GDPR Handbook

community games
endless possibilities

RCN: 20017057

TABLE OF CONTENTS

DATA PROTECTION POLICY

INTRODUCTION

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Community Games. This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the General Data Protection Regulation (GDPR) 2018, the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).

PURPOSE

Community Games must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by Community Games in relation to its staff, service providers and volunteers in the course of its activities. Community Games makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

SCOPE

The policy covers both personal and sensitive personal data held in relation to data subjects by Community Games. The policy applies equally to personal data held in manual and automated form.

Community Games as a Data Controller

In the course of its daily organisational activities, Community Games acquires, processes and stores personal data in relation to:

- Employees of Community Games
- Volunteers and Participants of Community Games
- Third party service providers engaged by Community Games

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, Community Games is committed to ensuring that its 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 Data Protection Officer is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by Community Games, there is regular and active exchange of personal data between Community Games and its Data Subjects.

In addition, Community Games exchanges personal data with Data Processors on the Data Subjects' behalf.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a Community Games staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed as soon as possible.

It is intended that by complying with these guidelines, Community Games will adhere to best practice regarding the applicable Data Protection legislation. Subject Access Requests forms can be found by emailing dataprotection@communitygames.ie

The Data Protection Principles

The following key principles are enshrined in the Irish legislation and are fundamental to the Community Games' Data Protection policy.

In its capacity as Data Controller, Community Games 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 and via our Privacy Statement, be made aware of:

- The identity of the Data Controller (Community Games)
- 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.

Community Games 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, Community Games will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Processing of the personal data will be carried out only as part of Community Games' lawful activities, and Community Games 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 Community Games and operating on its behalf.

2. BE OBTAINED ONLY FOR ONE OR MORE SPECIFIED, LEGITIMATE PURPOSES.

Community Games 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 Community Games holds their data, and Community Games 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 Community Games will be compatible with the purposes for which the data was acquired.

4. BE KEPT SAFE AND SECURE

Community Games will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Community Games 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.

5. BE KEPT ACCURATE, COMPLETE AND UP-TO-DATE WHERE NECESSARY.

Community Games 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. Community Games conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every year.

- conduct regular assessments in order to establish 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.

Community Games 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).

Once the respective retention period has elapsed, Community Games 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.

Community Games 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.

Data Subject Requests

As part of the day-to-day operation of the organisation, Community Games' staff engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by Community Games, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which Community Games must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the Subject Access Request Document which is available by emailing dataprotection@communitygames.ie

Community Games' staff will ensure that, where necessary, such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more one month from receipt of the request.

Implementation

As a Data Controller, Community Games 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.

Failure of a Data Processor to manage Community Games' data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of Community Games' staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

DATA BREACH POLICY

Introduction

Community Games collects, holds, processes and shares large amounts of personal data, a valuable asset that needs to be suitably protected. When it comes to the protection of personal data throughout Community Games, our end goal should be compliance and in doing so, adhering to best practice when it comes to securing the personal data of both our employees and client base. Therefore, every care is taken to protect personal data and to avoid a data protection breach. However, in such circumstances, it is vital that immediate action is taken to contain and remedy the breach.

The Data Protection Officer (DPO) is legally required to notify the Office of the Data Protection Commissioner of any personal data breach **within 72 hours** of becoming aware of this, consequently it is essential that immediate action is taken by Community Games when a breach has occurred or is likely to occur. Individuals affected by the personal data breach must also be notified promptly.

Following the containment and remedy stage, steps must be taken to assess and determine the cause of the breach to ensure processes are reviewed and risk is minimised going forward.

This Data Breach Management Procedure (the Procedure) provides guidance for employees of Community Games on how a Personal Data Breach should be handled and is intended for internal use.

It places obligations on employees, Management Committee, Board of Directors, contractors and Volunteers to report actual or suspected personal data breaches and sets out the steps to be followed by Community Games for managing and recording actual or suspected breaches. The Procedure applies to all personal data held and processed by Community Games regardless of format.

1. Scope

1.1 The aim of this Procedure is to standardise the response to all reported data breach incidents and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

1.2 By adopting a standardised, consistent approach to all reported incidents it aims to ensure that:

1.2.1. Immediate action is taken;

1.2.2 incidents are handled by appropriately authorised and skilled personnel;

1.2.3 incidents are recorded and documented;

1.2.4 the impact of the incidents is understood, and action is taken to prevent further damage:

1.2.5 external bodies or Data Subjects (defined below) are informed as required;

1.2.6 incidents are dealt with in a timely manner and normal operations restored;

1.2.7 evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny; and

1.2.8 incidents are reviewed to identify improvements in policies and procedures.

1.3 The following terminology is used in this Procedure:

Term	Meaning
Data Protection Officer or DPO	The person appointed by Community Games who is involved in all aspects of the development and implementation of our data protection and data privacy strategy and compliance with the GDPR and other applicable laws.
Data Subject	The individual to whom the personal data relates.
GDPR	The General Data Protection Regulation. (Regulation EU 2016/679)
Personal Data	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 a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (GDPR Article 4s1)

Personal Data Breach	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. (GDPR Art 4s12)
Special Category Data	Personal Data which reveals an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information for the purpose of uniquely identifying a natural person, and data concerning an individual's health, sex life or sexual orientation. (GDPR Art 9s1)

1. What is a Personal Data Breach?

1.1 A Personal Data Breach causes, or has the potential to cause, damage to Community Games information assets, its reputation or to a Data Subject. A personal data breach may be recent, or historical and only just discovered.

1.2 Examples of a Personal Data Breach include but are not restricted to, the following:

1.2.1 loss or theft of Personal Data or equipment on which Personal Data is stored (e.g. loss of mobile phone, laptop, USB pen, iPad/tablet device, hard copy file or paper record);

1.2.2 alteration of personal data without permission or authorisation;

1.2.3 unauthorised disclosure of Personal Data;

1.2.4 sending Personal Data to the wrong recipient;

1.2.5 attempts (failed or successful) to gain unauthorised access to information or IT systems;

1.2.6 loss of availability of Personal Data (e.g. hacking attacks);

1.2.7 'blagging' offences where information is obtained by deceiving the organisation who holds it;

1.2.8 human error;

1.2.9 an identified vulnerability or weakness which may lead to a Personal Data breach;

1.2.10 improper disposal of data;

1.2.11 personal data left unsecured in accessible areas.

3. Who is responsible under this Procedure?

3.1 All users including but not limited to employees, Management Committee, Board of Directors, contractors, third party suppliers or vendors, and volunteers employed or otherwise engaged at Community Games must report any actual, suspected, threatened or potential Personal Data Breach and assist with investigations as required, particularly if urgent action is required to prevent further damage.

3.2 The DPO must ensure that all users including employees, members of the Management Committee and Board of Directors, contractors and volunteers comply with this Procedure, assist with investigations and implement improvement measures. The DPO is responsible for managing a Personal Data Breach in accordance with this Procedure and will be the point of contact with the Office of the Data Protection Commissioner. Contact details for the DPO are as follows:

Sinead Colleran DPO

20 Inish Carraig House

Golden Island

Athlone. County Westmeath

Contact No: 090 6433388

Email dataprotection@communitygames.ie

Reporting a Personal Data Breach

4.1 Anyone discovering an actual, suspected, threatened or potential Personal Data Breach must report it immediately to the DPO as the primary point of contact using the Data Breach Report Form set out in Appendix 1 (where possible) followed up immediately by a phone call to **090 6433388**.

4.2 Any actual, suspected, threatened or potential Personal Data Breach discovered outside of normal working hours must be reported by calling the DPO on **086 0264974.**

4.3 The report to the DPO should include full and accurate details of the incident including who is reporting the incident and what Personal Data is involved.

4.4 When a data breach has been reported to the DPO, the incident will be logged on a central system to facilitate effective management of the breach and to aid reporting.

4.5 All employees should be aware that any Personal Data Breach by them or any failure to report a Personal Data Breach in accordance with this paragraph 4 may result in the matter being considered under the relevant disciplinary procedure.

5. Dealing with a Personal Data Breach

5.1 There is no single method of response to a Personal Data Breach. Incidents must be dealt with on a case by case basis.

5.2 Evaluate the severity of the Personal Data Breach

5.2.1 Once a Personal Data Breach has been reported to the **DPO**, an initial assessment will be carried out by the **DPO** to establish the severity of the incident.

5.2.2 The DPO will evaluate the severity of the Personal Data Breach by considering the following factors:

(a) the impact to the individuals concerned

- this is the overriding consideration in deciding whether a Personal Data Breach should be reported to the Office of the Data Protection Commissioner.
- impact includes emotional distress as well as both physical and financial damage. It can include:
    - exposure to identity theft through the release of non-public identifiers, e.g. passport number
    - information about the private aspects of a person's life becoming known to others, e.g. health or medical conditions.

(b) the sensitivity of the Personal Data

- there should be a presumption to report to the Office of the Data Protection Commissioner where smaller amounts of Personal Data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.
- this is most likely to be the case where the Personal Data Breach involves Special Category Personal Data. If the information is particularly sensitive, even a single record could trigger a report.

(c) the volume of Personal Data involved

- there should be a presumption to report to the Office of the Data Protection Commissioner where:
    - a large volume of personal data is concerned, and
    - there is a real risk of individuals suffering some harm.
- it will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.

(d) **the number of individuals concerned**.

(e) the potential media interest.

(f) the impact on Community Games.

5.2.3 Specific consideration will be given to whether Data Subjects will suffer any discrimination, identity fraud, financial loss, reputational damage, loss of confidentiality and economic or social disadvantage, as a result of the Personal Data Breach.

5.3 Containment and Recovery

5.3.1 The **Controller**, supported by the **DPO**, will take appropriate steps as necessary to contain the Personal Data Breach and recover the Personal Data as quickly as possible. Such steps will include (but are not limited to):

(a) immediately contain the Personal Data Breach (if this has not already occurred). Corrective action may include retrieval or recovery of the Personal Data, ceasing unauthorised access, shutting down or isolating the affected system;

(b) where the Personal Data Breach relates to a managed ICT system, notify senior ICT manager immediately (as required);

(c) contact relevant staff to advise of precautionary measures where a risk remains live (as required);

(d) attempt to retrieve misdirected emails and contact recipients to instruct them to delete and destroy the material sent to them in error;

(e) ensure that any codes or passwords are changed where the information has been compromised and that users are notified;

(f) assess the availability of back-ups where Personal Data is damaged/lost/stolen;

(g) whether there are wider consequences to the Personal Data Breach.

5.4 Notifications/Communications

Notification to the Office of the Data Protection Commissioner

5.4.1 The DPO and the Controller will establish whether the Personal Data Breach needs to be reported to the Office of the Data Protection Commissioner. Where the decision is taken to notify the Office of the Data Protection Commissioner, the DPO will report the Personal Data Breach

within 72 hours of the Personal Data Breach being initially discovered.

5.4.2 A decision to report or not to report the Personal Data Breach will be based on an assessment of the severity of the Personal Data Breach and any potential risk to the rights and freedoms of the Data Subjects.

5.4.3 Where a Personal Data Breach is reported to the Office of the Data Protection Commissioner, the following information **must be** included within the report:

(a) a description of the Personal Data Breach;

(b) the categories and approximate number of individuals concerned;

(c) the categories and approximate number of Personal Data records concerned;

(d) the name and contact details of the DPO and where more information can be obtained;

(e) description of the likely consequences of the Personal Data breach; and

(f) a description of the measures taken, or proposed to be taken, to deal with the Personal Data Breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

5.4.4 The Office of the Data Protection Commissioner contact details are available at: www.dataprotection.ie

Notification to Data Subjects

5.4.5 The Controller and the DPO will consider the need to notify the Data Subjects. This decision will be based on the risk to the rights and freedoms of Data Subjects. The DPO will notify the affected Data Subject(s) without undue delay in clear and plain language including:

(a) full details of the Personal Data Breach including a description of the Personal Data affected;

(b) the likely consequences of the Personal Data Breach;

(c) the measures we have or intend to take to address the Personal Data Breach, including, where appropriate, recommendations for mitigating potential adverse effects; and the name and contact details of the DPO

(d) When determining whether and how to notify Data Subjects of the Personal Data Breach, Community Games will co-operate closely with the Office of the Data Protection Commissioner and other relevant authorities, e.g. An Garda Siochána; and take account of the factors set out in **Appendix 2**.

Notification to An Garda Síochána

5.4.6 Community Games will consider the need to contact the Gardai for the purpose of containment and recovery. In addition, where it transpires that the Personal Data Breach arose from a criminal act perpetrated against Community Games, the Controller will notify the Gardai and/or relevant law enforcement authorities.

Notifying Other Parties

5.4.7 Community Games will consider whether there are any legal or contractual requirements to notify any other parties.

5.5 Evaluation and Response

5.5.1 Once the incident is contained, the Controller and DPO will lead a full review of:

(a) the cause(s) of the Personal Data Breach;

(b) the effectiveness of the response(s); and

(c) whether any changes to the systems, policies and procedures should be undertaken.

5.5.2 All employees, members of Management Committee, Board of Directors, contractors or volunteers employed or otherwise engaged at Community Games will be required to comply in full and promptly with any investigation.

5.5.3 An audit will be led by the DPO within 6 months from the date of report to ensure that recommendations have been implemented.

APPENDIX 1

Data Breach Report Form	
Time and Date Personal Data Breach was identified **(Also, time and date breach occurred if different to when identified)**	
Who is reporting the breach: Name/Post/Dept	
Contact details: **Telephone/Email**	
Description of the Personal Data Breach:	
Volume of Personal Data involved, and number of individuals affected	
Is the breach confirmed/suspected/ possible/threatened?	
Is the breach contained or ongoing?	
What actions are being taken **to stop the breach and/or recover the data?**	
Who has been informed of the breach?	
Any other relevant information	

Email form to: dataprotection@communitygames.ie

Received by:	
Date/Time:	

APPENDIX 2

FACTORS AFFECTING IF AND HOW TO NOTIFY DATA SUBJECTS OF A PERSONAL DATA BREACH

Factor	Impact on obligation to notify data subject
Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether it would involve disproportionate effort to notify the data subject(s).	If so, it is not necessary to notify the data subject(s)—but we must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject(s) in any event.

PRIVACY STATEMENT

Introduction

Community Games is committed to protecting and respecting your privacy. We wish to be transparent on how we process your data and show you that we are accountable with the GDPR in relation to not only processing your data but ensuring you understand your rights.

It is the intention of this privacy statement to explain to you the information practices of Community Games in relation to the information we collect about you.

For the purposes of the GDPR the data controller is:

- Community Games
- Contact details of Community Games: Community Games, 20 Inish Carraig House, Golden Island, Athlone. www.communitygames.ie | dataprotection@communitygames.ie | 0906433388
- When we refer to 'we' it is Community Games

Please read this Statement carefully as this sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us.

Who are we?

Community Games was founded in 1967 to provide young people with the means and the opportunity to utilise their leisure time in a healthy and productive manner through friendly competition.

The organisation is child-centred and the focus is on participation rather than winning. Children compete in friendly rivalry, in a fun and healthy way. In order to qualify for the National Festivals individual participants must first compete at an area, then at County and sometimes at Provincial level.

It is an independent voluntary organisation, operating in local communities throughout Ireland. The organisation aims to provide opportunities for children and young people aged 6-16 years to develop active healthy lives in a safe environment through experiencing a wide range of sporting and cultural activities. Community spirit and co-operation is fostered and encouraged.

The organisation believes that every young person should have the opportunity to take part in sports and art in their local community and grow up understanding how good it makes you feel when you are leading an active lifestyle in your community.

Our Data Protection Officer can be contacted directly here:

- Sinead Colleran – 090 6433388
- dataprotection@communitygames.ie

Purpose for processing your data - why are we processing your data? Our legal basis.

- In order for Community Games to administer its wide range of events, both children and volunteer's details are entered into an Online Registration System. This is a legitimate basis for processing your data. Data includes: Name, Address, Phone Number, Email Address, Date of Birth (for volunteers this is necessary for Garda Vetting – for participants this is to establish age for panel entries).
- For Child Protection all our volunteers are Garda Vetted before being recruited to Community Games. In this regard, the Garda Vetting status of our volunteers ie: Pending, Accepted or Expired is shared with Area/County Children's Officers and Secretaries.
- Contact details for all our volunteers is required (for our under 18 volunteers - parental/guardian consent is required and their contact details) to comply with all our obligations ie: Charities Regulator, Children's First, Garda Vetting.
- Our volunteers are informed about events and changes to legislation via email, web and bulk text. Consent is acquired at the first stage of registration.

How will Community Games use the personal data it collects about me?

Community Games will process (collect, store and use) the information you provide in a manner compatible with the EU's General Data Protection Regulation (GDPR). We will endeavour to keep your information accurate and up-to-date and not keep it for longer than is necessary.

Special Categories of personal data

If for any reason in the future we need to collect any special categories of personal data (e.g. health, religious beliefs, racial, ethnic origin) – we will ensure the below:

- Your explicit consent will be obtained

Who are we sharing your data with?

Your personal data may be shared with a third-party service providers contracted to Community Games in the course of dealing with you. Any third parties that we may share your data with are obliged to keep your details securely, and to use them only to fulfil the service they provide on your behalf. When they no longer need your data to fulfil this service, they will dispose of the details in line with Community Games' procedures.

If we wish to pass your sensitive personal data onto a third party we will only do so once we have obtained your explicit consent, unless we are legally required to do otherwise.

If we transfer personal data to a third party or outside the EU we, as the data controller, will ensure the recipient (processor or another controller) has provided the appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for you the data subject are available.

Data Subjects Rights:

Community Games facilitate your rights in line with our data protection policy and the subject access request procedure. This is available on request or by visiting www.communitygames.ie/saf

Your rights as a data subject

At any point while we are in possession of or processing your personal data, you, the data subject, have the following rights:

- **Right of access** – you have the right to request a copy of the information that we hold about you.
- **Right of rectification** – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- **Right to be forgotten** – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- **Right to restriction of processing** – where certain conditions apply to have a right to restrict the processing.
- **Right to object** – you have the right to object to certain types of processing such as direct marketing.
- **Right to judicial review -** in the event that Community Games refuses your request under rights of access, we will provide you with a reason as to why.

All of the above requests will be forwarded on should there be a third party involved, as indicated, in the processing of your personal data.

Retention of your personal data

Data will not be held for longer than is necessary for the purpose(s) for which they were obtained. Community Games will process personal data in accordance with our retention schedule. This retention schedule has been approved by our internal governance.

Complaints

In the event that you wish to make a complaint about how your personal data is being processed by Community Games or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority (Data Protection Commission – Ireland) and Community Games Data Protection Officer.

ADDITIONAL PROCESSING

If we intend to further process your personal data for a purpose other than for which the data was collected, we will provide this information to you prior to processing this data.

CONTACT US

Your privacy is important to us. If you have any comments or questions regarding this statement, please contact us on 090 6433388, dataprotection@communitygames.ie, Community Games, 20 Inish Carraig House, Golden Island, Athlone, Co. Westmeath

PRIVACY STATEMENT CHANGES

Community Games may change this privacy policy from time to time. When such a change is made, we will post a revised version online. Changes will be effective from the point at which they are posted. It is your responsibility to review this privacy policy periodically so you're aware of any changes. By using our services you agree to this privacy policy.