Bord na gCon

DATA PROTECTION POLICY

COMPLIANCE WITH

THE GENERAL DATA PROTECTION REGULATION 2016 (EU) 2016/679

MAY 2018

CONTENTS

IRISH GREYHOUND BOARD DATA PROTECTION POLICY

Policy Statement

It is the policy of the Irish Greyhound Board (IGB) to comply with its legal obligations as set out in the General Data Protection Regulation 2016 (EU) 2016/679 (the Regulation) and national law. The IGB recognises that the concept of accountability is one of the central themes of the Regulation. For IGB accountability essentially means that data privacy must be one of the shared values and practices of the organisation. It will therefore manage privacy risk and privacy compliance in accordance with the accountability principle contained in Article 5(2) and demonstrate compliance with each of the regulatory principles through its policies and practices. The organisation will ensure that it has sufficient organisational and technical measures in place to satisfy Article 24 of the Regulation. This requires data controllers to demonstrate that the processing of all personal data is performed in accordance with the Regulation and national law. IGB will ensure that data processing carried out by data processors on its behalf will only take place under contract in accordance with Article 28 of the Regulation. In satisfying its obligations under the Regulation, IGB will consider its legal and regulatory compliance requirements, risk profile, business objectives and the context and circumstances of all data processing carried out by the organisation. The organisation is committed to having in place policies, procedures, guidelines, checklists, training and awareness, transparency measures, organisational and technical safeguards to mitigate against internal and external risks to privacy. It is IGB policy to record all company processing activities as required under Article 30 of the Regulation. As part of its record management system, the organisation will review this policy at least annually. It will be updated as necessary considering new legislation, risk assessment processes, employee feedback, organizational changes, and practical experience. A record of changes will be maintained to ensure appropriate record management wherein the obsolete version will be removed, and the updated version circulated across the organisation as necessary.[1] This policy applies to all employees of IGB, its subsidiaries, contractors and customers. This policy becomes effective from the 25th May 2018.

[1] The revision number, date of revision and description of changes will be recorded on the Revision Control List (See Appendix 4).

GLOSSARY OF TERMS AND DEFINITIONS

The following definitions will 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, in particular 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, genic, mental, economic, cultural or social identify of that natural person;

- **Processing** means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such a collection, recording, organisation, structuring, storage, adaption 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, in particular to analyse or predict aspects concerning that natural persons performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

- **Pseudonymisation** 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;

- **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;

- **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;

SCOPE AND PURPOSE

Territorial Scope and Material Scope

The IGB as a data controller recognises that the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not as provided for by Article 3. It recognises that the material scope of this Regulation applies to the processing of personal data wholly or partly by automated means (i.e. electronically) and to the processing other than by automated means (i.e. paper records) of personal data which form part of a filing system as provided by Article 2 (1). IGB will abide by these provisions.

Purpose

To ensure that the organisation complies with the Regulation, national data protection laws and follows best practice.

- To ensure that when processing personal data, the organisation protects the privacy rights of its employees, customers and all individuals whose data it holds who may be affected by its operations.
- To ensure openness, transparency and accountability with respect to how the organisation obtains, processes, secures, transfers, updates, manages and erases personal data.
- To ensure that there is a risk management approach to the protection of personal data and that risk exposures to privacy breaches are appropriately controlled.
- To ensure that the organisation has in place procedures to respond to any breaches of privacy data rights.
- To ensure full cooperation with the supervisory authority.

This policy applies to:

- The head office of the Irish Greyhound Board.
- All subsidiaries of the Irish Greyhound Board.
- All employees and where relevant any apprentice or volunteer working or acting for the Irish Greyhound Board.
- All contractors, suppliers and others working or engaged by the organisation where the personal data of individuals is processed on behalf of IGB.
- All personal data that the organisation holds that is related to identifiable individuals as defined by the Regulation. This may include: names of individuals, postal addresses, email addresses, telephone numbers, bank details and/or any other information relating to individuals**.**

GOVERNANCE STRUCTURE & ASSIGNMENT OF RESPONSIBILITES

Board & Chief Executive Officer

The Board of Directors and the Chief Executive Officer have ultimate responsibility for ensuring that the Irish Greyhound Board (Bord na gCon) meets its legal obligations under the Regulation and national data protection legislation. This responsibility is shared by the senior executive team, the data protection officer and line management across the organisation that will ensure that the data processing activities of the company are carried out in full compliance with the Regulation. The executive and individual departmental management will ensure:

- That corporate governance processes demonstrate IGB's commitment to compliance with the Regulation.
- That the necessary organisational structures exist at a senior level and that data processing is properly managed from the top down.
- That the organisation is kept informed of all legislative changes with respect to the processing of personal data of all individuals affected by its operations.
- That this policy will be reviewed at least annually in conjunction with the data protection officer to ensure that data processing operations are compliant when preparing the Annual Directors Report for IGB.
  The responsibilities of individuals and departments are set out below:

Data Protection Officer:

- Inform and advise the Executive and the organisation of their obligations under the Regulation and national legislation.
- Engage with all stakeholders on privacy matters (e.g. marketing, IT, HR etc.)
- Monitor compliance with the Regulation and national legislation.
- Keep the Executive and the organisation updated about data privacy risks.
- Act as the contact point for the supervisory authority and co-operate with its requirements.
- Review and update as required data protection policies and related procedures to ensure compliance with the Regulation and national legislation.
- Provide advice and assistance to management and employees in relation to compliance with the Regulation and national legislation.
- Provide oversight and co-ordinate data subject access requests and act as point of contact.
- Provide guidance on privacy data security management throughout the organisation.
- Conduct audits and inspections to identify non-compliance and advise of corrective action.
- Investigate and evaluate data protection breaches, incidents and associated matters and liaise with the supervisory authority.

Management & Employees

Management and employees will ensure that all data processing undertaken by the organisation is carried out in compliance with the Regulation, national legislation and the organisations data privacy policy. At a departmental level, management and employees will ensure that there is ongoing accountability within each department to demonstrate compliance with the privacy principles contained in the Regulation. Each department will ensure it knows:

- The nature, scope and context of the personal data it processes.
- The risks associated with the data processing it undertakes.
- How it collects personal data.

- The categories of persons on whom the department holds personal data.
- The elements of personal data held on each of the data categories.
- If special categories of data are held by its department.[2]
- The purpose for which personal data is collected.
- How and where personal data is stored.
- How long the personal data is to be held.
- If personal data is shared outside the organisation.
- The name and contact details of data processors it uses.
- How to assist the DPO in responding to subject access requests.

In dealing with personal data the following principles will be observed by each member of staff:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the date subject **("lawfulness, fairness and transparency")**.
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes **("purpose limitation")**.
- Personal date shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **("data minimisation")**.
- Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must 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 **("accuracy")**.
- Personal 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 processed **("storage limitation")**.
- Personal data shall be processed in a manner that ensures appropriate security of the personal date, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **("integrity and confidentially")**.
- The controller shall be responsible for, and be able to demonstrate compliance with the Data Protection Principles **("accountability")**.

[2] Special categories of personal data are data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

ORGANISATIONAL MEASURES FOR THE PROTECTION OF DATA PRIVACY

Organisational Privacy Management Activities

- The organisation will maintain a privacy programme and mission statement which will require all stakeholders to agree and adhere to the organisations data privacy policies and procedures. It will maintain an inventory of what personal data is held and how it is processed internally and externally by the organisation. The inventory will form part of the organisations risk management approach to data privacy and will form part of this compliance manual. The organisation will conduct regular reviews and communications between those responsible and accountable for data privacy and update its records accordingly. Data privacy will be integrated into the business risk assessment and reporting structure to ensure that control measures are reviewed and updated as part of the company's risk management strategy.

Training, Information and Consultation

- The organisation is committed to maintaining a programme of information, training and awareness for employees to promote compliance with company policy and the Regulation. All staff will be given data protection training at induction stage with further refresher training provided to all staff on an annual basis. This will include training in compliance with data protection law and the organisations internal data handling policies and procedures. The organisation has a designated person from each department who liaises directly with the data protection officer on data privacy issues. This will ensure that data risk management procedures are embedded into specific departmental operations and the management of operational risks related to data privacy.

Lawful Basis for Processing Personal Data

- The organisation as Data Controller recognises that it must have a lawful basis for processing personal data as set out in Article 6 of the Regulation. The legal basis for processing personal data may include: the consent of the individual; performance of a contract; compliance with a legal obligation; necessary to protect the vital interests of a person; necessary for the performance of a task carried out in the public interest; or in the legitimate interests of the organisation except where those interests are overridden by interests or rights and freedoms of the data subject.

Special Categories of Personal Data

- The organisation will only process special categorises of data (sensitive) personal data in accordance with Article 9 of the Regulation. Special categories of personal data are data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Principles Related to the Processing of Personal Data

As required by Article 5 of the Regulation, all processing activities carried by the organisation will abide by the following principles. Personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes unless further processing is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89 (1) purposes ('purpose limitation');
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- 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 ('accuracy');
- Kept in a form which permits the identification of data subjects for no longer than necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar that the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes of statistical purposes in accordance with Article 89 (1) subject to implementation of appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')
- 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')

In compliance with Article 5 (2) of the Regulation i.e. the accountability principle, IGB is committed to demonstrating compliance with the above requirements.

Management of Individual Data Privacy

The organisation recognises the following privacy rights of individuals under the Regulation It will ensure that there are sufficient organisational and technical measures in place to comply with the following requirements:

- The right to be informed and the right to know what information has been collected (Article 13 & 14 of the GDPR)
- The right to access information (Article 15)
- The right to rectification (Article 16 & 19)
- The right to erasure (Articles 17 & 19)
- The right to portability (Article 20)
- The right to object to the processing of personal data (Article 21)
- The right of restriction (Article 18)
- Rights in relation to automated decision making, including profiling (Article 21)

Information Security Risks

- Data privacy forms part of the organisations integrated corporate security policy which includes the protection of premises and hard assets. The company is committed to maintaining an appropriate security posture relative to the risks associated with threats to persona data considering the requirements of Article 32 of the Regulation. The organisation is committed to maintaining an effective information security programme based on legal requirements, ongoing risk assessments and meeting appropriate organisational and technical standards to protect personal data. In considering information security risks, the organisation recognises best practice as set out in ISO 27001 – 2013 Information Security Standard. It will ensure that its technical security is robust and that all systems, services and

equipment used for processing and storing personal data meet the security standards required by the Regulation and national legislation. It will ensure that its protective systems such as intrusion detection, monitoring, fire walls, anti-virus, malware, encryption, cryptographic and password controls are adequate to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed. Regular checks and scans are carried out to ensure IT security hardware and software are functioning properly and that security systems are adequate to protect personal data as part of the organisation's risk management strategy.

Managing Third Party Risks

- Data processing outsourced to third party processors will only take place where the data processor has provided sufficient guarantees to implement appropriate technical and organisational measures as required by the Regulation. Processors will only process personal data on the instructions of IGB as the controller and this will be governed by a contract consistent with the IGB's legal obligations as set out in Article 28 of the Regulation. Procedures to execute contracts or agreements with all third-party processors will be maintained. The IGB is committed to conducting due diligence on the data privacy and security posture of potential vendors/processors and maintaining a privacy risk assessment process on third party processing. It will maintain a policy on 'cloud' providers and have in place procedures to address instances of noncompliance by third party processors.

Disclosing to Third Part Controllers – Data Sharing

- Where the IGB shares data with other third-party controllers it will only do so in accordance with the Regulation.

Maintaining Privacy Notices

- The organisation will maintain privacy notices to individuals consistent with its legal obligations, its data privacy policy and operational risk tolerance**.** The organisation will maintain a data privacy notice that details the organisations data privacy handling practices. It will provide data privacy notices at all points where personal data is collected. It will provide data privacy notices on location signage and through marketing and promotional website and online communications.

Responding to Requests and Complaints

- The organisation maintains effective procedures for its interactions with individuals about their personal data. This includes procedures for addressing complaints and responding to requests for access to personal data. The organisation will maintain a mechanism to update or correct personal data, respond to requests to 'opt out', restrict or object to processing personal data. Provision will be made for data portability and requests to be forgotten or erasure. The organisation will investigate root causes of data privacy complaints to ensure that corrective action is taken in a timely manner. (See Appendix 2 for SAR Procedure)

Monitoring for New Operational Practices - Data Privacy by Design and Data Privacy by Default

- IGB is committed to monitoring organisational practices to identify new processes or material changes to existing processes to ensure the implementation of privacy by design principles. Data privacy by design and data privacy by default are two crucial concepts for

future proofing the organisations data protection obligations as provided for in Article 25 of the Regulation. It is committed to embedding data privacy features and enhancing technologies into the design of future projects at an early stage in the planning process.

Data Impact Privacy Assessments

- IGB is committed to conducting data impact assessment as required by Article 35 of the Regulation where a project or initiative is likely to affect in a high-risk manner the rights and freedoms of natural persons. This approach will ensure that risks arising out of data processing activities will be identified and minimised so far as is reasonably practicable and as early as possible. The risk profile of the personal data processed within the organisation will be determined by the personal data processing operations being carried out, the complexity and scale of data processing, the sensitivity of the data processed, and the protection required for the data being processed.

Processing Children's Data

- Any processing of Children's data by IGB will only take place in full compliance with the Regulation.

Data Retention

- The organisation recognises that storing, holding and retaining data (either within the organisation or by appointing a third-party processor to do so on the organisations behalf) amounts to 'processing' under the Regulation. Accordingly, IGB recognise it is a requirement of data protection law that personal information is not kept for longer than necessary for the purpose for which acquired as set out in Article 5 (5). In complying with this requirement, IGB will ensure that all periods chosen for the retention of personal data will be fully evidenced based. Personal data will be kept for as long as any relevant statutory limitation period. IGB's policies will ensure that the above legal requirements are complied with. Where third party processors are used to store data, this will be governed by contract incorporating the above requirements.

Cooperation with the Supervisory Authority

- IGB will cooperate with all enquires, audits and/or investigations made or carried out by the Data Protection Commission and its officers.

Data Breach Management

- The organisation will maintain an effective data privacy incident and breach management program. This will include a data privacy response plan and arrangements for notifying the supervisory authority within 72 hours as required by Article 33, unless the breach is unlikely to result in a risk to the rights and freedoms of the individual/s concerned. Where breaches are likely to result in a high risk to the rights and freedoms of individuals, the person/s affected will be notified without undue delay in accordance with Article 34 of the Regulation. **(See Appendix 3)**

Risk Register

- IGB will maintain data privacy inventory and data privacy will be assessed as part of the corporate risk register to identify and mitigate against data privacy risks on an ongoing basis and to demonstrate compliance in the event of a regulatory or investigative audit.

Appendix 1 Internal Policy on Protecting Personal and Sensitive Data While at Work

Irish Greyhound Board	**Title:** **Policy on Protecting Personal and Sensitive Data while at Work**	**Department:**	All Depts.
		Document developed by:	HCLP
		Document Collaborators:	IGB Executive & Departments
		Document Approved By:	CEO
Document Reference Number:	GDPR 2018	**Responsibility for Implementation:**	HCLP
Revision Number	IGB GDPR Policy 001	**Responsibility for Review**	HCLP
Approval Date:	24th May 2018	**Responsibility for Audit**	HCLP
Implementation Date:	25th May 2018		
Review/Update Date:			

Policy Statement

The Irish Greyhound Board (IGB) is fully committed to complying with all the requirements of the General Data Protection Regulation EU 2016/679. This includes having policies and procedures in place to demonstrate how the organisation protects the personal data of its employees, contractors and customers. It is the policy of IGB to ensure that all organisational and technical measures necessary to protect data privacy will be employed by the organisation, including procedures for internal processing, handling, storing, securing and the destruction of personal data when no longer required.

Purpose

The purpose of this policy is to create employee awareness and achieve a commitment from employees to protect personal and sensitive data while at work.

Scope

This policy applies to all employees of IGB and its subsidiaries.

Roles & Responsibilities

All employees of the Irish Greyhound Board are required to comply with the requirements of the Regulation to protect the privacy rights of all individuals whose data is process by the Irish Greyhound Board.

Procedural Guidance

The below list is not exhaustive but gives an indication of some simple steps that should be taken to protect personal and sensitive data while at work.

- Employees are required to keep all data secure by taking sensible precautions and not allowing data to become vulnerable to unauthorised access, accidental loss, alteration, damage or destruction.
- The only people permitted to access personal data are those that are required to do so as part of their work.
- Personal data should not be shared informally within the organisation but should only be processed in line with company policy.
- Personal data should not be disclosed to unauthorised persons either within the company or externally.
- Personal and sensitive data should not be left on desks during breaks or for prolonged periods but should be secured until the staff member returns.
- Personal and sensitive information should be locked away when not in use or at end of day.
- When not required, paper records should be kept secure in a drawer, filing cabinet or office.
- Personal data (paper records) should be protected against unauthorised access, including unauthorised visual access.
- Personal data should not be left where unauthorised access may inadvertently be gained e.g. on photocopiers.
- Data printouts should be shredded and securely disposed of when no longer required.
- Data should be regularly reviewed and updated if found to be out of date. If no longer required, it should be appropriately disposed of.
- Where data is stored electronically it must be protected from unauthorised access, accidental loss and malicious hacking attempts.
- Computer screens should be locked when unattended.
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- Personal data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- Employees should not save copies of personal data to their own computers.
- Where data is being transferred electronically using memory sticks, these must be encrypted.

References

The General Data Protection Regulation EU 2016/679.

Revision History

This document will be updated arising from changes in legislation, risk improvements, organizational, developments, employee feedback and experience.

Appendix 2 Subject Access Request Policy & Procedure

Irish Greyhound Board	**Title:** **Subject Access Request Policy & Procedure**	**Department**	All Depts.
		Document developed by:	HCLP
		Document Collaborators:	IGB Executive & Departments
		Document Approved By:	CEO
Document Reference Number:	GDPR 2018	**Responsibility for Implementation:**	HCLP
Revision Number	IGB GDPR Policy 002	**Responsibility for Review**	HCLP
Approval Date:	24th May 2018	**Responsibility for Audit**	HCLP
Implementation Date:	25th May 2018		
Review/Update Date:			

Policy Statement

It is the policy of the Irish Greyhound Board to comply fully with Article 15 of the Regulation with respect to personal data access requests. Requests will be responded to without undue delay but in any event within one month of receipt of the request. Information shall be provided free of charge with the exception of where a reasonable administrative fee may be applied for additional copies of the records requested. A fee may also apply if a request is *'manifestly unfounded or excessive'* or may be refused for this reason as provided for in Article 12 (5) of the Regulation. The rights of individuals to obtain copies of their personal data (through subject access requests) will not be permitted to adversely affect the rights and freedoms of others. Subject access requests can be sent to the dataprotectionofficer@igb.ie

Purpose

The purpose of this SOP is to ensure that all subject access requests are dealt with in compliance with the Regulation.

Scope

Article 15 of the Regulation addresses the right of data subjects to: obtain confirmation of whether their personal data is being processed, where, how and what data is being processed and how the right to access can be achieved. The Article lists further information that should be supplied including: purpose of processing, categories of data, recipients of data, data storage period, right to rectification & complaint, source of data, existence of automated processing as well as associated logic and consequences and, safeguards for transfer to third countries or international organisations. Accordingly, this SOP applies to all individuals that are the subject of personal data as defined by the Regulation and which are held by the Irish Greyhound Board.

Definitions

'Personal data' for the purposes of this procedure 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 name, an

identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genic, mental, economic, cultural or social identify of that natural person.

Roles & Responsibilities

The Data Protection Officer (DPO) is the point of contact for all Subject Access Requests to the organisation. The DPO is responsible for overseeing compliance with Article 15 of the Regulation and ensuring that the request is logged, assessed, circulated and responded to within the statutory period. The executive team are responsible for ensuring cooperation with SAR's and that all records /information is provided in a timely manner from within individual departments to respond to the SAR's within the statutory period of one month.

Procedure

When the organisation receives a subject access request (SAR), it is passed to the Data Protection Officer (DPO) as the point of contact for dealing with such requests. The DPO will ensure sufficient proof of the identity of the person making the request prior to processing. The DPO will circulate the SAR to the relevant parties' e.g. Human Resource department or across the organisation as required. A full review of all records relevant to the request will be carried out to meet the requirements of the SAR under the Regulation. The SAR will be responded to within one month.

References

The General Data Protection Regulation EU 2016/679

Revision History

This policy will be updated as necessary considering new legislation, risk assessment processes, employee feedback, organizational changes, and practical experience.

Appendix 3 Data Breach Policy & Procedure

Irish Greyhound Board	**Title:** **Data Breach Policy & Procedure**	**Department**	All Depts.
		Document developed by:	HCLP
		Document Collaborators:	IGB Executive & Departments
		Document Approved By:	CEO
Document Reference Number:	GDPR 2018	**Responsibility for Implementation:**	HCLP
Revision Number	IGB GDPR Policy 003	**Responsibility for Review**	HCLP
Approval Date:	24th May 2018	**Responsibility for Audit**	HCLP
Implementation Date:	25th May 2018		
Review/Update Date:			

Policy Statement

It is the policy of the Irish Greyhound Board (IGB) to deal with any potential data privacy breach in compliance with the Regulation. IGB as data controller will, without undue delay and where feasible, but no later that 72 hours of becoming aware of the breach notify the supervisory authority, unless the data breach is unlikely to result in a risk to the rights and freedoms of the persons subject to the breach. If for any reason notification to the supervisory authority is not made within 72 hours, the notification will be accompanied with reasons for the delay. Where a personal data breach is likely to result in a high risk to the rights and freedoms of the person/s concerned, IGB as data controller will inform the person/s affected without undue delay.

This policy covers three different types of notification: (i) notification by a data controller to the supervisory authority (ii) notification by a data processor to the data controller whose data is the subject of the breach; and (iii) notification by a data controller to data subjects i.e. individual/s affected by the data privacy breach.

Note: IGB will maintain a register of all data protection breaches whether or not such breaches are to be notified to the supervisory authority.

Purpose

The purpose of this procedure is to ensure that IGB plan in advance and have in place processes to detect and properly contain a breach, to assess the risk to individuals, and determine whether it is necessary to notify the competent supervisory authority, and communicate the breach to the individuals concerned. Communicating a breach to individuals where necessary will allow IGB as data controller to provide information on the risks presented as a result of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan will be on protecting individuals and their personal data. This policy forms part of IGB's formal personal data breach notification procedure in compliance with Articles 33 and 34 of the Regulation.

Scope

This policy applies to IGB, its subsidiaries and all data processors used by IGB.

Definition

Article 4 (12) of the Regulation defines 'personal data breach' "*as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of , or access to, personal data transmitted, stored or otherwise processed."*

Roles & Responsibilities

All managers and employees of IGB have responsibility to report any potential breach of data protection to the their line manager and the Data Protection Officer who will assess the situation and decide if the matter is to be reported to the supervisory authority and the Individual/s concerned. Where a data breach involves a data processor engaged by IGB, the data processor is obliged to contact IGB's data protection officer without undue delay but not later than 24 hours of becoming aware of the data breach.

This risk assessment will take account of the following:

- The type of breach.
- The nature, sensitivity and volume of personal data.
- Ease of identification of the individual/s subject of the breach.
- Severity of consequences for individuals.
- Numbers of individuals affected.

If deemed necessary the DPO will set up an incident team to deal with all aspects of the data privacy breach within specific timelines which will include (Phase 1) close down breach and establish facts within 48 hours (Phase 2) complete investigation report and notify the supervisory authority within 24 hours (Phase 3) without undue delay, implement lessons learned and update policies and systems. Where a data privacy breach has been notified to IGB by one of its data processors, the above approach will be taken in cooperation with the data processor in accordance with the contract.

Procedure

Where a data privacy breach has occurred which will is likely to result in a risk to the rights and freedoms of the persons concerned, the supervisory authority and the individual/s concerned will be notified.

Notification to the supervisory authority will include the following information:

- Description of the nature of the personal data breach including where possible, the categories and approximate numbers of data subjects/records concerned.
- The name and contact details of the data protection officer.
- Description of the likely consequences of the personal data breach.
- Description of the measures to be taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible effects.

Notification to the individual/s concerned will be without undue delay unless:

- The personal data is encrypted (and is backed up/otherwise available)
- Immediate measures have been taken to ensure there is no longer a high risk to the data subject.
- Where notification to individuals would require disproportionate effort an effective public communication will be made to inform individuals on what steps are being taken to deal with the data breach and how the individuals can best protect themselves from its impact.

References

- Article 33 & 34 of the Regulation.
- Article 29 Guidelines on Personal Data Breach Notification under Regulation EU 2016/679

Revision History

This policy will be updated as necessary considering new legislation, risk assessment processes, employee feedback, organizational changes, and practical experience.

Appendix 4 Revision Control

Document Control No. - IGB GDPR POLICY 25052018 (Revision No.)	
Section	**Changes Made: By:**

Appendix 5 Signature Sheet

I have read, understand and agree to adhere to the attached Policy & Procedure:

Print Name	Signature	Area of Work	Date