# GDPR FAQs

sportscotland
the national agency for sport

HM Harper Macleod LLP

# 1. Introduction

*This document sets out some of the most frequently asked questions from sports governing bodies (SGBs) regarding data protection. This should be read in conjunction with our guide "Data Protection for Sports Governing Bodies" and the **sport**scotland data protection templates available to SGBs.*

### 1.1 What is the GDPR

The General Data Protection Regulation (EU) 2016/679 (the GDPR) came into force across all EU Member States on 25 May 2018 and governs how organisations use personal data and increases the protection of individuals' privacy regarding their personal data.

### 1.2 Does it apply to Sports Governing Bodies?

Sports Governing Bodies (SGBs) are often "controllers" of personal data (including, name, address, date of birth, email address, qualification, eligibility, etc.) that they collect, store, share and delete (known as "processing" of personal data). The GDPR applies to any SGB, regardless of size.

### 1.3 Does the GDPR apply to ALL information held by SGBs?

The GDPR is mainly concerned with electronic personal data. However, if a SGB uses a paper filing system that allows information to be picked from specific criteria then the GDPR will apply to this paper filing system.

Most SBGs will use email and any personal data included in the emails will need to be processed in accordance with the provisions in the GDPR.

### 1.4 What is "special category personal data"?

This definition includes data revealing a person's racial or ethnic origin; health; sex life or sexual orientation; or religious or philosophical beliefs.

### 1.5 Do we need to appoint a Data Protection Offer?

Public authorities, organisations that have core activities requiring large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking) or organisations that have core activities consisting of large scale processing of special categories of personal data or personal data relating to criminal convictions and offences must appoint a Data Protection Officer under the GDPR.

Larger SGBs will need to consider if their processing activities will fall under this requirement and document their decision whether or not to appoint a Data Protection Officer. If a SGB does appoint a Data Protection Officer, they must comply with the statutory duties under the GDPR.

### 1.6 What is the difference between a controller and a processor?

A controller determines the purposes and means of processing, which essentially means that they decide how and why personal data is processed. A processor is anyone who only processes personal data on behalf of the controller (for example, to provide services to the controller).

The GDPR states that there must be a contract between a controller and processor – please refer to the **sport**scotland data processing templates to see what contractual provisions must be included in such contracts.

## 2. "Lawful" processing under the GDPR

Whenever SGBs process personal data, they must have identified a "lawful basis" for such processing. There are six lawful bases under the GDPR and SGBs need only identify one lawful basis for each processing activity, which will depend on the nature of the personal data, the relationship the SGB has with the indivdual and the purposes for the processing.

The six lawful bases under the GDPR are:

- where the individual has given their consent (in limited circumstances);
- the processing is necessary to perform a contract with the individual or take steps at the individual's request to enter into a contract with them;
- the processing is necessary to comply with a legal obligation;
- the processing is necessary to protect the vital interests of the individual or another person (emergency situations);
- the processing is necessary to perform a task in the public interest or to exercise the controller's official authority (primarily used by public bodies); or
- the processing is necessary for the controller's or a third party's legitimate interests, only where such interests are not overridden by the individual's interests.

Further, where SGBs process special category personal data they must have a lawful basis and meet at least one of the specified conditions for processing special category personal data. The template privacy notice includes some examples of these conditions but there are more available under the Data Protection Act 2018, if required.

Some of the most frequently asked questions relating to lawful processing are as follows:

### 2.1 Is consent required before we use any personal data?

No – as per the text above, consent is only one lawful basis under the GDPR for processing of personal data. Consent should only be used where:

- no other lawful basis applies;
- it is not required in order for the individual to access a service provided by the GDPR; and
- there is no imbalance of power between the SGB and the individual (for example, there is an imbalance of power between an employer and an employee).

Consent to process personal data requires a positive action from the individual. Pre-ticked boxes or any other method of default consent does not form valid consent. Consent statements should remain separate from other terms and conditions and SGBs should keep records to evidence consent.

Consent requests should include:

- the name of the SGB;
- the name of any third party relying on the consent;
- why the SGB wants the personal data;
- what the SGB will do with the personal data; and
- that individuals can withdraw their consent at any time.

The individual must be able to freely consent and not suffer detriment by not consenting. Using incentives to entice users to consent would potentially constitute a contradiction of freely given consent.

### 2.2 What is the lawful basis for processing employees' data?

SGBs will be able to rely on the "contract" lawful basis, as employees will have a contract of employment or the "legal obligation" lawful basis, to comply with employment law obligations.

### 2.3 What is the lawful basis for processing members' personal data?

When processing members' personal data (for example, membership admission or renewal) SGBs may be able to rely on the "contract" lawful basis as SGBs will need to use members' personal data to comply with the terms of their membership.

SGBs may also be legally required to process members' personal data for specific purposes under the "legal obligation" basis. This would apply to processing of members' personal data to comply with health and safety or company law requirements, as well as **sport**scotland's regulatory requirements.

### 2.4 What is required to rely on the "legitimate interests" lawful basis?

The application of the "legitimate interests" lawful basis requires SGBs to undertake a "legitimate interests assessment" by considering the following three-part test:

- **Purpose Test:** is the SGB pursing a legitimate interest?
  - For example, promotion of the SGB's objects, to encourage participation in sport, etc.
- **Necessity Test:** is the processing necessary for that purpose?
  - Will the processing actually help achieve the purpose?
  - Can the SGB achieve the same purpose without the processing?
  - Is the personal data particularly private?
  - Can the SGB achieve the same purpose by processing less personal data, or by processing the personal data in another more obvious or less intrusive way?
- **Balancing test:** do the individual's interests override the legitimate interest?
  - Will the individual reasonably expect the SGB to use their personal data in this way?
  - What will the potential impact on the individual be, will the processing cause them any harm or damage?

If any of these tests are not satisfied then SGBs will not be able to rely on the "legitimate interests" lawful basis. SGBs will need to keep a record of completed legitimate interests assessment for each processing activity under this lawful basis.

### 2.5 Does the posting of the competition results on a website require a lawful basis?

Yes, the publishing of results from competitions on a website constitutes the processing of personal data. The SGB may be able to rely on the "legitimate interests" lawful basis, provided the test set out above is assessed and met, or ask individuals for their consent.

If SGBs are relying on consent to publish the results, the relevant consent statement must include the information listed above and also make clear to the individual that the information will be published on a website and, therefore, will be in the public domain.

## 3. Privacy notices

Under the GDPR, individuals have a 'right to be informed' about how their personal data is being used by an organisation. SGBs are required to give individuals "privacy notices" upon the collection of personal data from an individual or within one month of receiving an individual's personal data from a third party. For example, the privacy notice should be included in applications for membership, membership renewal form and employment / volunteer forms.

### 3.1 What is a privacy notice?

A "privacy notice" is a statement by a controller explaining to individuals what they do with their personal data. Privacy notices must explain clearly what personal data is collected and what purpose it will to be used for. Privacy notices must be made available to all individuals for whom SGBs hold personal data.

### 3.2 What needs to be included in a privacy notice?

The GDPR sets out what information must be included in a privacy notice and further details can be found in our guide "Data Protection for Sports Governing Bodies".

The headings in the **sport**scotland template privacy notices set out the information required under the GDPR for inclusion in the privacy notice. However, the text under the headings may be tailored by SGBs to ensure that the type of processing is accurately covered.

It is important for SGBs to cover all of their personal data processing activities in privacy notices – SGBs should explain clearly what personal data needs to be taken and what purpose this personal data is going to be used for.

### 3.3 Do individuals need to approve or acknowledge receipt of a privacy notice?

SGBs, as controllers, need to be able to evidence that an individual was given a privacy notice and keep a record of what version of the privacy notice that a particular individual received to ensure that their personal data is processed in accordance with that privacy notice.

There is no need for individuals to approve or acknowledge receipt of a privacy notice.

### 3.4 Do we need to provide a privacy notice to an individual where we receive their personal data from a third party?

Where SGBs receive personal data from a third party, the obligation to provide a privacy notice still applies unless specific exemptions apply.

SGBs will need to issue a privacy notice to the relevant individual in their first communication with them, as soon as the SGB receives their personal data (no later than one month from receipt).

If it is not possible to send a privacy notice directly to the relevant individuals, another option would be to make this available on a website and direct individuals to the relevant webpage.

The key for SGBs is to ensure that the information within privacy notices is made available to individuals in whatever manner is most appropriate and practicable for the SGB.

### 3.5 Does a Scottish SGB need a separate privacy notice from the British SGB?

As it is a separate legal entity it is recommended that Scottish SGBs have their own privacy notices so that individuals understand that the Scottish SGB processes their personal data as a controller. Any sharing of personal data between Scottish and British SGBs will need to be detailed in the relevant privacy notice.

## 4 Subject access requests (SARs)

The most commonly used right of individuals regarding their personal data is the right to access their personal data, known as a "subject access request" or "SAR". This right entitles an individual to ask the SGB to confirm that they are processing their personal data, provide them with access to the personal data that the SGB holds on them and other supplementary information regarding the processing of their personal data (similar to what needs to be included in a privacy notice).

A SAR can be made in writing (including email) or verbally and can be for all personal data held by the SGB or for a particular type of personal data (for example, email correspondence between a specific date range relating to a particular topic).

SGBs must respond to SARs within one month of receipt, starting the day the SGB receives the SAR (whether or not this is a working day) and ending on the corresponding date in the following month (or the next working day). There are limited circumstances in which this time limit can be extended by two months, provided the SGB informs the individual within the first month that an extension is being applied and the reasons for this.

SGBs will need to be satisfied that the requestor has authority and may request information from the requestor to verify their identity. If a SGB has requested ID verification from a requestor then the tone for responding starts when that information is received, provided the SGB makes the request as soon as possible.

### 4.1 Does a SAR apply to all SGB email correspondence?

Where an individual is the subject of an email and is able to be identified from that email then it would fall to be disclosed in response to a SAR (for example, an email from X to Y talking about Z would constitute Z's personal data) if the SAR requests all data or refers to emails.

SGBs will need to consider whether anyone involved in SGB business uses a private email address to process personal data on behalf of the SGB as such email correspondence may need to be considered in response to a SAR. Any personal data held by processors on behalf of SGBs will also fall to be disclosed in response to a SAR.

### 4.2 Can a parent submit a SAR on behalf of their child?

In Scotland, children aged 12 and over are presumed to have capacity to exercise their data protection rights, including the right to make a SAR. Accordingly, unless SGBs have a reason to believe that a child aged 12 and over does not have capacity to make a SAR, SGBs should be mindful of this where a parent submits a SAR on behalf of a child aged 12 of over.

Where SGBs receive a SAR from a parent of a child who, for example, is 15 years old, the SGB should not release any personal data of the child to the parent until the SGB is satisfied that the child has consented to the release of their personal data to the parent. If sufficient consent is not forthcoming, the SGB may deem it appropriate to release the personal data covered under the SAR to the child and not the parent. SGBs will need to consider what information to release and to whom on a case by case basis.

### 4.3 Can SGBs disclose personal data of other people in response to a SAR?

SARs entitle individuals to receive a copy of their own personal data, not anyone else's. There is an exemption to withhold certain information from disclosure in response to a SAR where disclosure of such information would involve disclosing information relating to another individual who can be identified from that information.

However, this exemption is not an absolute exemption. SGBs may release third party personal data where that third party has consented to the disclosure or it is reasonable to disclose the information without their consent.

Where SGBs decide to apply this exemption, they may seek to redact the third party personal data, rather than withholding the relevant information in full, where the SGB is satisfied that disclosure of the redacted information does not have a risk of identifying the third party.

### 4.4 Are there any exemptions to withhold information under a SAR?

There are certain exemptions that will allow SGBs to withhold certain information under a SAR (for example, where information constitutes legal advice and is subject to solicitor / client privilege in Scotland).

However, if SGBs have concerns regarding the disclosure of information under a SAR, they should seek advice through the **sport**scotland legal expert resource helpline (details below) to determine whether any exemptions apply to that information.

## 5 General FAQs

Below are some general frequently asked questions:

### 5.1 What are the required security measures for controllers?

The GDPR does not define what security measures are needed. It requires SGBs to have a level of security which is appropriate to the risks presented by the relevant processing activity and the resources available to the SGB.

SGBs should carry out risk assessments to help define what level of security is appropriate for their data processing. SGBs should aim to build a culture of security awareness within their organisation. SGBs should identify a person with day-to-day responsibility for information security and make sure this person has the appropriate resources to do their job effectively.

### 5.2 What is the privacy shield?

Under the GDPR, transfers of personal data outside of the European Economic Area are restricted unless there are "appropriate safeguards" or an exemption applies. The EU-US Privacy shield is a framework which allows the exchange of personal data between the EU and the USA.

If an organisation is certified under the Privacy Shield framework, this is an "appropriate safeguard" to transfer personal data to that company. Any such transfers need to be detailed in the SGB's privacy notice, together with details of the applicable "adequate safeguard" or exemption.

### 5.3 Is there a requirement for SGBs to register with the ICO?

SGBs can make use of a self-assessment test to see if they are required to register with the ICO at https://ico.org.uk/for-organisations/register/self-assessment/

### 5.4 Do SGBs have to report all breaches to the ICO?

Under the GDPR, SGBs are only required to report a personal data breach to the ICO if it is likely that the breach will result in a risk to the individual's rights and freedoms. For example, SGBs will need to consider if a breach could have an adverse effect on individuals, including emotional distress, physical or material damage. The obligation to notify is 72 hours from the SGB becoming aware of the breach (including evenings and weekends).

The GDPR also requires SGBs to report personal data breaches to affected individuals where that breach is likely to result in a high risk to their rights and freedoms. This notification should take place as soon as possible.

All personal data breaches suffered by SGBs must be recorded in an internal record, regardless of whether or not the breach is reported to the ICO or affected individuals, together with reasons of why the SGB decided not to report the breach.

## Get in touch

SGBs can access the **sport**scotland legal expert resource helpline by email at sportscotlandinfo@harpermacleod.co.uk or by calling 0141 227 9333.

# About us

Harper Macleod is a leading Scottish independent law firm that is driven to deliver.

Our growth and success is determined by your success, which is why we always try harder. We don't just see ourselves as lawyers, we see ourselves as problem solvers and business advisers, who focus on understanding your needs. We work side by side with you, using law as a tool to provide innovative solutions that are tailored to organisations and individuals.

It's this drive that sets us apart and delivers a better outcome for you or your organisation.


 harpermacleod.co.uk

 info@harpermacleod.co.uk

 @HarperMacleod

**Glasgow**
The Ca'd'oro
45 Gordon Street
Glasgow G1 3PE
t: +44 (0)141 221 8888

**Edinburgh**
Citypoint
65 Haymarket Terrace
Edinburgh EH12 5HD
t: +44 (0)131 247 2500

**Inverness**
Alder House
Cradlehall Business
Park Inverness IV2 5GH
t: +44 (0)1463 798777

**Lerwick**
St Olaf's Hall
Church Road, Lerwick
ZE1 0FD
t: +44 (0)1595 695583

**Thurso**
Naver House
Naver Road
Thurso KW14 7QA
t: +44 (0) 1847 630930




HM Harper Macleod LLP


JMc/KS_021018