FOOTBALL ASSOCIATION OF IRELAND

DATA PROTECTION POLICY

2018

TABLE OF CONTENTS

Associated policies available upon request from datamanager@fai.ie

Glossary of Terms

Data means information in any form which can be processed. It includes automated and manual data. Data includes but is not limited to a person's name, address, date of birth, email address, telephone number, photograph, qualifications, kit size, registrations, bank account number, credit card number and medical conditions.

Data Subject is an individual who is the subject of the Personal Data.

European Economic Area (EEA) includes the 28 EU countries and the 3 EFTA countries (Norway, Liechtenstein and Iceland). The 28 EU countries are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Republic of Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

Manual Data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Association.

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping data
- collecting, organising, storing, altering or adapting the data
- retrieving, consulting or using the data
- disclosing the information or data by transmitting, disseminating or otherwise making it available
- aligning, combining, blocking, erasing or destroying the data.

Special Categories of Data relates to specific categories of data which are defined as data relating to a person's racial or ethnic origin; political opinions or religious or philosophical beliefs; trade union membership; the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Stakeholders means all interested parties to include, but not limited to, employees, contractors, commercial partners, sponsors, affiliates and volunteers.

Introduction

This Data Protection Policy is underpinned by the intent of the Football Association of Ireland (FAI) to comply with its Data Protection requirements and best practice.

This Policy is a statement of our commitment to protect the rights and privacy of individuals in accordance with the General Data Protection Regulation and any associated implementing legislation in Ireland (together 'GDPR').

This policy supports the structure, which assists our compliance with the Data Protection legislation, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

Data Protection Commissioner

The role of the Data Protection Commissioner (DPC) is to ensure that organisations which use personal information, comply with the provisions of the GDPR. The DPC has a wide range of enforcement powers to assist in ensuring that the principles of data protection are being observed. These powers include the serving of legal notices compelling data controllers to provide information needed to assist in its enquiries, or compelling a data controller to implement one or more provisions of the GDPR.

The DPC may investigate complaints made by the general public or carry out investigations proactively. They may, for example, authorise officers to enter premises and to inspect the type of personal information being kept, how it is processed and the security measures in place. In such instances, the FAI and its employees must cooperate fully with such officers.

Depending on the breach, a data controller found guilty of an offence under the GDPR can be fined amounts up to the greater of €20,000,000 or 4% of total worldwide turnover, on conviction on indictment and/or may be ordered to delete all or part of a database.

For further information on the Data Protection Commissioner please refer to the Data Protection Commissioner website (www.dataprotection.ie).

Purposes for Holding Personal Information

In general, we will collect and use Personal Data (information) for a variety of purposes about employees, members, volunteers or other individuals who engage with FAI ('Stakeholders') and other individuals who come into contact with us.

We use personal information to provide us with information on products or services and to help us better understand the needs and interests of our Stakeholders. Specifically, we may use information to help complete a transaction or order, for communication purposes, the provision of a service and support, to update Stakeholders on programmes services and

benefits, to personalise promotional offers and to personalise FAI websites. Occasionally, we may also use Stakeholder information to contact Stakeholders for market research regarding our programmes, products or services. We give our Stakeholders the opportunity of choosing their privacy preferences regarding such communications and Stakeholders can amend these preferences at any stage by contacting us.

The types of personal information we hold may include name, postal address, date of birth, phone number, e-mail address, ethnicity, nationality, disability, photographs, billing and transaction information credit card information and contact preferences. Other personal information may also be held including Special Categories of Data.

It is evident therefore that the purpose of holding information is crucial to us running an effective service for our Stakeholders. We will only share personal information with third parties where there is a legal basis for doing so. In line with our obligations of data security, we will only share Personal Data across departments within the FAI where such transfer is necessary for the processing of the data in accordance with its purpose. Our Privacy statement is available from our website (www.fai.ie).

Legal Obligations of the Association and its Employees

Our employees receive training on Data Protection which equips them with the knowledge to carry out their roles in accordance with data protection requirements.

We administer our responsibilities under the legislation in accordance with the stated data protection principles outlined in the GDPR as follows:

1. **Process data lawfully, fairly and transparently***:*
   We will obtain and process Personal Data in a lawful, fair and transparent manner and ensure that data subjects are kept aware of what, how and why we process their data.

2. ***Purpose Limitation****:*
   We will keep data for purposes that are specific, legitimate and explicit and clearly stated and the data will only be processed in a manner compatible with these purposes.

3. ***Data Minimisation****:*
   No more information than is necessary for the purpose should be collected from the data subject. Personal Data held by us will be adequate, relevant and not excessive in relation to the purpose(s) for which it is kept.

4. ***Keep it safe and secure:***

We will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. We are aware that high standards of security are essential for all personal information.

5. ***Keep it accurate, complete and up-to-date****:*
   We will have procedures that are adequate to ensure high levels of data accuracy. We will examine the general requirement to keep Personal Data up-to-date. We will put in place appropriate procedures to assist employees in keeping data up-to-date.

6. **Storage Limitation**
   We will maintain Personal Data in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed.

Age of Consent

The Board of the FAI has set the age of consent at 18. We do not communicate with individual children directly unless an initial consent has been given by the child's parent/guardian. As much as possible, all communication with children is channelled through their parents/or guardians.

Access Requests under the GDPR

An access request must be made by the data subject to whom the request concerns and can not be made by one individual on behalf of another. Although we have set the age of consent at 18, in the case of access requests, a person aged 13 and over can request their own data. Where the individual is aged under 13 and makes an access request, it will be dealt with on a case by case basis. In certain cases, a letter of consent signed by the child's parent/guardian may be required in order to process a request.

Subject Access Requests should be made in accordance with our Subject Access Request Policy which is annexed hereto.

Other Rights of Our Stakeholders

In addition to the right of access, each Stakeholder has the following rights in relation to his or her Personal Data

- Right of access
- Right of rectification or erasure

- Right of restriction of processing
- Right of objection to processing
- Right to request the transfer of their Personal Data to a third party
- Right to withdraw consent
- Right to have name removed from a direct marketing list
- Right to complain to the Data Protection Commissioner
- Right to seek compensation through the Courts

Right of Access (as detailed in previous section)

Each Stakeholder is entitled to the personal information held on computer or in a manual filing system that facilitates access to information about him or her in accordance with our Subject Access Request Policy.

Right of rectification or erasure

Each Stakeholder has the right to have inaccurate information held about them corrected or rectified. In some circumstances, a Stakeholder may also have the information erased altogether from the database - for example, if the body keeping the information has no good reason to hold it (i.e. it is irrelevant or excessive for the purpose), or if the information has not been obtained fairly. A Stakeholder can exercise his or her right of rectification or erasure simply by writing to us.

Right of restriction/suspension to processing

A Stakeholder may request us to suspend the processing of their Personal Data in the following scenarios: (a) they want us to establish the data's accuracy; (b) where our use of the data is unlawful but we have not been requested to erase it; (c) where they need us to hold the data even if we no longer to enable them to establish, exercise or defend legal claims; or (d) they have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Right of objection to processing

A Stakeholder may object to certain processing where we rely on a legitimate interest (or those of a third party) and there is something about that particular situation which makes the Stakeholder want to object to the processing where they feel it impacts on their fundamental rights and freedoms. Unless we can demonstrate that we have compelling legitimate ground for the processing which outweighs the objection then the processing complained of will cease within 30 days of receipt of a written request to do so.

In addition, if we hold information for the purposes of direct marketing (such as direct mailing, or telephone marketing) each Stakeholder has the right to have his or her details removed from that database. The Stakeholder can exercise this right simply by writing to us. We must write back to the individual within 30 days confirming that we have dealt with the request. It is important that all employees do what is necessary to observe this timescale. Our online marketing materials will include an automated option for opting out of receipt of further marketing materials.

Right to request us to transfer Personal Data to a third party.

Upon request of a Stakeholder we will provide to the Stakeholder, or a third party they have chosen, their Personal Data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which the Stakeholder initially provided consent for us to use or where we used the information to perform a contract with the Stakeholder.

Right to withdraw consent

Where we are relying on consent to process Personal Data consent can be withdrawn at any time. However, this will not affect the lawfulness of any processing carried out before consent is withdrawn.

Right to complain to the Data Protection Commissioner

If a Stakeholder is having difficulty in exercising their rights, or should they feel that we are not complying with our responsibilities, then they may complain to the Data Protection Commissioner, who will investigate the matter on their behalf.

Right to seek compensation through the Courts

If a Stakeholder suffers damage through the mishandling of information about him or her, then he or she may be entitled to claim compensation through the Courts. Any such compensation claims are a matter for the Courts.

SHARING OF DATA

Provided there is a legitimate reason for doing so, we may have to share personal data with certain third parties such as

- Service providers based in EEA who provide IT and system administration services.

- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers based in Ireland who provide consultancy, payroll, banking, legal, insurance and accounting services.

- Revenue, governmental agencies, regulators, grant authorities and other authorities acting as processors or joint controllers based in Ireland who require reporting of processing activities in certain circumstances or to whom we are obliged to share information about our organisation and participation in it.

- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

We require all third parties to respect the security of the personal data we share with them and to treat it in accordance with the law. We do not allow our third-party service providers to use the personal data for their own purposes and only permit them to process the personal data for specified purposes and in accordance with our instructions.

Transfers Abroad of Data

In certain limited cases we transfer data abroad (for player registrations in certain competitions for example). We take adequate care when transferring Personal Data abroad. For international matches, information on fans travelling abroad (such as itinerary, accommodation) is provided to an Garda Síochána who then, if need be, forward the details to the police in the host country. This data is transferred for security purposes.

The European Union has recognised that Personal Data can flow from the 28 EU member states and 3 EEA member countries (Norway, Liechtenstein and Iceland) to certain third countries about which the European Union has made a finding of adequacy without any further safeguard being necessary. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection..

Transfers to countries other than those approved may be required from time to time and will only be done in accordance with the permitted exceptions or derogations.

Retention of Data

We do not store Personal Data either on computer or paper forms indefinitely. In general, Personal Data is retained in accordance with the periods set out in our Retention and

Destruction Schedule. We generally dispose of Personal Data either by shredding, permanent deletion or anonymisation.

Marketing and Communicating with Stakeholders

Our core activities are to promote, foster and develop the sport within Ireland. We are not primarily involved in marketing or promotional activities. We do however observe data protection requirements in accordance with legislation when processing Personal Data and engaging with Stakeholders. For instance, we do not distribute or sell the personal details of Stakeholders to third parties. Equally, we do not send unsolicited direct marketing material. Furthermore, we endeavour to send information to named persons and not to unnamed persons to avoid any unsolicited mail. All marketing communications include details of how to opt out of future communications.

Clarification

If you are unsure or unclear of anything relating to the Data Protection Policy of the FAI, please contact datamanager@fai.ie

You may also find the Data Protection Commissioner website a useful resource (www.dataprotection.ie).

Policy Review

This Policy will be reviewed regularly in light of any legislative or other relevant indicators.