GYMNASTICS IRELAND

Data Protection Policy

Our Policy

Gymnastics Ireland ("GI") takes its data protection obligations very seriously and is committed to complying with the law.

The policy applies to all of our staff, members, clubs, volunteers, coaches and consultants ("**GI Community**" or **"you"** or **"your"**).

This Data Protection Policy ("**DP Policy**") is designed to:

i. give practical guidance on GI's approach to data protection law

ii. raise awareness amongst the GI Community about data protection law, including rights and responsibilities

iii. provide guidance on how to comply with those responsibilities

This DP Policy is a guidance document only. It is not a summary of the law or an exhaustive list of your data protection responsibilities.

GI's Approach to Data Protection Compliance

GI has appointed a dedicated Data Protection Liaison Officer ("DPLO") to oversee compliance with data protection laws for GI. GI is not required, under data protection law, to appoint a Data Protection Officer.

Each club should appoint a DPLO with responsibility for overseeing compliance with data protection laws within that club.

Any queries on data protection should be directed, in the first instance to your club DPLO. If the query cannot be resolved at club level, GI's DPLO can be contacted at ask@gymnasticsireland.com or by phoning 01 6251125.

GI has taken steps to ensure it is compliant with data protection law including;

i. Itemising it on the agenda for discussion/action at Board level including a commitment to the ongoing development of the GI membership system as the primary system/store for GI members data and developing this to be as practically functional for GI club administration as national member administration;
ii. Identifying and appointing a DPLO;
iii. Attending data protection-specific training workshops and seminars;
iv. Engaging experts regarding compliance and a project plan;
v. Creating an inventory of personal data, mapping out what personal data we hold and process and the justifications for doing so;
vi. Considering the direct member registration system and any related data protection obligations;
vii. Drafting policies
viii. Continuously monitoring our policies and our compliance with data protection law including refresher trainings where required

This DP Policy should be read in conjunction with existing policies and rules, including but not limited to the following:

- Member privacy policy
- Complaints and Disciplinary Rules
- Employee handbook
- Coaching policy
- Judging policy
- National Events policy
- Safeguarding policy
- Code of Ethics
- Garda Vetting
- International Travel/Selection policy
- Disability policy

1. Who is responsible for data protection?

1.1 During any given activity involving gymnastics and the GI Community, personal information may be collected, stored, viewed, archived, deleted, transferred, amended and so on. When we do this, we are processing personal data and we are required to do so in accordance with data protection law.

1.2 It is the responsibility of anybody involved in processing or controlling or using this personal data to do so in an appropriate and lawful manner.

1.3 Each person in the GI Community is potentially affected. It is your responsibility to make yourself aware of the DP Policy and implement it when processing personal data.

1.4 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

1.5 It is important that you notify the Data Protection Liaison or relevant person in your club of any potential breach involving you or anybody in the GI Community.

1.6 The Office of the Data Protection Commissioner ("DPC") is the statutory independent body responsible for enforcing data protection law in Ireland. The DPC has extensive powers, including the ability to impose civil fines of up to Euros 20 million or 4% of group worldwide turnover, whichever is higher. Also the data protection laws can be enforced in the courts and the courts have the power to award compensation to individuals.

2. Data protection laws

2.1 The General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 ("**DPA 2018**") (together "**data protection laws**"). In the aftermath of Brexit the UK will adopt laws equivalent to these data protection laws.

2.2 The data protection laws require that the personal data is processed in accordance with the Data Protection Principles (see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

3. Key Data Protection Principles

3.1 All personal data must be:

3.1.1 Processed fairly and lawfully and transparently

3.1.2 Processed for specified, lawful and compatible purposes

3.1.3 Adequate, relevant and not excessive to the purpose it was collected for

3.1.4 Accurate and up to date

3.1.5 Not kept longer than necessary

3.1.6 Processed and kept securely

3.2 See Schedule 1 below for further detail on these principles.

4. Key Phrases

4.1 **"Personal Data"** means data that relates to a living individual who can be identified from the data. It is limited to information about living people only. In the gymnastics context, this includes; athletes, coaches, judges, volunteers, parents, members, employees, contractors, suppliers etc… Personal data can include:

4.1.1 information held electronically or on paper or provided orally (phone recordings) or visually (e.g. CCTV).;

4.1.2 an expression of opinion about the individual e.g. records stored in the course of a coaching assessment or details regarding a participant's performance;

4.1.3 medical records, credit history, a recording of their actions, or contact details;

4.2 **"Sensitive Personal Data**" – means information containing facts or opinions about a living individual relating to: • Racial or ethnic origin • Political opinions • Religious beliefs • Trade Union Membership • Health • Sex life • Criminal proceedings or convictions

4.3 **Data subject** is the living individual to whom the relevant personal data relates.

4.4 **Processing** is widely defined under the data protection laws and can include for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

4.5 **Lawful basis for processing**

4.5.1 For personal data to be processed lawfully, we must be process it on one of the legal grounds set out in the data protection laws.

4.5.2 For the processing of ordinary personal data in our organisation these may include, among other things:

4.5.2.1 the data subject has given their consent to the processing;

4.5.2.2 the processing is necessary for the performance of a contract with the data subject;

4.5.2.3 the processing is necessary for the compliance with at legal obligation to which the data controller is subject; or

4.5.2.4 the processing is necessary for legitimate interest reasons of the data controller or a third party i.e. you are processing someone's personal data in ways they would reasonably expect it to be processed and which have a minimal privacy

impact on the data subject or where there is a compelling justification for the processing.

4.6 **Data controller** is the person who decides how personal data is used, for example we will always be a data controller in respect of personal data relating to our employees.

4.7 **Data processor** is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example an outsourced payroll provider will be a data processor.

4.8 **Data users** include employees or volunteers whose work involves using personal data. Data users have a duty to protect the information they handle by following this data protection policy at all times.

5. Your obligations – "Do's and Don'ts"

5.1 You should always try to apply a practical, logical and common-sense approach to how you use personal data, including the following steps where practical:

5.1.1 Do not take personal data out of the organisation's premises (unless necessary).

5.1.2 Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else.

5.1.3 Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc. and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

5.1.4 Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

5.1.5 If you are staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when you do not need to have them with you.

5.1.6 Where possible, encrypt laptops, mobile devices and removable storage devices containing personal data.

5.1.7 Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

5.1.8 Do password protect documents and databases containing personal data.

5.1.9 When disposing of personal data, ensure to shred it or dispose of it in a confidential manner.

5.1.10 Do not leave personal data lying around, store it securely.

5.1.11 When transferring personal data, especially sensitive data, to third parties consider whether you have a justifiable basis for doing so.

5.1.12 Do notify your DPLO immediately of any suspected security breaches or loss of personal data.

6. Consequences for non-compliance

6.1 There are a number of serious consequences for both yourself and us if we do not comply with data protection laws. These include:

6.1.1 For you:

6.1.1.1 **Disciplinary action:** If you are an employee, your terms and conditions of employment require you to comply with our policies. Failure to do so could lead to disciplinary action including dismissal. Where you are a volunteer, failure to comply with our policies could lead to termination of your volunteering position with us.

6.1.1.2 **Criminal sanctions:** Serious breaches could potentially result in criminal liability.

6.1.1.3 **Investigations and interviews**: Your actions could be investigated and you could be interviewed in relation to any non-compliance.

6.1.2 For GI or your club:

6.1.2.1 **Criminal sanctions:** Non-compliance could involve a criminal offence.

6.1.2.2 **Civil Fines:** These can be up to Euro 20 million or 4% of group worldwide turnover whichever is higher.

6.1.2.3 **Assessments, investigations and enforcement action**: We could be assessed or investigated by, and obliged to provide information to, the DPC.

6.1.2.4 **Court orders:** These may require us to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

6.1.2.5 **Claims for compensation:** Individuals may make claims for damage they have suffered as a result of our non-compliance.

6.1.2.6 **Reputational damage:** Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner quickly become public knowledge and might damage our brand. Court proceedings are public knowledge.

6.1.2.7 **Use of management time and resources:** Dealing with assessments, investigations, enforcement action, complaints, claims, etc. takes time and effort and can involve considerable cost.

7. Special category data

7.1 Special category data under the data protection laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data.

7.2 Under data protection laws this type of information is known as special category data and criminal records history becomes its own special category which is treated for some parts the same as special category data. Previously these types of personal

data were referred to as sensitive personal data and some people may continue to use this term.

7.3 To lawfully process special categories of personal data we must ensure that one of the following conditions has been met:

7.3.1 the individual has given their explicit consent to the processing;

7.3.2 the processing is necessary for the performance of our obligations under employment law;

7.3.3 the processing is necessary to protect the vital interests of the data subject. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;

7.3.4 the processing relates to information manifestly made public by the data subject;

7.3.5 the processing is necessary for the purpose of establishing exercising or defending legal claims; or

7.3.6 the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.

7.4 To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:

7.4.1 ensure that either the individual has given their explicit consent to the processing; or

7.4.2 ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

7.5 We would normally only expect to process special category personal data or criminal records history data usually in a Human Resources context and also in the context of our members/athletes/coaches/volunteers etc. in relation to areas such as Garda vetting, safeguarding & anti-doping.

8. Data subject rights

8.1 Under data protection laws individuals have certain rights in relation to their own personal data. In summary these are:

8.1.1 The rights to access their personal data, usually referred to as a subject access request;

8.1.2 The right to have their personal data rectified;

8.1.3 The right to have their personal data erased, usually referred to as the right to be forgotten;

8.1.4 The right to restrict processing of their personal data;

8.1.5 The right to object to receiving direct marketing materials;

8.1.6 The right to portability of their personal data;

8.1.7 The right to object to processing of their personal data; and

8.1.8 The right to not be subject to a decision made solely by automated data processing.

8.2 Not all of these rights are absolute rights, some are qualified and some only apply in specific circumstances. More details on these rights can be found in Schedule 2 of this Policy.