Data Protection and Retention Policy

Irish Dodgeball Association

Version No: 1.2
Issue Date: May 2019

VERSION HISTORY

Version	Date Issued	Brief Summary of Change	Owner's Name
V1.0	11/12/2018	Initial Document	Ireland Dodgeball Association
V1.1	31/01/2019	Data owners added	Ireland Dodgeball Association
V1.2	07/05/2019	Organisation name changed	Irish Dodgeball Association

For more information on the status of this document, please contact:	Name: Tom Eastaway Tel: +353 86 0855704 E-mail: eastawat@tcd.ie
Date of Issue	07/05/2019

Issue date:	January 2019	**Review date:**	
Policy title:	**Data Protection and Retention Policy**		
Version:	1.1	**Issued by:**	Tom Eastaway – Data Protection Officer, Irish Dodgeball Association

Aim:	To outline the relevant controls and measures within the organisation, and to highlights safeguards where needed.
Scope:	

Associated documentation:	**Legal Framework:** General Data Protection Regulation 2018 **Policies:** Data Protection Statement
Appendices:	
Approved by:	Tamas Heitzmann, IDBA Chair
Date:	31/01/2019
Review and consultation process:	Policy to be reviewed annually. Reviews to be sanctioned by Irish Dodgeball Association committee.
Responsibility for Implementation:	Data Protection Officer

HISTORY

Revisions:		
Date:	**Author:**	**Description:**
31/01/2019	Tom Eastaway	Data owners added

Distribution methods:	Emailed to committee members upon completion. Copy published on Irish Dodgeball Association website.

Contents

1 Introduction

In its everyday operations the Irish Dodgeball Association (IDBA) collects and stores records of individuals involved with playing dodgeball in and for Ireland and the running of dodgeball events in Ireland and for the Irish national team abroad.

It is important that these records are protected from loss, destruction, falsification, unauthorised access and unauthorised release and a range of controls are used to ensure this, including backups, access control and encryption.

IDBA also has a responsibility to ensure that it complies with all relevant legal, regulatory and contractual requirements in the collection, storage, retrieval and destruction of records. Of particular relevance is the European Union General Data Protection Regulation (GDPR) and its requirements concerning the storage and processing of personal data.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to IDBA systems.

The following documents are relevant to this policy:

- *Data Protection Statement*

2 Records Protection and Retention Policy

This policy begins by establishing the main principles that must be adopted when considering record protection and retention. It then sets out the types of records held by IDBA and their general requirements before discussing record protection, destruction and management.

2.1 General Principles

There are a number of key general principles that must be adopted when considering record retention and protection policy. These are:

- Records must be held in compliance with all applicable legal, regulatory and contractual requirements
- Records must not be held for any longer than required
- The protection of records in terms of their confidentiality, integrity and availability must be in accordance with their security classification
- Records must remain retrievable in line with the organisation's requirements at all times
- Where appropriate, records containing personal data must be subject as soon as possible to techniques that prevent the identification of a living individual

2.2 Record Types and Guidelines

In order to assist with the definition of guidelines for record retention and protection, records held by IDBA are grouped into the categories listed in the table on the following page. For each of these categories, the required or recommended retention period and allowable storage media are also given, together with a reason for the recommendation or requirement, and the method of disposal where relevant.

Note that these are guidelines only and there may be specific circumstances where records need to be kept for a longer or shorter period of time. This should be decided on a case by case basis as part of the design of the information security elements of new or significantly changed processes and services.

Record Category	Description	Retention Period	Reason for Retention Period	Allowable Storage Media	Final Disposal	Owner
Player data	--	--	--	--	--	
Consent to store basic player and club data	Consent tag	Retain as long as consent is valid (as long as a player is affiliated with IDBA or an IDBA-affiliated club + up to 1 year)	To record individuals' consent to store data	Electronic only	Secure deletion of electronic records	IDBA Data Protection Officer
Player bio details	Player names, dates of birth	Retain as long as a player is affiliated with IDBA or an IDBA-affiliated club + up to 1 year	Used for eligibility for club competitions and registering players for competitions	Electronic only	Secure deletion of electronic records	IDBA Data Protection Officer
Player club affiliation records	History of player club affiliation	Retain as long as a player is affiliated with IDBA or an IDBA-affiliated club + up to 1 year	Used for eligibility for club competitions and registering players for competitions	Electronic only	Secure deletion of electronic records	IDBA Data Protection Officer
Consent to store international data	Consent tag	Retain as long as consent is valid (as long as a player is affiliated with IDBA or an IDBA-affiliated club + up to 1 year)	To record individuals' consent to store data	Electronic only	Secure deletion of electronic records	ROI Squad Manager
International selection history	History of attendance at international trials, history of appearances in competition, stats and notes on competitive international appearances, stats and notes on performance at trials	Retain indefinitely	Required to retain history of Irish teams in international competitions	Electronic only	Appropriate filing/archiving	ROI Squad Manager
International trials history	History of attendance at international trials, stats and notes on performance at trials	Retain up to one year after last trial attendance	Required for international squad selection	Electronic only	Secure deletion of electronic records	ROI Squad Manager
International eligibility records	Proven eligibility tag, proof of nationality/proof of address/proof of parent or grandparent nationality	Retain documentatary proofs only until they have been provided to international body (maximum 1 year). Retain tag that proof was	For players to be eligible in international competition, proof of	Electronic only	Secure deletion of electronic records	ROI Squad Manager

		provided as long as player is affiliated with IDBA or an IDBA-affiliated club + up to 1 year	eligibility must be provided to the competition's governing body			
Committee/ Officer/ Referee/ IDBA Assistant Data	--	--	--	--	--	
Consent to store data (non-players only)	Consent tag	Retain as long as individual is involved with IDBA activities + up to 1 year	To record individuals' consent to store data	Electronic only	Secure deletion of electronic records	IDBA Data Protection Officer
Contact data	Names and contact details for any committee members, officers, or non-players who assist with the running of IDBA or its activities		To contact individuals involved in the organising or running of IDBA activities	Electronic only	Secure deletion of electronic records	IDBA Data Protection Officer
IDBA Operational Data	--	--	--	--	--	
IDBA policies and procedures		Retain current until superseded		Electronic and paper copies	Appropriate filing/archiving	IDBA Data Protection Officer
Written complaints	Records received/created as a result of investigating complaints	Retain for 5 years after resolution of complaint or from date of last correspondence		Electronic or paper	Confidential shredding / secure deletion of electronic records	IDBA Data Protection Officer

Table 1 - Record types and retention periods

2.3 Use of Cryptography

Where appropriate to the classification of information and the storage medium, cryptographic techniques must be used to ensure the confidentiality and integrity of records.

Care must be taken to ensure that encryption keys used to encrypt records are securely stored for the life of the relevant records and comply with the organisation's Information Security Policy.

2.4 Media Selection

The choice of long term storage media must take into account the physical characteristics of the medium and the length of time it will be in use.

Where records are legally (or practically) required to be stored on paper, adequate precautions must be taken to ensure that environmental conditions remain suitable for the type of paper used. Where possible, backup copies of such records should be taken by methods such as scanning. Regular checks must be made to assess the rate of deterioration of the paper and action taken to preserve the records if required.

2.5 Record Retrieval

There is little point in retaining records if they are not able to be accessed in line with organisational or legal requirements. The choice and maintenance of record storage facilities must ensure that records can be retrieved in a usable format within an acceptable period of time. An appropriate balance should be struck between the cost of storage and the speed of retrieval so that the most likely circumstances are adequately catered for.

2.6 Record Destruction

Once records have reached the end of their life according to the defined policy, they must be securely destroyed in a manner that ensures that they can no longer be used. The destruction procedure must allow for the correct recording of the details of disposal which should be retained as evidence.

2.7 Record Review

The retention and storage of records must be subject to a regular review process carried out under the guidance of management to ensure that:

- The policy on records retention and protection remains valid
- Records are being retained according to the policy
- Records are being securely disposed of when no longer required
- Legal, regulatory and contractual requirements are being fulfilled
- Processes for record retrieval are meeting organisational requirements

The results of these reviews must be recorded.