gaelcon irish games association

IGA

Data Protection Policy

Date of Last Review	14/05/2024
Revision Number	0

Table of Contents

1. Background – Who we are and what we do

For information on the Gaelcon Irish Games Association (hereafter referred to as The IGA), Refer to our Vision and Missions Statement and our website.

2. Statement of Policy

The purpose of this document is to provide a concise policy regarding the data protection obligations of The IGA.

The IGA is a data controller with reference to the personal data which it manages, processes and stores.

Members/volunteers of The IGA should refer to the guidance provided by the Office of the Data Protection Commissioner (www.dataprotection.ie) as well as seeking professional advice regarding best practice in this area.

This policy shall be amended as required and the Executive will review this policy as part of its organisation-wide policies review process outlined in the matrix for reviewing all IGA policies.

3. Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions apply within this Policy.

Data

This includes both automated and manual data.

Automated data means data held on a computer, or stored with the intention that it is processed on a computer.

Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.

Personal Data

Information that relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of The IGA.

Sensitive Personal Data

Sensitive personal data is personal data which relates to specific aspects of one's identity or personality, and includes information relating to ethnic or racial identity, political or ideological

beliefs, religious beliefs, trade union membership, mental or physical well-being, sexual orientation, or criminal record.

Data Controller

The legal entity responsible for the acquisition, processing and use of the personal data. In the context of this policy; The IGA is the data controller.

Data Subject

A living individual who is the subject of the personal data, i.e. to whom the data relates either directly or indirectly.

Data Processor

A person or entity who processes personal data on behalf of The IGA on the basis of a formal, written contract, but who is not an employee of The IGA.

Data Protection Officer (DPO)

A person appointed by The IGA to monitor compliance with the appropriate data protection legislation, to deal with Subject Access Requests, and to respond to data protection queries from staff members and the general public.

Staff

Any Director, Exec member, or volunteer of The IGA, or any person acting in an official capacity as part of or on behalf of The IGA.

4. Scope

The policy covers both personal and sensitive personal data held in relation to its data subjects by The IGA. The policy applies equally to personal data held in manual and automated form. All personal and sensitive personal data will be treated with equal care by The IGA. Both categories will be equally referred to as personal data in this policy, unless specifically stated otherwise.

5. Rationale

As a data controller The IGA and its staff, including all volunteers, must comply with the data protection rules set out in the relevant Irish legislation.

This Policy applies to all personal data collected, processed and stored by The IGA in the course of its activities.

Personal data gathered may include a combination of identification elements such as physical limitations, occupation, home address, contact details, etc.

In its role as a volunteer coordinator, The IGA may keep information relating to a volunteer and/or staff member's physical, physiological or mental well-being, as well as their economic, cultural or social identity, where necessary.

The IGA collects data on those purchasing from our website for the purpose of processing orders, including, but not limited to, names, addresses, and emails.

To the extent that The IGA's use of personal data qualifies as 'business to customer' processing, including the organisation's communications to its Staff, the organisation is mindful of its obligations under the relevant Irish legislation, namely:

- The Irish Data Protection Acts (1988 - 2018);
- The Irish Data Protection (Amendment) Act (2003); and
- General Data Protection Regulation (GDPR) 2016/679,

6. The IGA as a Data Controller

In the course of its daily organisational activities, The IGA acquires, processes and stores personal data in relation to living individuals. To that extent, The IGA is a data controller, and has obligations under Data Protection legislation, which are reflected in this document.

In accordance with Irish Data Protection legislation, this data must be acquired and managed fairly.

The IGA is committed to ensuring that all Staff have sufficient awareness of the legislation in order to be able to anticipate and identify a data protection issue, should one arise. In such circumstances, Staff must ensure that the DPO is informed, in order that appropriate corrective action is taken.

Due to the nature of the services provided by The IGA, there is a regular and active exchange of personal data between The IGA and its data subjects. In addition, The IGA exchanges personal data with data processors on the data subjects' behalf. This is consistent with The IGA's obligations under the terms of its contracts with its data processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the DPO to seek clarification.

6.1. Third-Party Processors (where applicable)

In the course of its role as data controller, The IGA engages third-party service providers, or data processors, to process personal data on its behalf.

In each case, a formal, written contract is in place with the processor, outlining their obligations in relation to the personal data, the security measures that they must have in place to protect

the data, the specific purpose or purposes for which they are engaged, and the understanding that they will only process the data in compliance with Irish Data Protection legislation.

The contract will also include reference to the fact that the data controller is entitled, from time to time, to audit or inspect the data management activities of the data processor, and to ensure that they remain compliant with the legislation, and with the terms of the contract.

6.2. The Data Protection Rules

The following key rules are enshrined in Irish and EU legislation such as the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) which are fundamental to The IGA's data protection policy.

In its capacity as data controller, The IGA ensures that all data shall:

1. Be obtained and processed fairly and lawfully

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the data controller (The IGA);
- The purpose(s) for which the data is being collected;
- The person(s) to whom the data may be disclosed by the data controller;
- Any other information that is necessary so that the processing may be fair.

The IGA will meet this obligation in the following way:

- Where possible, the informed consent of the data subject will be sought before their data is processed;
- Where it is not possible to seek consent, The IGA will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where The IGA intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view, prior to the recording;
- Processing of the personal data will be carried out only as part of The IGA's lawful activities, and it will safeguard the rights and freedoms of the data subject;
- The data subject's data will not be disclosed to a third party other than to a party contracted to The IGA and operating on its behalf, or where The IGA is required to do so by law.

2. Be obtained only for one or more specified, legitimate purposes

The IGA will obtain data for purposes which are specific, lawful and clearly stated. A data subject will have the right to question the purpose(s) for which The IGA holds their data, and it will be able to clearly state that purpose or purposes.

3. Not be further processed in a manner incompatible with the specified purpose(s)

Any use of the data by The IGA will be compatible with the purposes for which the data was acquired.

4. Be kept safe and secure

The IGA will employ high standards of security in order to protect the personal data under its care and implement privacy by design and by default principles across all our systems and processes. The IGA's Password Policy and Data Retention & Destruction Policies guarantee protection against unauthorised access to, or alteration, destruction or disclosure of any personal data held by The IGA in its capacity as data controller.

Access to, and management of, staff and customer records is limited to those staff members who have appropriate authorisation and password access.

In the event of a data security breach affecting the personal data being processed on behalf of the data controller, the relevant third party processor will notify the data controller without undue delay.

Data breaches shall be addressed as per the approach outlined in Section 6.5.

5. Be kept accurate, complete and up-to-date where necessary

The IGA will:

- Ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. The IGA will aim to conduct a review of sample data every six months to ensure accuracy;
- Ensure that staff contact details are reviewed and updated every two years, or on an 'ad hoc' basis where staff members inform the office of such changes;
- Conduct regular assessments in order to validate the need to keep certain personal data.

6. Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed

The IGA will ensure that the data it processes in relation to data subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. Not be kept for longer than is necessary to satisfy the specified purpose(s)

The IGA has identified a matrix of data classification, see Appendix 1, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the respective retention period has elapsed, The IGA undertakes to destroy, erase or otherwise put this data beyond use.

8. Be managed and stored in such a manner that, in the event a data subject submits a valid Subject Access Request seeking a copy of their personal data, this data can be readily retrieved and provided to them

The IGA has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

A person is able to request a copy of the data retained on them through our 'Contact Us' page on the website or by directly emailing The IGA at secretary@iga.ie and/or the DPO at dpo@iga.ie; the DPO will be made aware of all requests for personal data.

6.3. Data Subject Access Requests

As part of the day-to-day operation of the organisation, The IGA's staff engages in active and regular exchanges of information with data subjects. Where a valid, formal request is submitted by a data subject in relation to the personal data held by The IGA which relates to them, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which The IGA must respond to the data subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

The IGA's staff will ensure that such requests are forwarded to the DPO in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 calendar days from receipt of the request. If you wish to make a complaint or have concerns regarding the handling of your Subject Access Request, please follow our designated complaints procedure outlined in our Complaints Policy.

Every Data Subject has the right to know, from the Data Controller:

- Who processed their personal data where, when and how;
- Why such data was processed;
- For how long such data was processed;
- The recipients of the personal data;
- Where applicable, the logic involved in automatic processing, including profiling and the consequences of such processing.

6.4. Implementation

As a data controller, The IGA ensures that any entity which processes personal data on its behalf (a data processor) does so in a manner compliant with the Data Protection legislation through a formal Data Processor Agreement.

Regular audit trail monitoring will be done by the DPO to ensure compliance with this Agreement by any third-party entity which processes personal data on behalf of The IGA.

Failure of a data processor to manage The IGA's data in a compliant manner will be viewed as a breach of contract. An assessment of the nature and scale of the breach will be conducted and appropriate action shall be taken, including, but not limited to, dismissal of the data processor, pursuit of legal actions and reporting to the Data Protection Authority.

Failure of The IGA's staff to process personal data in compliance with this policy may result in disciplinary proceedings, the nature of which is to be determined after assessment.

6.5. Data Breach

In the event of a data breach occurring, The IGA will review the nature of the breach and begin compiling a report utilising the Data Breach Form, see Appendix 2. The IGA will review the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place, and whether the personal data of vulnerable individuals has been exposed.

The IGA shall ensure that all passwords and accesses are secured and shall complete a full assessment of accesses and retained data to ensure that they are resecured. The IGA will continue to monitor any breached information to ensure that no further unexpected accesses have been granted and that the data is properly secured.

The extent and nature of the data exposed shall be assessed and determined as to what impact the breach could potentially have on individuals whose data has been exposed, making use of the following levels:

- 🟢 **Low Risk:** The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
- 🟠 **Medium Risk:** The breach may have an impact on individuals, but the impact is unlikely to be substantial.
- 🔴 **High Risk:** The breach may have a considerable impact on affected individuals.
- 🔴 **Severe Risk:** The breach may have a critical, extensive or dangerous impact on affected individuals.

Regardless of risk level, The IGA will inform the affected individuals and will provide an update as to the nature of the breach and the actions taken to ensure the security of the information.

Where a breach is likely to result in a high or severe risk to the affected individuals, The IGA will inform those individuals without undue delay and will report the breach to the Data Protection within 72 hours of becoming aware of the breach.

The IGA will take all necessary steps to ensure that the cause of the breach does not reoccur, including, but not limited to, additional training, increased security, and revising all access levels.

Appendix 1: Data Classification Matrix

	Public	Internal	Confidential	Restricted
Risk Level	**No risk**	**Low**	**Medium**	**High/Severe**
Description	Data that is freely available and accessible to the general public. This type of data can include government publications, open access research papers, census data, and other freely available datasets.	Data that is generated and owned by an organization or its employees. This may include sales figures, customer data, financial records, and other sensitive information that is not intended for public consumption.	Data that is strictly protected and only accessible to authorized individuals. This may include PII, trade secrets, financial information, or any information that could cause harm if compromised.	Data that is highly sensitive and should only be accessed by authorized personnel on a need-to-know basis. It includes data that, if compromised, could cause significant harm to an organization or individuals.
Access Rights	No restrictions or access controls, available to anyone.	Limited access to certain individuals or groups within The IGA.	Access only granted to those with a legitimate need to know, such as authorized Exec members or contractors.	Highly sensitive data with strict access controls, available only to a select few Exec members or Directors.
Impact	A breach of public data will not harm individuals or The IGA.	The publication of this data may cause some inconvenience.	In the event that this information falls into the wrong hands, the	The impact of this data being revealed to the public can be devastating to The

	Public	Internal	Confidential	Restricted
Risk Level	**No risk**	**Low**	**Medium**	**High/Severe**
			consequences may result in losses that are not deemed crucial to The IGA.	IGA, IGA members and possibly its customers.
Examples	● Government publications and reports ● Court records and judgments ● Press releases and news articles ● Company annual reports ● Social media posts and profiles that are set to public ● Publicly available financial statements of companies	● Executive records ● Financial data ● Operational data ● Intellectual property ● Marketing data ● Legal documents ● IT infrastructure and network information ● Administrative data	● Financial data ● Legal documents ● Intellectual property ● Personal identifiable information ● Contract agreements	● Personal Public Service (PPS) ● Payment Information ● Passwords ● Financial Statements ● Trade Secrets ● Intellectual Property ● Personal Identifiable Information (PII) ● Confidential Legal Documents

	Public	Internal	Confidential	Restricted
Risk Level	**No risk**	**Low**	**Medium**	**High/Severe**
Storage Options	Can be stored on public servers or cloud storage systems that can be accessed by anyone with an internet connection.	Can be stored on internal servers or cloud storage systems that are accessible only to Exec within The IGA.	Should be stored on secure servers or cloud storage systems that are accessible only to authorized personnel.	Should be stored on highly secure servers or cloud storage systems that are accessible only to a select few individuals with strict access controls.
Additional Security Considerations	No security measures are required to access public data. However, it should be protected against unauthorized modification and deletion. For example, backups and logs should be maintained to provide data integrity and availability.	In addition to access controls, monitoring, logging, and encryption, should be implemented to protect internal data.	In addition to access controls, data loss prevention software and encryption should be implemented to protect confidential data from unauthorized use, storage, modification, and disclosure.	Restricted data is protected by additional layers of security, including multi-factor authentication, encryption, monitoring, and specialized access controls. Data should be stored on a server with high-level security and restricted to a small group of senior Exec.

	Public	Internal	Confidential	Restricted
Risk Level	**No risk**	**Low**	**Medium**	**High/Severe**
Audit Controls	No audit controls required.	It may be necessary to conduct some form of monitoring or review.	The task of monitoring and evaluating the system for misuse is assigned to data stewards. They must report any anomalous activities to their superiors based on the severity of the incident.	The duty of data stewards involves monitoring and evaluating the system for any possible instances of misuse or unauthorized entry. To address any issues promptly, a contingency plan must be in place.
Retention Period	Indefinitely.	IGA generated information pertaining to The IGA operational processes shall be retained indefinitely. Names of Directors and Executive members shall be retained indefinitely. Records of games submitted to Gaelcon, including the writer's name, shall be retained indefinitely	IGA generated information pertaining to The IGA operational processes shall be retained indefinitely. Records of information related to Gaelcon shall be retained for a period of 5 years following the event unless GDPR approval was provided to further retain provided information in	IGA generated information pertaining to The IGA operational processes shall be retained indefinitely. Purchase records shall be retained for a period of 5 years from date of purchase. Information related to IGA members shall be retained

	Public	Internal	Confidential	Restricted
Risk Level	**No risk**	**Low**	**Medium**	**High/Severe**
		for IGA records unless otherwise requested by the writer.	keeping with our Data Protection Policy. Information on Charity auctions shall be retained indefinitely; this information will not include personal or payment details related to the individual making the pledge.	for 3 years from point of cessation of membership. Records of information on the Directors and Executive members, not including names, shall be maintained with the same approach as membership records.

Appendix 2: Data Breach Form

Data Breach Form

Date & Time Occurred	
Date & Time Notified	
IGA Member Notified	

Nature of the Breach

Describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

Contact Details

Communicate the name and contact details of the data protection officer (DPO) or other contact point where more information can be obtained.

DPO	
Name	Isabella Storey-Cosgrave
Email	hellsbella15@gmail.com

Contact Point	
Name	
Email	

Likely Consequences

Consequences could include financial loss, reputational damage, legal implications and actions, targeting due to loss of sensitive personal data.

Measures Taken

Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Conclusion

Final Result of the Breach and any other Outcomes