Bord na gCon

DATA PROTECTION POLICY

COMPLIANCE WITH

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

And

DATA PROTECTION ACTS 1988-2018

CONTENTS

IRISH GREYHOUND BOARD DATA PROTECTION POLICY

It is the policy of the Irish Greyhound Board (IGB) as a data controller to comply with its legal obligations as set out in the General Data Protection Regulation 2016 (EU) 2016/679 (the Regulation) and the Data Protection Acts 1988 -2018. The IGB recognise the concept of accountability as one of the central themes of the Regulation. For IGB, the principle of accountability essentially means the protection of personal data must be maintained as one of its shared values and practices across the organisation. It will therefore manage data protection 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 (1) and (2) 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. It is IGB policy to maintain a record of all personal data processing activities as stipulated by Article 30 of the Regulation. IGB will ensure that personal 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, IGB will consider its legal and regulatory compliance requirements, risk profile, business objectives and the context and circumstances of all personal data processing carried out by the organisation. The organisation has a designated Data Protection Officer and 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. In meeting its obligations under Article 24 and 30, the organisation will review this policy at least annually. It will be updated as necessary taking into consideration any new legislation, risk assessment processes, employee feedback, organisational changes, and practical experience. A record of changes will be maintained to ensure appropriate transparency 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 and contractors for the safeguarding of the personal data processed by IGB or its data processors.

[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, genetic, mental, economic, cultural or social identity 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** 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 or 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;

Article 4 of the Regulation should be referenced for additional definitions related to personal data processing and compliance.

SCOPE AND PURPOSE

Territorial Scope and Material Scope

The IGB as a data controller recognises 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 (1). 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 processing other than by automated means (i.e. paper records) of personal data which form part of a filing system or intended to form part of a filing system as provided by Article 2 (1). IGB will abide by these provisions.

Purpose

- To ensure the organisation complies with the Regulation, national and other associated data protection laws and best practice.
- To ensure when processing personal data, the organisation safeguards the personal data and privacy rights of its employees, customers and all individuals whose data it processes and who may be affected by its processing operations.
- To ensure openness, transparency and accountability with respect to how the organisation, collects, records, organises, structures, stores, adapts, alters, retrieves, consults, uses, discloses by transmission, disseminates or otherwise makes available, aligns, combines, restricts, erases or destroys personal data.
- To ensure that there is a risk management approach to the protection of personal data and that risk exposures related to the processing of personal data are appropriately controlled.
- To ensure that the organisation has in place procedures to respond to incidents or security breaches, which may lead to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed.
- To ensure appropriate internal support and cooperation with the DPO in meeting the organisations obligations under data protection law.
- To ensure full cooperation with the supervisory authority.

The application of this policy includes the following:

- The Irish Greyhound Board head office.
- 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 are processed on behalf of IGB.
- Any information that the organisation processes that relates to an identified or identifiable natural person as defined by the Regulation. This may include names of individuals, postal addresses, email addresses, telephone numbers, bank details and/or any other information.
- All personal data processing undertaken by IGB including: any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure, by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction.

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. The Executive team and line management across the organisation also share responsibility and will ensure data processing activities of the company are carried out in full compliance with the Regulation. The Data Protection Officer, Owen O'Doherty will advise and monitor compliance with the Regulation. The Executive 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 compliance is properly managed from the top down including within their respective departments.
- That the organisation and individual departments maintain appropriate records of compliance related to personal data processing.
- That appropriate resources, support and co-operation are given to the DPO to carry out his tasks as provided for by the Regulation.

Responsibilities of individuals and departments

Data Protection Officer

As a public body, IGB has a formally designated Data Protection Officer (DPO). As data controller, IGB is committed to ensuring that the DPO is properly involved in a timely manner on all issues related to data protection, including access to all data processing operations. The DPO will have proper support and access to resources to fulfil his functions. The DPO will:

- Inform all levels of the organisation and its employees of their obligations under the Regulation.
- Monitor compliance with the Regulation and with company policy related to the protection of personal data, including staff training and conducting internal audits.
- Provide advice, where requested, concerning Data Privacy Impact Assessments and monitor its performance.
- Cooperate with the supervisory authority on issues related to data protection processing and related matters.
- Haver regard to the risks associated with processing personal data and engage with all stakeholders on such matters.
- Review and arrange the update of data protection policies and related procedures to ensure compliance with the Regulation and national legislation.
- Provide advice to employees in relation to data protection 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 security risks associated with the data processing activities of the organisation.
- Act as the contact point for the supervisory authority and co-operate with its requirements.
- Evaluate data protection compliance, investigate non-compliance, incidents, and security breaches, associated matters, and liaise with the supervisory authority as required.

Management & Employees

Executive members, line managers and employees will ensure that all data processing undertaken at departmental level is compliant with the Regulation, national legislation and the organisation's data protection policy. At departmental level, management and employees will ensure there is ongoing accountability within each department to demonstrate compliance with the principles and requirements of the Regulation. Executive members and line managers will ensure their staff know and understand:

- The nature, scope and context of personal data processing carried out.
- The risks associated with the data processing it undertakes.
- How and why it collects personal data.
- The data subject categories on whom its department processes and holds personal data.
- The elements of personal data processed for each of the data subject categories.
- Know the special categories of data processed and held by its department.[2]
- The purpose for which personal data is processed.
- The legal basis on which personal data is processed.
- How and where personal data is stored.
- How long the personal data is retained relative to its purpose.
- If personal data is shared outside the organisation, where, how, when and with whom.
- The name and contact details of external data processors it uses.
- That a data processor contracts are in place for any external data processors.
- How to assist the DPO in his compliance role and in responding to subject access requests.

When processing personal data, the following principles will be adhered to by each staff member:

- 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 identify 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 that will require all stakeholders to agree and adhere to the organisation's data privacy policies and procedures. It will maintain a register of the data processing activities of the organisation on the personal data processed internally and externally. The register will form part of the organisation's risk management approach to data privacy. The organisation will conduct regular reviews and communications with those responsible and accountable for personal data processing and update its records accordingly. Data protection compliance 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 relevant staff will be given data protection training at induction stage with further refresher training as required. Training in data protection is reviewed 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 nominated a person from each department who is responsible for maintaining records related to the data processing activities of its department. Training individuals with responsibility for processing personal data at all levels is a prerequisite to meeting compliance requirements.

Lawful Basis for Processing Personal Data

- The organisation recognises it must have a lawful basis for processing personal data as set out in Article 6 of the Regulation. The legal basis for data processing is considered under the specific criteria specified in the Article. Including: consent of the individual, performance of a contract, a legal obligation of the controller, to protect the vital interests of a person, 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 the 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 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.

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)
- The right to erasure (Articles 17)
- The right to portability (Article 20)
- The right to object to the processing of personal data (Article 21)
- The right of restriction (Article 18)
- The right to object to automated decision making, including profiling (Article 22)
- Right to be notified regarding rectification, erasure or restriction (Article 19)

Information Technology - Security Risks

- The IGB is committed to ensuring data protection precaution is maintained and integrated into the organisations corporate security policy, including 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 personal data and the requirements of Article 5 (1) (f) and the stipulations of Article 32 (1) for safeguarding personal data including:

  (a) the use of pseudonymisation and encryption of personal data;

(b) the ability to ensure 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, and

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

The organisation is committed to maintaining an effective data protection security programme based on legal requirements, ongoing risk assessments and meeting organisational and technical standards to protect personal data. 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, firewalls, anti-virus, malware, encryption, cryptographic and password controls are adequate to safeguard 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. External auditors conduct audits on IGB's internal and cyber security risks.

Managing Third Party Risks

- The IGB is committed to ensuring that 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 data controller. 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.

Disclosing to Joint Controllers – Data Sharing

- Where the IGB shares data as a joint controller or with other independent controllers, it will only do so in accordance with the Regulation.

Maintaining Privacy Notices

- The organisation will maintain privacy notices consistent with its legal obligations, its data privacy policy and operational risk tolerance**.** It recognises the requirement of Article 12 (7) with respect to providing information specified in Articles' 13 and 14 and more particularly, information with respect to data subject rights as set out in Articles' 15-22 of the Regulation. The organisation will maintain data privacy notices that detail the organisation's data privacy handling practices. It will provide data privacy notices at points where personal data is collected. It will provide data privacy notices on location signage and through marketing and promotional websites and online communications.

Responding to Requests and Complaints

- The IGB 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. The organisation will maintain a mechanism to update and/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 made 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 DSAR 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 by Article 25 of the Regulation. IGB 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 assessments 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 from proposed data processing activities will be identified and minimised at an early state so far as is reasonably practicable. The risk profile of the personal data processed within the organisation will be determined by the personal data processing operations being carried out, including: the complexity and scale of data processing, the number and categories of data subjects, the nature and 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 and the Data Protection Act 2018.

Data Retention Period

- 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) qualifies as 'processing' under the Regulation. IGB recognise it is a requirement of data protection law, that personal data should not be retained beyond the specified, explicit and legitimate purpose for which it was required as set out in Article 5 (1) (e) of the Regulation. Where personal data may be stored for longer periods, this will only be insofar that the personal data is processed solely for archiving purpose in the public interest, scientific or historical purposes in accordance with Article 89 (1). In complying with this requirement, IGB will ensure that all criteria and periods chosen for the Retention Period of personal data will be fully evidenced based. Personal data will be retained for as long as any relevant statutory limitation period or in accordance with company retention periods and/or specific criteria in compliance with the Regulation. 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 (DPC). The DPO will cooperate with the DPC in his role as provided for under the Regulation.

Data Breach Management

- The organisation will maintain an effective breach management strategy. This will include risk assessment, remedial action, mitigation, and arrangements for notifying the supervisory authority. The supervisory authority will be notified within 72 hours, after becoming aware of the breach 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)**

Register of Processing Activities

- To meet the requirements of Article 24 and 30 of the Regulation, IGB will maintain a record of its data processing activities across the organisation. The appropriateness of these measures is based on a risk assessment that takes into account the nature, scope, context and purpose of processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals. IGB's personal data processing activities are informed by the organisation's policy and procedures that enable IGB monitor compliance with the Regulation. IGB will maintain a record of its processing activities and cooperate with the supervisory authority in making these records available to the authority on request.

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 prepared by:	DPO
		Document Collaborators:	DPO & IGB Departments
		Document Approved By:	CEO
Document Reference Number:	GDPR 2018	**Responsibility for Implementation:**	IGB Executive & Department staff
Revision Number	IGB GDPR Policy 001	**Responsibility for Review**	DPO
Approval Date:	24th May 2018	**Responsibility for Audit**	DPO
Implementation Date:	25th May 2018		
Review/Update Date:	9th September 2019		

Policy Statement

The Irish Greyhound Board (IGB) is 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 processed 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 inside or outside the company.
- Personal and/or 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/or sensitive information should be locked away when not in use and 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 erased or shredded. If no longer required, it should be securely 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. However, where data is being transferred electronically to laptops or using memory sticks, these must be encrypted.
- Employees should not save copies of personal data to their own computers.

References

The General Data Protection Regulation EU 2016/679.

Revision

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

Appendix 2 Data Subject Access Requests Policy & Procedure

Irish Greyhound Board	**Title:** **Subject Access Request Policy & Procedure**	**Department**	All Depts.
		Document prepared by:	DPO
		Document Collaborators:	DPO & IGB Departments
		Document Approved By:	CEO
Document Reference Number:	GDPR 2018	**Responsibility for Implementation:**	Executive & Department staff
Revision Number	IGB GDPR Policy 002	**Responsibility for Review**	DPO
Approval Date:	24th May 2018	**Responsibility for Audit**	DPO
Implementation Date:	25th May 2018		
Review/Update Date:	9th September 2019		

Policy Statement

It is the policy of the Irish Greyhound Board to comply with Article 15 of the Regulation with respect to 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. As provided for by Article 12 (5) (a) & (b) of the Regulation, a fee may apply if a request is *'excessive'* or may be refused if 'unfounded'. 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

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 additional information that should be available to a data subject making a request. This includes the purpose of processing, categories of data, recipients of data, data storage period, right to rectification, erasure, restriction and the right to lodge a complaint. The right to know the source i.e. who provided the data, existence of automated processing as well as logic and consequences of automated processing and the safeguards in place related to transfer of personal data to third countries or international organisations is also provided for. These provisions are available to any individual whose personal data is processed by the Irish Greyhound Board as defined by the Regulation.

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 Data Subject Access Requests (DSAR's) to the organisation. The DPO will oversee compliance with Article 15 of the Regulation to ensure that the request is logged, assessed, circulated and responded to within the statutory period. The executive team are responsible for ensuring cooperation with DSAR's and that any information related to the identified or identifiable data subject is provided in a timely manner from within their departments to enable a response to the DSAR within the statutory period of one month.

Procedure

When the organisation receives a data subject access request (DSAR), 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 identity of the person making the request prior to processing. The DPO will circulate the DSAR to the relevant parties within the organisation. A review of all information relevant to the request will be carried out to meet the requirements of the DSAR under the Regulation. The DSAR will be responded to within one month unless an extension of time is necessary as provided by the Regulation. In responding to DSAR'S, IGB will ensure that the rights and freedoms of others will not be adversely affected.

References

The General Data Protection Regulation EU 2016/679
Data Protection Act 2018

Revision

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

Appendix 3 Data Breach Policy & Procedure

Irish Greyhound Board	**Title:** **Data Breach Policy & Procedure**	**Department**	All Depts.
		Document prepared by:	DPO
		Document Collaborators:	DPO & IGB Departments
		Document Approved By:	CEO
Document Reference Number:	GDPR 2018	**Responsibility for Implementation:**	IGB Executive & Department staff
Revision Number	IGB GDPR Policy 003	**Responsibility for Review**	DPO
Approval Date:	24th May 2018	**Responsibility for Audit**	DPO
Implementation Date:	25th May 2018		
Review/Update Date:	9th September 2019		

Policy Statement

It is the policy of the Irish Greyhound Board (IGB) to deal with any data protection breach in compliance with the Regulation. IGB as data controller will, without undue delay but no later than 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 types of notification:

(i) notification by IGB as data controller to the supervisory authority

(ii) notification by a data processor to IGB as data controller of a data protection breach of which the data processor has become aware; and

(iii) notification by a data controller to data subjects i.e. individual/s affected where there is a high risk to the rights and freedoms of the data subjects. IGB will maintain a register of all data protection incidents regardless of whether or not such incidents are required to be notified to the supervisory authority.

Purpose

The purpose of this procedure is to ensure that IGB plan and have in place procedures to detect and properly contain a breach, assess the risk to individuals, and determine whether it is necessary to notify the competent supervisory authority, and/or communicate the breach to the individuals concerned. Communicating a breach to individuals where necessary will allow IGB to provide information on the risks presented because of the breach and the steps that individuals can take to protect themselves from its potential consequences. The focus of the breach response plan will be on risk mitigation and 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 IGB managers and employees have responsibility to report any potential security breach of personal data to 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 affected. 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.

On being made aware of a breach, the DPO will set up an incident team to deal with all aspects of the data breach within specific timelines. This will include, (Phase 1) close down the breach and establish facts within 24 hours (Phase 2) complete a preliminary investigation report within 48 hours (Phase 3) where required, notify the supervisory authority within 72 hours of becoming aware of the incident. Where a security 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.

IGB recognize that a personal data breach can affect the availability and integrity of personal data as well as confidentiality and other related infringements. As part of its breach management and risk mitigation plan, IGB 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.
- The risks to the rights and freedoms of those affected.
- The varying likelihood and severity, which may result from the breach.
- The physical, material and/or non-material damage.
- Whether the breach may give rise to discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage where data subjects might be deprived of their rights or freedoms or prevented from exercising control over their personal data.
- Risk exposures and reporting obligations of the organisation.

Reporting 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 where required relative to the respective provisions of the Regulation. **(See Appendix 4)**

Notification to the supervisory authority will include the following information:

- Description of the nature and circumstances 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 taken and/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

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

Appendix 4 Personal Data Breach Report Form

PERSONAL DATA SECURITY BREACH REPORT FORM: if you discover a personal data security breach, please notify your Head of Department immediately. Please complete this form and return it to the Data Protection Officer at dataprotectionofficer@igb.ie as soon as possible.

Notification of data security breach - date(s) of when breach is known to have occurred:	
Date breach was discovered:	
Name of person that discovered breach:	
Name of person reporting breach:	
Contact details of person that discovered breach:	
Contact details of person reporting breach:	
Brief description of the nature of personal data security breach:	
Number of Data Subjects affected – if known	
Brief description of any action taken when breach was discovered:	
Date reported to the Data Protection Officer	
DPO's use Only Date received:	
Was incident reported to the Data Protection Commission?	
Date incident was reported to DPC:	

Appendix 5 Data Retention Period Policy

Irish Greyhound Board	**Title:** **Policy on the Retention Period of Personal data**	**Department:**	All Depts.
		Document prepared by:	DPO
		Document Collaborators:	DPO & IGB Departments
		Document Approved By:	CEO
Document Reference Number:	GDPR 2018	**Responsibility for Implementation:**	IGB Executive & Departments
Revision Number	IGB GDPR Policy 004	**Responsibility for Review**	DPO
Approval Date:	24th May 2018	**Responsibility for Audit**	DPO
Implementation Date:	25th May 2018		
Review/Update Date:	9th September 2019		

Policy Statement

The IGB is committed to complying with all requirements of the General Data Protection Regulation EU 2016/679 including its obligation related to storage limitation as set out in Article 5 (1) (e) of the Regulation. This stipulates that personal data should not be kept in a form, which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed. Personal data may however be stored for longer periods insofar that the personal data is being processed solely for archiving purpose in the public interest, scientific or historical purposes in accordance with Article 89 (1). This provision is subject to the implementation of appropriate technical and organisational measures required by the Regulation to safeguard the rights and freedoms of the data subjects.

The organisation is committed to ensuring that time limits are established for all personal data retained based on statutory time limits or company policy. Personal data will only be retained where there exists a specified, explicit and legitimate purpose for the processing, which is underpinned by a legal basis for the processing the personal data. Where personal data is no longer to be retained based on company policy in compliance with the Regulation, it will be appropriately erased and/or destroyed following review.

Purpose

To create employee awareness and achieve a commitment from employees to appropriately manage personal data, ensuring that that personal data are not retained except for specified, explicit and legitimate purpose in accordance with company policy and the Regulation.

Scope

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

Roles & Responsibilities

Department heads and staff are required to maintain an inventory of data processing activities to ensure that data subjects and categories of data pertaining to them are only retained for times consistent with the stipulations set down by the Regulation.

Procedural Guidance

- A top-down approach will be taken with respect to data retention periods and destruction.
- Each department is responsible for the retention period it applies to the personal data it processes and erasure/destruction of the personal data as necessary in compliance with its departmental retention periods.
- To ensure IGB retains personal data in compliance with the Regulation, departments will maintain a record of their processing activities in writing including established time limits and criteria, which will be periodically reviewed in accordance with departmental requirements.
- Personal data will only be retained where there is a specified, explicit and legitimate purpose for the processing with the exception of the provisions set out in Article 5 (1) (e).
- Personal data will only be retained where there is a lawful basis for processing.
- IGB will ensure that personal data retained is protected, providing appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organizational measures.
- Personal data will be retained and erased in accordance with IGB's Retention Policy and in compliance with the Regulation.
- Hardcopy documents will be securely destroyed by shredding at the end of their retention period.
- Electronically stored data will be securely erased at the end of their retention period.
- Electronic media used to store data such as hard disc will be physically destroyed at the time of their decommissioning.
- Methods used to erase by digital deletion and/or physical destruction will ensure that the data cannot be retrieved.

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 6 Revision Control

Document Control No. - IGB GDPR POLICY 25052018 (Revision No. 1)	
Section	**Changes Made:** General amendments made throughout the document in November 2019 review **By: DPO**
All	Changes made in light of greater understanding of GDPR requirements by the organisation.
	Name of DPO, department heads and designated staff members added relative to data processing area and responsibility.
	Departmental data mapping document added to policy document.
	Inserted data breach report form.
	Reviewed and updated retention policy.

Appendix 7 Records of Departmental Processing Activities

Department Heads and Designated Persons

Print Name	Signature	Area of Work	Date
		Human Resources	
		Finance	
		Marketing Syndication Communications	
		IT Department & Wagering	
		Regulation	
		Greyhound Welfare	
		Laboratory	
		Greyhound Stadia	
		Events Hospitality Services	
		CEO's Office & Board Meetings	
HC-DPO Owen O'Doherty			