

DATA PROTECTION AND PRIVACY NOTICE

INTRODUCTION

This is your guide to how personal data is managed by FENCING IRELAND. Data privacy is taken very seriously at FENCING IRELAND. It is important that you know exactly what we do with the personal information you and others provide to us, why we gather it and what it means to you.

SERVICES OF FENCING IRELAND

FENCING IRELAND is the national governing body for the sport of Olympic fencing in Ireland. We organise the sport in Ireland, which involves running competitions, licencing clubs and members, seeking new participants for fencing, and promoting the sport via all types of media. FENCING IRELAND is a member of the Fédération Internationale d'Escrime / International Fencing Federation, the World Governing Body for fencing, www.fie.org and the European Fencing Confederation www.eurofencing.info

OUR DATA PROTECTION POLICY

This document outlines our approach to Data Privacy to fulfil our obligations under the General Data Protection Act (2018) and General Data Protection Regulation (EU) 2016/679).

We want you to know the following:

1. Who we are
2. The information we collect about you
3. When and how we collect information about you
4. How we use your information*
5. With whom do we share your information
6. Implications of not providing information
7. The legal basis for using your information
8. Processing your information outside the EEA
9. Exercising your information rights (including the right to object)
10. How to contact us
11. Changes to this notice

*This notice applies to all our products and services. If you have any questions about how your information is gathered, stored, shared or used, please contact FENCING IRELAND.

1. Who we are

Throughout this document, “we”, “us”, “our” and “ours” refer to FENCING IRELAND, Sport Ireland HQ, Sport Ireland Campus, Snugborough Road, Blanchardstown, Dublin 20.

E: info@irishfencing.net

2. The information we collect about you

There are a number of reasons for gathering information about you. For instance, we need to know how to get in touch with you, we need to be certain of your identity if you are a member or guardian of a child or if you are acting for someone else. We need to understand some your financial circumstances if you are a member of guardian. The information we collect falls into various categories.

Identity & contact information

Name, contact details, email address, work and/ or personal phone numbers. We may also be required under law to seek proofs of identity such as copies of passports, utility bills, etc.

Financial details/circumstances

Financial account details from those from whom we collect membership fees and other charges.

Information you provide us about others or others provide us about you

If you give us information about someone else (for example, information about a child, or club member), or someone gives us information about you, we may add it to any personal information we already hold and we will use it in the ways described in this Data Protection and Privacy Notice.

Consent

Before you disclose information to us about another person, you must be sure that you have their agreement to do so or have the authority to do so. You need to ensure they confirm that they know you are sharing their personal information with us for the purposes described in this Data Protection and Privacy Notice.

Information for Which You Have Given Us Consent to Use and Process

This type of data may include:

1. Information which you have consented to us using by disclosing it to us.
2. Information which you have disclosed to us directly.
3. Your agreement to allow us contact you through certain channels to offer you relevant information and services.
4. Information from your online activities.
5. We collect information about your internet activity using technology known as cookies, which can often be controlled through internet browsers. For detailed information on the cookies we use and the purposes for which we use them, see our Cookie Policy, which is available on our website.
6. Other personal information
7. Telephone and image recordings.
8. Information in relation to data access, correction, restriction, deletion, porting requests and complaints.

Sometimes we may collect and use your information even though you are not a member of FENCING IRELAND

If we do so, we will apply the principles outlined in this Data Protection and Privacy Notice when dealing with your information.

3. When and how we collect information about you

As you join FENCING IRELAND, make enquiries and engage with us, information is gathered about you. We may also collect information about you from other people and other parties, for example, when you use the services of a club to register for a competition or other FENCING IRELAND activity or when you make a payment for a service offered by FENCING IRELAND, or when you like a FENCING IRELAND social media page.

When do we collect information about you?

1. When you use our website or social media page.
2. When you or others give us information verbally, over the telephone, or in writing. This information may be on application forms, file notes, correspondence or in records of your transactions with us or if you make a complaint to us.
3. When you use our services, we gather details about you.
4. Possibly from information publicly available about you – for example in business cards, correspondence, online forums, websites, or other social media.

4. How we use your information

Whether we are using it to confirm your identity, to help in the processing of your membership or some other service or to improve your experiences with us, your information is always handled with care and the principles outlined in this Data Protection and Privacy Notice are always applied.

We use your information:

1. To provide services to you, and to fulfil our contract with you.
2. To provide services to you and perform our contract with you, we use your information to:
 - a. Establish your eligibility for competitions and other services offered by us.
 - b. Manage and administer the processing of data necessary to perform services that we or our partners may offer to you.
 - c. Contact you by post, phone, text message, email, social media, fax, or other means, but not in a way contrary to your instructions to us or contrary to law.
 - d. Recover debts you may owe us.
 - e. Manage and respond to a complaint or appeal.
3. To manage our business for our legitimate interests.

To manage our business at FENCING IRELAND we may use your information to:

1. Collect and enforce debts and arrears.
2. Provide service information, to improve our service quality and for training purposes.
3. We may gather information about your interactions with us – for example, where you consent, we may gather information from your mobile phone or other electronic device you may use to interact with us.
4. Conduct marketing activities, for example, running promotions and direct marketing (provided that you have not objected to us using your details in this way), and research, including customer surveys, analytics and related activities.

To run our business on a day to day basis including to:

1. Carry out strategic planning and business management.
2. Compile and process your information for audit, statistical or research purposes (including, in some instances, making your

data anonymous) in order to help us understand trends in our members' behaviour and to understand our risks better, including for providing management information, operational and data risk management.

3. Protect our business, reputation, resources and equipment, to manage network and information security (for example, developing, testing and auditing our websites and other systems).
4. Dealing with accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services and prevent and detect fraud, dishonesty and other crimes (for example, to prevent someone trying to steal your identity).
5. Manage and administer our legal and compliance affairs, including complying with our obligations to conform to regulatory guidance and voluntary codes of practice to which we may have committed ourselves.
6. Enable our employees, servants or agents to share or access your information for internal administrative purposes, audit, prudential, statistical or research purposes (including making your data anonymous) to help us understand trends in customer behaviour, to help us to understand our risks better and for the purposes set out in this Data Protection and Privacy Notice (but not for the purposes of direct marketing where you have objected to this).
7. We may in the future wish to transfer or merge part or all of our business or assets or to buy a new business or the assets of another business or enter into a merger with another business. If so, we may disclose your personal information under strict duties of confidentiality to a potential buyer, transferee, merger partner or seller and their advisers, so long as they agree to keep it confidential and to use it only to consider the possible transaction. If the transaction goes ahead, the buyers, transferee or merger partner may use or disclose your personal information in the same way as set out in this Data Protection and Privacy Notice.
8. To comply with our legal and regulatory obligations
9. We need to use your information to comply with legal and regulatory obligations including:
 - a. Complying with financial services legislation.
 - b. Complying with your information rights.

- c. Providing you with statutory and regulatory information and statements.
- d. Establishing your identity,
- e. Complying with binding production orders or search warrants, and orders relating to requests for mutual legal assistance in criminal matters received from foreign law enforcement agencies/prosecutors.
- f. For other reasons where a statutory reason is given
- g. Complying with court orders arising in civil or criminal proceedings.
- h. Performing a task carried out in the public interest.

When you have given us permission (which you can withdraw at any time) we may:

- 1. Send electronic messages to you about service offers from us.
- 2. Use transaction history/account information from your FENCING IRELAND file to identify and inform you of services which may of interest to you or which are of a type in which you have expressed an interest to us.
- 3. Use cookies in accordance with our Cookie Policy.
- 4. Use special categories of data, or sensitive data
- 5. Use information you have made public and combine this with the activities outlined above.

When we ask for your consent, we will provide you with more information on how we will use your data in reliance on that consent, including in relation to third parties with which we would like your consent to share your data.

5. With whom do we share your information?

We are licenced under the FIE (www.fie.org) to govern Olympic fencing in Ireland in a smooth and seamless way. We only share your information with a select number of individuals and companies, and only as necessary. Please see APPENDIX I for a list (non-exhaustive) of data which is shared with others. Sharing can occur in the following circumstances and/or with the following persons:

- 1. Sellers, or purchasers, involved in organising and facilitating the completion of a FENCING IRELAND related transaction who will receive some of your personal data. This data will only be

shared as necessary for the timely completion of the transaction. The data shared will vary, as required, but it may be any of the following, typically your name, contact details, certain financial details, proof of personal identity, etc.

2. Your authorised representatives:
 - a. These include your attorney (under a Power of Attorney) and any other party authorised by you to receive your personal data.
 - b. Third parties we need to share your information with in order to facilitate our services to you.
3. We may disclose your information to our agents and third parties for administration, regulatory, member care and service purposes.
4. Your personal information remains protected when our service providers use it. We only permit service providers to use your information in accordance with our instructions, and we require that they have appropriate measures in place to protect your information.
5. Our service providers include (or may include), analytics companies, IT and telecommunication service providers, software development contractors, data processors, computer maintenance contractors, printing companies, archiving services suppliers, and consultants, including legal advisors.
6. Statutory and regulatory bodies (including central and local government) and law enforcement authorities.
7. These include the courts and those appointed by the courts, government departments, statutory and regulatory bodies in all jurisdictions where the FENCING IRELAND operates including (but not limited to):
 - a. The Data Protection Commission,
 - b. An Garda Síochána/police authorities/enforcement agencies in relevant jurisdictions,
 - c. Revenue Commissioners or similar tax authorities in relevant jurisdictions,
 - d. US authorities,
 - e. EU and other designated authorities.

6. Implications of not providing information

Sharing information with us is in both your interest and ours.

We need your information in order to:

1. Provide our services to you and fulfil our contract with you.
2. Manage our business for our legitimate interests.

3. Comply with our legal obligations.

Of course, you can choose not to share information, but doing so may limit the services we are able to provide to you.

We may not be able to provide you with certain services that you request. We may not be able to continue to provide you with or renew existing services. We may not be able to assess your suitability for a service, or, where relevant, give you a recommendation to provide you with another service.

When we request information, we will tell you if providing it is a contractual requirement or not, and whether or not we need it to comply with our legal obligations.

7. The legal basis for using your information

We will use your data and share that data when:

1. Its use is necessary in relation to a service or a contract that you have entered into or because you have asked for something to be done by us so you can enter into a contract with us.
2. Its use is in accordance with our legitimate interests outlined in this notice.
3. Its use is necessary because of a legal obligation that applies to us (except an obligation imposed by a contract).
4. You have consented or explicitly consented to the using of your data (including special categories of data) in a specific way.
5. Its use is necessary to protect your “vital interests”.
6. Where you have made public clearly sensitive categories of data about yourself.
7. Where the processing of special categories of data is necessary

8. Processing your information outside the EEA

Your information may be stored electronically on secure systems by providers of secure information storage or by FENCING IRELAND

We may transfer or allow the transfer of information about you and our products and services used by you to our service providers and other organisations outside the European Economic Area (EEA), but only if they agree to act solely on our instructions and protect your information to the same standard that applies in the EEA.

Those external organisations may process and store your personal information abroad and may disclose it to foreign authorities as required by law.

Using companies to process your information outside the EEA.

Some of our service providers, for example IT, telecommunication, and contractors may be based outside of the EEA. Where we authorise the processing / transfer of your personal information outside of the EEA, we require your personal information to be protected to at least Irish standards and include the following data protection transfer mechanisms:

1. Adherence to the EU/US Privacy Shield. You can find more information on the EU/US Privacy Shield at www.privacyshield.gov including a list of all organisations that have signed up to the EU/US Privacy Shield framework. Please contact us for further details on any transfers of personal information to entities in the US.
2. Use of contractual clauses which oblige such non-EEA companies to comply with GDPR

9. Exercising your information rights (including the right to object)

You have rights in relation to how we use your information. If you make your request electronically, we will, where possible, provide the relevant information electronically unless you ask us otherwise or it is more convenient to provide it in another format.

You have the right to:

1. Find out if we use your information, to access your information and to receive copies of the information we have about you.
2. Request that inaccurate information is corrected and incomplete information updated.
3. Object to particular uses of your personal data where the legal basis for our use of your data is our legitimate business interests (for example, profiling we may carry out for our legitimate business interests) or the performance of a task in the public interest. However, doing so may have an impact on the services we can / are willing or able to provide.
4. Object to use of your personal data for direct marketing purposes. If you object to this use, we will stop using your data for direct marketing purposes.

5. Have your data deleted or its use restricted – you have a right to this under certain circumstances. For example, when you withdraw consent you gave us previously and there is no other legal basis for us to retain it, or where you object to our use of your personal information for particular legitimate business interests.
6. Obtain a transferable copy of certain data, which can be transferred to another provider, known as “the right to data portability”.
7. This right applies where personal information is being processed based on consent or for performance of a contract and the processing is carried out by automated means. The right also permits the transfer of data directly to another provider where technically feasible. Therefore, depending on the technology involved, we may not be able to receive personal data transferred to us and we will not be responsible for the accuracy of same.
8. Withdraw consent at any time, if the processing is based on consent. If you withdraw your consent, it will not affect the lawfulness of processing based on your consent before its withdrawal.
9. We are obliged to respond in most instances, within 30 days. If we are unable to deal with your request within 30 day we have a duty to inform you of this within the 30 day limit, and we may extend this period by a further two calendar months. Should this occur, we will explain the reasons why the delay has occurred. If you make your request electronically, we will, where possible, provide the relevant information electronically unless you ask us otherwise.
10. You have the right to complain to the Data Protection Commission or another supervisory authority.
11. You can contact the Office of the Data Protection Commissioner at www.dataprotection.ie , info@dataprotection.ie , Data Protection Commission, Canal House, Station Road, Portarlinton, R32 AP23, Co. Laois.

10. How to contact us

FENCING IRELAND, Sport Ireland HQ, Sport Ireland Campus, Snugborough Road, Blanchardstown, Dublin 20.

E: info@irishfencing.net

11. Changes to this notice

We will update this Data Privacy Notice from time to time. Notice of any changes will be communicated to you and made available on this page and, where appropriate, notified to you e-mail.

Dated: 29.05.2020

SCHEDULE – Data Processing Activities

Category of data	Type of data subject	Purpose of processing	Legal basis for processing	Original source of data	Recipients of data	Retention period
Names	Member	Licence	Consent	Form	EFC/FIE	Two years after expiry of season
eMail	Member	Communications	Consent	Form	EFC/FIE	Two years after expiry of season
Addresses	Member	Communications	Consent	Form	EFC/FIE	Two years after expiry of season
Mobile phone	Member	Communications	Consent	Form	EFC/FIE	Two years after expiry of season
Date of Birth	Member	Eligibility for competitions	Consent	Form	EFC/FIE	Two years after expiry of season
Nationality	Member	Eligibility for competitions	Consent	Form	EFC/FIE	Two years after expiry

						of season
Club	Member	Identification	Consent	Form	EFC/FIE	Two years after expiry of season
Images	Member and /or general public attending a competition	Communications / Publicity	Consent	Photographic images and / or video images	General Public via Facebook	???

APPENDIX II DATA SECURITY AND HANDLING

Data security

1. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
2. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself. In addition, we will have appropriate written agreements in place with all of our data processors.
3. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:
 - a. **Confidentiality** means that only people who are authorised to use the data can access it.
 - b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
 - c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on a server instead of individual Personal Computers.
4. Our physical security procedures include:
 - a. Usernames and associated passwords to provide access
 - b. Deletion of data two years after a season has elapsed
5. Our computer-related, device-related and electronic-related security procedures include only granting access to our server to those people who need such access and who use secure password protection.