework Decision 2008/977/JHA
- Safety, Health, and Welfare & Work Act 2005
- Occupiers Liability Act 1995 (as amended)
- The Equal Status Acts 2000-2018 (the Acts') prohibit discrimination in the provision of goods and services and covers nine grounds of discrimination: gender, marital status, family status, age disability, sexual orientation, race, religion, and membership of the Traveler community.
- Greyhound Racing Act 2019.
- The Courts and Civil Law (Miscellaneous Provisions) Act 2023.
- The Gambling Regulation Act 2024.

Glossary of Terms and Definitions

The following definitions apply to this policy to ensure compliance with the Regulation.

- **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, by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural, or social identity of that natural person.

- **Processing** means any operation or set of operations performed on personal data or sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alternation, retrieval, consultation, use, disclosure, by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- **Restriction of processing** means the marking of stored personal data with the aim of limiting their processing in the future.

- **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, 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 personal data are not attributed to an identified or identifiable natural person.

- **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.

- **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 purpose 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.

- **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.

- **Third party** means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

- **Consent** of the data subject means any freely given, specific, informed, and unambiguous indication of the data subjects 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.

- **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.

- **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 health of that natural person, and which result in particular, from an analysis of a biological sample from the natural person in question.

- **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics or a natural person which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

- **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.

- **Main establishment** means as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.

Risk Management

GRI acknowledge and value the privacy rights of its employees, service providers and patrons and is committed to safeguarding the fundamental rights and freedoms of those affected by its use of CCTV through its policies, procedures, and practices. All images collected and stored by CCTV is personal data processing as defined by data protection law. In utilising CCTV and associated electronic systems, GRI lawfully justifies the proportionate use of these systems to manage identified risks, including:

  - to protect buildings, assets and operations, during and after operational hours,
  - to monitor and protect the safety, health and welfare of employees and visitors during operations, within the premises, car parks and the environs of the stadia grounds,

- to investigate accidents and/or incidents occurring on the premises or within the environs of stadia grounds,
- to monitor and protect the integrity of greyhound racing, sales and trial sessions within the environs of greyhound stadia grounds,
- to protect betting operations against non-compliance, fraud, and/or other criminal activity,
- to prevent bullying, pranks and/or horseplay likely to endanger safety,
- to reduce and where necessary investigate incidence of crime and anti-social behaviour (including theft, fraud or vandalism),
- to support the Gardaí in a bid to deter, detect and investigate crime,
- to assist in identifying, apprehend and prosecute offenders regarding criminal matters,

Lawful Basis for using CCTV.

GRI has a common law and statutory duty to take all reasonable steps to safeguard its employees, visitors and patrons, and therefore processes personal data to meet these requirements. In exercising its official authority as a regulatory body, GRI processes personal data as part of its regulatory function related to the greyhound racing industry and to enhance its compliance obligations under gambling regulations. It also acts in the public interest to deter, detect, and assist with investigating crime. Within the boundaries of lawful processing, GRI where necessary and proportionate will process CCTV images:

- of intruders or individuals (including employees where necessary) damaging property; removing goods without authorisation, engaging in fraudulent activity, or using violent; abusive or threating behaviour toward employees or others,
- to deter, detect, investigate, and assist in the prosecution of crime,
- for child safeguarding purposes in line with GRI's Child Safeguarding Policy,
- of activities violating greyhound racing or welfare, or betting regulations and/or protocols, including breaches of employment protocols related to such work activities,
- related to safety, security, accidents/incidents where breaches of safety rules or liability may arise,
- related to insurance and associated investigations.

When processing personal data, GRI will ensure data is:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

- Kept in a form that allows identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- Processed in a manner that ensures proper 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 to do so.

- GRI as data controller accepts responsibility for demonstrating compliance with the data protection principles set out in the GDPR.

Camera Locations

Using CCTV to monitor areas where individuals have a reasonable expectation of privacy can be difficult to justify. Accordingly, camera location is a key consideration when managing safety and security risks, while at the same time trying to safeguard the privacy rights of individuals. GRI has sought to select CCTV locations that are least intrusive, while at the same time managing safety and security risks related to its operations. Cameras installed to monitor external areas are situated in a manner to prevent and/or minimise recording passers-by or another person's private property. CCTV installation and use is proportionate to safety, security and regulatory risks to employees and operations, including wagering, food and beverage, and greyhound related activities. CCTV monitoring in public areas, by necessity, may include access/egress routes, stairs, dance floors, bars, tote, cash locations, delivery areas for goods and services, car parks, weigh rooms and kennels.

Notification and Signage

This policy can be accessed on GRI's website at www.grireland.ie. The policy sets out the purpose and legal basis for data processing related GRI's use of CCTV. Signs are posted at each site location indicating the presence of CCTV monitoring. The contact details for Greyhound Racing Ireland as data controller for this scheme is 061 448000.

Covert Surveillance

Using covert electronic systems to obtain personal data without an individual's knowledge is generally unlawful. Only in exceptional circumstances associated with a criminal investigation and in consultation with An Garda Síochána will covert surveillance be considered for use. In any situation where covert surveillance may be considered, it will be a proportionate response to risks faced by GRI, having carefully considered the matter in consultation with An Garda Síochána. In such circumstances, cognisance will be taken of the fundamental rights and freedoms of those affected. A Data Protection Impact Assessment will be conducted prior to the installation of any covert systems to assess whether the measure can be justified based on necessity and proportionality to achieve the intended purpose. Covert surveillance must be focused and of short duration. Only specific (and relevant) individuals/locations will be recorded. If no evidence is obtained within a reasonable period, surveillance will cease. If surveillance is intended to prevent crime or regulatory breaches, overt cameras will be used as a more appropriate measure and less invasive of individual privacy. Where a data processor is engaged to assist in covert surveillance, a data processor contract with GRI as data controller will be put in place in advance in compliance with the Regulation.

Managing Data Processors

The GRI as data controller will ensure that data processing carried out by its data processors (service providers) on its behalf, including security service providers, will only take place where the data processor has provided sufficient guarantees to implement appropriate technical and organisational measures to safeguard personal data. The processing arrangement between GRI as data controller and the data processor will be governed by a contract consistent with GRI's legal obligations as set out in the Regulation. Processors engaged by GRI will only process personal data on the written instructions of GRI as data controller. Procedures to execute contracts and written protocols with external processors will be adhered to by individual departments. GRI is committed to conducting due diligence on the security posture of the data processors it engages with respect to how the personal data it processes is safeguarded.

CCTV Remote Monitoring – Data Processor

CCTV remote monitoring is outsourced to an external security company as part of GRI's security protocol for the protection of its premises, assets, and employees. The service provider is a data processor as defined by the Regulation. GRI is cognisant that data protection law places several obligations on data controllers and data processors. These include a requirement for the data controller to have in place a contract with the data processor outlining what the security company may do with the data, what security standards should be in place, and for how long the data should be retained. The processor is required to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of the data particularly where the processing involves risks related to the transmission of data over a network.

Event Security and Body Worn Cameras (Bodycams)

Security companies contracted to GRI for events may only use bodycams with the permission of GRI as data controller. The arrangements for using bodycams must be incorporated into a written contract between the parties. It is GRI policy that mobile CCTV devices, where contracted and in use, should only be activated in extreme cases based on specific pre-defined criteria, and where justified for safeguarding security and safety. Personal data of recordings of employees, patrons, or others on GRI premises or within its environs must be made available to GRI on request. Where body cameras have audio recording capability, they must have separate video and audio recording controls. This is to ensure that if a situation arises which requires the video recording of an incident, the audio recording is not automatically instigated in tandem. Details of body camera recordings of incidents must be reported to GRI consistent with GRI accident/incident reporting procedures.

Data Retention

The GDPR stipulates that personal data be: *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed;"*.

Images captured by GRI's CCTV systems will be kept for a maximum of 30 days. Where images identify an issue within the 30-day retention period that lawfully justifies further investigation, the footage may be retained for a further period. Where required, the relevant footage will be downloaded and securely stored for investigative purposes until the matter has concluded. The recorded footage and recording equipment will be stored in a secured area. Access will be restricted to authorised personnel and the area secured when not occupied by authorised personnel.

Stadia management at each location are responsible for the oversight, maintenance, and access to the CCTV system. Records of access must be maintained on site including the date, time, purpose, and name of the person downloading or copying footage from GRI's electronic systems, including downloading, or copying images for any internal investigative purpose. Stadia management must maintain access records for future audit and make same available to the DPO or Data Protection Commission if/when requested.

A log of authorised individuals must be maintained on site as well as a log of access to the recorded images. In right circumstances, CCTV footage may be accessed by:

- An Garda Síochána where GRI (or its agents) are required to make a report regarding the commission of a suspected crime; or
- An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on GRI property, or
- Tusla, Child and Family Agency and/or other statutory bodies charged with child safeguarding; or
- Data subjects (or their legal representatives), pursuant to an access request in writing where the time, date and location of the recording is furnished to GRI, or
- Data subjects (or their legal representatives), subject to a court order.
- GRI racing and/or regulation officials, the Control Committee or Control Appeals Committee related to a breach of greyhound racing laws, regulations, or protocols and/or
- GRI Management to assist with a data access request or to investigate an incident or accident.
- GRI's insurance company where the insurance company require access to personal data to investigate a public or employer's liability claim, or a claim related to damaged property.

The GRI is committed to maintaining effective procedures regarding its interactions with individuals about their personal data. This includes procedures for addressing complaints and responding to requests for access to personal data.

Data Subject Access Requests

Any person whose image is recorded on a CCTV system has a right to request and be supplied with a copy of his or her personal data, but this must not adversely affect the rights and freedoms of others. The individual's identity will be verified before their request will be processed. 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.

Where an access request is received, the footage should not be deleted until the request has been fulfilled. Where an access request is received and the footage includes images of other individuals (apart from the data subject), the images of the other individuals will be pixelated or otherwise de-identified before supplying a copy of the footage to the requester. Alternatively, the consent of the other individuals featured in the footage may be sought to release the unedited version containing their images, but their consent must be received in writing in advance of releasing the footage. If for any reason, the footage is technically incapable of being copied to another device, or in other exceptional circumstances, it is not possible to provide the footage in digital format; consideration may be given to providing picture stills as an alternative to video footage. If picture stills are being relied on to satisfy the access request, enough stills for the duration of the recording (in which the

requester's image appears) will be provided to satisfy the legal obligation to supply a copy of all personal data held.

To exercise the right of access, a data subject must make an application in writing to the Data Protection Officer to have the request processed in compliance with the GDPR and the Act. The applicant is required to provide all necessary information to assist in locating their personal data, such as the date, time, and location of the recording. If the images are of such inferior quality and do not clearly identify the requester, the images may not be considered personal data and may not be released by GRI. Any requests for CCTV recordings/images by An Garda Síochána or other state agency are subject to a written request where precise details of the specific investigation or issue must be provided.

Roles and Responsibilities

The Chief Executive Officer oversees governance related to the implementation of data protection legislation for the organisation.

GRI's Data Protection Officer provides advice and monitors compliance with this policy and data protection law.

The Executive team and line managers are responsible for ensuring that departments under their remit comply with the requirements of GRI's CCTV Data Protection Policy and data protection law.

Policy Review and Update

This policy will be reviewed and amended as required considering experience, risk assessment and/or as required by law.

Appendix I Revision History Record:

Document Control No.	**(Revision No. 1) 25.06.2020 HCDP** **(Revision No.2) 05.10.2022 HL&C** **(Revision No. 3) 12.04.2024. HL&C** **(Revision No.4) 23.10.2024 HL& C**
Section	**Changes Made**
All sections	General review and update to bring greater clarity to policy and procedural aspects in line with GDPR and the Law Enforcement Directive. The review included addressing CCTV remote monitoring, managing data processors, responding to subject access requests, dealing with covert surveillance and data retention. 25.06.2020 by HCDP

	Changes made to incorporate GRI'S new title and logo. 05.010.2022 by HL&C
	Definitions amended; contents page updated. 15.04.2024 HL&C Change due to the amendment of the Occupiers Liability Act 1995 by the Courts and Civil Law (Miscellaneous Provisions) Act 2023.
	To incorporate obligations related the Gambling Regulation Act 2024 which was signed into law on 23.10.2024.