sportscotland

Data Protection for Sports Governing Bodies

Driven by partnership

Harper Macleod LLP

Introduction

This Guide is intended to be a comprehensive and bespoke guide to the key compliance issues arising under the General Data Protection Regulation (EU) 2016/679 (the "GDPR") and the UK Data Protection Bill (the "DPB") for SGBs.

The new legal regime for data protection in the UK will be governed by both the GDPR and the DPB, which transposes the GDPR into UK law and replaces the Data Protection Act 1998. In this guide, any reference to the "Data Protection Legislation" refers to both the GDPR and the DPB.

The Guide considers some of the key implications of the Data Protection Legislation for SGBs in relation to processing personal data with reference to practical examples within the sports sector.

Special and detailed consideration is given to a number of topical issues, including: data security; data retention (including electronic document management systems); international transfers of personal data; photography and filming; and children and parental consent. This Guide is a useful desktop tool for all staff and volunteers within SGBs and includes high-level tips and action points for each section.

While the Guide is detailed in its content, it is not intended to be a substitute for professional legal advice, and SGBs should make use of the **sport**scotland expert resource should they require more detailed and specific advice on data protection matters. SGBs can access the **sport**scotland expert resource helpline by email at **sport**scotlandinfo@harpermacleod.co.uk or by calling 0141 227 9333.

The guide reflects the proposed law as at February 2018.

Get in touch

If you have any questions about the contents of this Guide, or would like to find out any more information, please do not hesitate to contact a member of our team.

Bruce Caldow, Partner
t: 0141 227 9339
e: bruce.caldow@
harpermacleod.co.uk

James McMorrow, Partner
t: 0141 227 9329
e: james.mcmorrow@
harpermacleod.co.uk

Kelly Sleight, Solicitor
t: 0141 227 9306
e: kelly.sleight@
harpermacleod.co.uk

Contents

1. Scope of the Data Protection Legislation

What you need to know...

- The Data Protection Legislation requires your SGB, as a controller, to handle personal data held in electronic files and within highly structured paper files in a responsible manner.
- The Data Protection Legislation applies to all activities undertaken by your SGB in relation to personal data.
- Your SGB will process a range of special categories of personal data, including health data, in relation to athletes, employees and others involved in your sport.

The Data Protection Legislation is concerned with ensuring that organisations handle personal data in a responsible manner. The Data Protection Legislation applies to the processing of personal data relating to data subjects by controllers.

A controller is the person who determines the purposes and means of processing any personal data in its possession. SGBs are the controllers of the majority of the personal data that they process in carrying out their functions relating to registered athletes and other individuals with whom they interact, including: employees; volunteers; board members; agents; sponsors; consultants; and coaches. Such persons are known as data subjects (they are referred to as "data subjects" and "individuals" interchangeably within this Guide).

Another body which is subject to the Data Protection Legislation is a processor, who processes personal data on behalf of a controller. Where, for example, payroll or membership administration or the marketing function of a SGB is outsourced to a third party, that third party will usually be a processor of any personal data that it processes in providing that function to the SGB. Processors also have obligations under the Data Protection Legislation.

Data is information that is held on a computer any electronic device, including smart mobile phones, and within highly structured paper filing systems. Such paper filing systems are those that are set up in a way that particular information in relation to a specific individual is readily accessible according to specific criteria. For example, if a SGB's employee files are indexed or sub-divided into categories (for example, sickness, absence, contact details, emergency next of kin details) enabling quick access to specific information, then they are likely to constitute a relevant filing system.

For data to be personal, it has to relate to an identified or identifiable living individual. This also includes pseudonymised data, which could identify an individual if additional information is used.

Examples of personal data with which SGBs may come into contact include: names; contact details; athlete performance data; medical history; education and training records; health and injury records; and membership records.

The Data Protection Legislation contains additional rules in relation to the processing of special categories of personal data, which consists of data relating to and individual's:

- racial or ethnic origin;
- political opinions;
- health;
- sexual life or sexual orientation;
- religious or philosophical beliefs;
- trade union membership; and
- genetic / biometric data for the purpose of uniquely identifying an individual.

The Data Protection Legislation prohibits the processing of special categories of personal data (and personal data relating to criminal convictions or offences) unless a special condition is met. Details of the most relevant special conditions for SGBs are set out in section 3 of this Guide.

Processing of personal data covers any activity carried out by a SGB on personal data, including collecting, storing, using, disclosing, amending and deleting.

2. Data protection principles

What you need to know...

- Your SGB must comply with the six data protection principles (the "DPPs") contained within the Data Protection Legislation when handling personal data.
- The DPPs apply during the full lifecycle of personal data within your SGB, from its collection to its continued use and through to its ultimate deletion.

As controllers, SGBs must comply with the DPPs. The DPPs require SGBs to ensure that:

- personal data is processed lawfully, fairly and in a transparent manner;
- personal data is collected only for specified, explicit and legitimate purposes and not processed in a manner which is incompatible with those purposes;
- personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- personal data is accurate and, where necessary, kept up to date, every reasonable step taken to erase or rectify personal data which is inaccurate;
- personal data is not kept in a form which permits identification of data subjects for longer than is necessary; and
- appropriate technical and organisational security measures processed in a manner that ensures appropriate security of personal data, including protection against using unauthorised or unlawful processing, accidental loss of or destruction or damage to personal data.

In order to ensure lawful processing of personal data on an ongoing basis, SGBs should do the following with regard to each DPP:

- DPPs 1 and 2 – SGBs cannot exceed scope of the initial privacy notice and must continue to process personal data for the purposes specified in that privacy notice at the time of data collection;
- DPP 3 – SGBs must ensure that the personal data they are processing remains relevant to the purposes for which it is processed;
- DPP 4 – SGBs must maintain the accuracy of any personal data that they process and must keep it up-to-date;
- DPP 5 – SGBs must not retain personal data for longer than necessary for the purposes for which it is processed by the SGB on an ongoing basis; and
- DPP 6 – SGBS must put and keep in place appropriate technical and organisational measures to guarantee the security of personal data processed by the SGB as part of its activities.

3. Lawfulness of processing

What you need to know...

- It is fundamental that your SGB ensures that any processing of personal data is lawful under the Data Protection Legislation.
- This means that your SGB must be satisfied that you have a legal basis for processing personal data before any processing takes place.
- The Data Protection Legislation provides that processing of personal data and special categories of personal data shall only be lawful where there is a legal basis and one of a prescribed set of circumstances applies.

In order to lawfully process personal data under the Data Protection Legislation, SGBs must have a legal basis for the processing. This means that before SGBs process any personal data, one of the following legal bases must apply:

- the consent of the individual has been obtained by the SGB in relation to the processing of their personal data for one or more specific purposes. Consent will only be appropriate in certain circumstances, details of these are set out below;
- the processing of the personal data is necessary for the performance of a contract to which the individual is a party or to take steps at the individual's request before entering into a contract. This might include performance of a SGB's obligations under a contract of membership with individual members;
- the processing of the personal data is necessary for compliance with a legal obligation to which the SGB is subject. For example, compliance with certain conditions imposed by **sport**scotland or statutory requirements;
- the processing of the personal data is necessary to protect the vital interests of an individual or another person. This covers life or death situations, for example, disclosure of an individual's age to emergency services
- the processing of personal data is necessary for the performance of a task carried out in the public interest. For example, processing that is necessary for the administration of justice, which is unlikely to apply to SGBs in many circumstances; or
- the processing of the personal data is necessary for the purposes of the SGB's legitimate interests, or those of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual, which require protection of their personal data, in particular where the individual is a child. For example, processing personal data for fraud prevention and, in some cases, direct marketing activities where these relate to the core activities of the SGB.

The Data Protection Legislation expressly prohibits the processing of special categories of personal data, unless specific conditions apply. SGBs must meet a legal basis and at least one special condition before processing any special category personal data.

This Guide does not set out all of these conditions. However, the conditions most likely to apply to SGBs' processing of special categories of personal data are:

- the **explicit** consent of the individual has been obtained by the SGB in relation to the processing of their special categories of personal data for one or more specified purposes. Explicit consent will require a clear affirmative statement by the individual. Consent will only be appropriate in certain circumstances, details of these are set out below;
- the processing of employees' special categories of personal data is necessary for carrying out obligations and exercising rights that SGBs have under employment law;
- the processing of the personal data is necessary to protect the vital interests of an individual where they are physically or legally incapable of giving consent. For example, disclosing information regarding an individual's injury in an emergency;
- the processing relates to personal data which are manifestly made public by the individual. This might cover the processing of information relating to an athlete's injury in relation to which they have already released a press statement;
- the processing of the personal data is necessary for SGBs to establish, exercise or defend a legal claim. For example, if a personal injury claim is raised against a SGB in relation to an event that it held or regarding proceedings for athlete conduct / disciplinary;
- the processing of the personal data is necessary for reasons of substantial public interest and is authorised by UK law. For example, processing personal data revealing an individual's racial or ethnic origin for equality monitoring purposes; or
- the processing of the personal data is carried out in connection with measures designed to eliminate doping in sport, at a sporting event or in sport generally or for the purposes of providing information about doping or suspected doping to, for example, UK Anti-Doping, or another authorised body.

Examples of processing activities that SGBs undertake and must meet at least one of the lawful bases set out above include:

- processing membership applications;
- administering emergency medical treatment on the field of play;
- submitting samples to UK Anti-Doping to detect anti-doping in sport;
- collecting athlete performance data using either wearable technology or video recording;
- entering into commercial arrangements with sponsors and providing them with access to SGB databases for the purposes of sending promotional communications to members on the sponsors' products and services;
- video and broadcasting of events;
- transfers of personal data to other countries as part of participating in competitions, including athlete accreditation; and
- publication of event results on the SGB website or SGB publications, such as newsletters.

Consent

It is possible for SGBs to ask for individuals' consent to the processing of their personal data to allow SGBs to use this as a legal basis for the processing. SGBs may only ask for individuals' consent where SGBs can offer individuals a genuine choice over how their personal data may be processed. This means that it is not always appropriate to ask individuals for their consent.

Under the Data Protection Legislation, consent will likely be inappropriate where:

- the SGB would still process the personal data under a different legal basis if an individual refused or withdrew their consent. For example, an individual is asked to consent to processing, which is necessary for the SGB to comply with a legal obligation;
- it is required by the SGB as a precondition of accessing its services. For example, to complete a course booking or competition entry; or
- the SGB is in a position of power over the individual. For example, an employer / employee relationship.

Where SGBs do ask for individuals' consent to process their personal data, the Data Protection Legislation requires that individuals are provided with a privacy notice that complies with the Data Protection Legislation and includes information on how individuals withdraw their consent. In addition, consent:

- must be a clear affirmative action: opt-in rather than opt-out and no pre-ticked boxes;
- should be separate from other terms and conditions;
- must provide granular options for different processing activities; and
- be easy to withdraw.

Photography and videos

Photographs and video may contain special categories of personal data of individuals where the images or footage reveal certain information, for example, where they reveal an individual's racial or ethnic origin or religious beliefs.

Where your SGB intends to use such footage or images, you will need to ensure that there is a lawful basis for doing so – it may or may not be appropriate to obtain the individual's explicit consent, provided your SGB can ensure that the footage or images are not further processed if the individual withdraws their consent.

4. Rights of individuals

What you need to know...

- Your SGB must recognise the rights that individuals have under the Data Protection Legislation. In particular, your SGB should ensure that individuals are informed of your SGB's processing activities regarding their personal data with the provision of an appropriate privacy notice.
- One of the rights most commonly exercised by individuals is the right of subject access. Your SGB must respond to requests for access within one month. Caution must be exercised to ensure that third party personal data is not inadvertently disclosed when responding to a subject access request.
- There are also other rights that individuals may seek to exercise directly against your SGB as a controller of their personal data. Your SGB should consider the exemptions from the subject access rights contained within the Data Protection Legislation in order to restrict the disclosure of confidential commercial information from disclosure to the individual requestor.

Right to be informed / Privacy notices

Individuals have a 'right to be informed' under the Data Protection Legislation, which encompasses a controller's obligation to provide 'fair processing information', typically through a privacy notice. The term 'privacy notice' is used to describe all privacy information made available to individuals when collecting their personal data. SGBs must ensure that their processing activities are transparent and that individuals are informed of the existence of any processing operation and its purposes of their personal data by SGBs.

Your SGB should provide individuals with a privacy notice at the time you collect their personal data or, where the personal data is obtained from another source, within a reasonable period depending on the circumstances of the case - one month.

Privacy notices can be included in online and offline forms which ask individuals to provide their personal data. The privacy notice can be included above the point at which the individual signs the form or clicks "Submit".

The Data Protection Legislation requires that your SGB's privacy notice includes the following information:

- the identity and contact details of your SGB as a controller;
- the purposes and legal basis for processing the personal data;
- where your SGB is processing the personal data in pursuit of your SGB's or a third party's legitimate interests, details of what these legitimate interests are;
- where your SGB is processing the personal data under consent, details of the individual's right to withdraw their consent;
- categories of the relevant personal data (only where the personal data is not obtained directly from the individual);
- details of each of the rights that the individual has under the Data Protection Legislation, including the right to lodge a complaint with the ICO regarding the SGB's processing of their personal data;
- details of any recipients or categories of recipients of the individual's personal data. For example, where the personal data is passed between your SGB and member clubs;
- details of whether or not the personal data is transferred outwith the EU and, if so, details of the safeguards put in place by the SGB for the transfer;
- the retention period for the personal data or criteria used by the SGB to determine that retention period;
- the source of the personal data and whether it came from publicly accessible sources (only where the personal data is not obtained directly from the individual);
- any possible consequences of failing to provide the personal data if the provision of the personal data is part of a statutory or contractual requirement (only where the personal data is obtained directly from the individual); and
- whether or not there are any automated decision-making processes applied to the personal data.

Examples of purposes which are relevant for SGBs to include within your privacy notices are:

- sending communications to individuals and member clubs relating to competitions, training courses and other activities;
- sharing personal data with third party organisations, such as **sport**scotland for audit and reporting purposes and Disclosure Scotland for the purposes of undertaking PVG checks;
- assisting in developing new programmes for the strategic development of the sport and the SGB; and
- retaining personal data for historical and statistical purposes, such as competition results and qualifications.

In the event that a SGB wishes to use collected personal data for a different purpose that is not included in the privacy notice, the SGB will need to provide a new privacy notice to the individuals concerned. SGBs must keep an audit trail of the privacy notice which individuals have been provided with and at what stage. This reduces the risk of using personal data for a purpose that is incompatible with the purposes notified to the individual.

Effective risk management

SGBs must ensure that privacy notices, both offline and online, are future-proof. This involves the SGB thinking ahead about the purposes for which it will use the personal data, which is important to ensure that the SGB does not exceed the scope of the privacy notice.

SGBs must retain effective audit trails with regard to the privacy notices that have been provided to individuals. This ensures that SGBs are clear as to what purposes they may use certain personal data for in respect of each individual.

Moreover, in the event that an individual seeks to exercise a right in respect of their personal data – for example, objecting to the SGB's processing of their personal data – the SGB must ensure that such requests are recorded, together with a record of the SGB's decision of whether or not to comply with the request. This is important from the point of view of ensuring that personal data in respect of which, for example, an objection has been received is not processed further by the SGB.

Personal data from third parties

There may be circumstances where SGBs receive personal data. For example, where member clubs pass their individual members' personal data to the SGB or where the SGB uses athletes' personal data, which is either available publicly or from another SGB.

Upon receipt of the personal data, of which the SGB then becomes the controller, the SGB must provide the relevant individuals with a privacy notice within a reasonable time period, unless:

- the SGB is satisfied that the individual already has the required privacy information; or
- provision of the privacy notice would involve a disproportionate effect.

Subject access requests

The Data Protection Legislation confers a number of rights on individuals in relation to their personal data held by SGBs, as controllers. An individual has a right, on making a request to a SGB, to be informed whether personal data of which they are the data subject is being processed by or on behalf of that SGB and, if so, the individual also has a right to receive:

- a description of the personal data held, the purposes for which the personal data are being processed and the recipients or categories of recipients to whom the personal data may be or has been disclosed;
- in particular, recipients in countries outside the EU or international organisations;
- any information available to the SGB as to the source of the personal data (subject to certain stated confidentiality and related protections for individual sources)
- where possible, details of how long the personal data will be stored or how this will be determined; and
- details of the rights of the individual under the Data Protection Legislation, including the processing of the personal data and the right to complain to the ICO.

The Data Protection Legislation provides that, in order to meet these obligations, a copy of the personal data in electronic form, where the request is made by electronic means, must be provided unless otherwise requested by an individual.

A subject access request must:

- be addressed in writing to the SGB (including email);
- contain information to enable the SGB to satisfy itself as to the identity of the individual making the request; and
- provide information to enable the SGB to locate the personal data sought.

SGBs must comply with requests promptly and, in any event, within one month from the receipt of the request or from the receipt of the information necessary to enable the SGB to comply with the request (for example, from the date of the provision of sufficient information to allow for the verification of the identity of the data subject), whichever is later. It is possible to extend this time period by two months but only for complex or numerous subject access requests.

Where disclosure in response to a subject access request includes the disclosure of third party personal data to the individual making the request, such as the personal data of witnesses on the field of play or in a disciplinary context, then the Data Protection Legislation provides that, if it is not possible to edit or delete the third party data, the SGB need not provide information in response to a subject access request unless the third party concerned has consented or it is reasonable in all the circumstances to comply with the subject access request without such consent.

A SGB need not comply with a subject access request where it is similar or identical to one that has already been complied with, unless a reasonable period of time has elapsed in the interim.

Other rights

Other rights of individuals under the Data Protection Legislation include:

- the right to rectification allows individuals to request a SGB corrects their personal data if it is inaccurate or incomplete;
- the right to erasure is also known as the right to be forgotten allows, as individuals to request that SGBs delete or remove their personal data where there is no compelling reason to continue processing it. This right only applies in certain circumstances;
- the right to restrict processing allows individuals to request SGBs to restrict the processing of their personal data and SGBs must comply with such a request in certain circumstances;
- the right to data portability allows individuals to obtain their personal data from SGBs to re-use it for their own purposes. This right only applies in certain circumstances; and
- the right to object allows individuals to object to SGBs processing of their personal data in certain circumstances.

If a SGB receives any of the above requests from an individual and decides to comply, that SGB must also let any third parties who have received the relevant personal data know. For example, if a SGB complies with a request to rectify a participant's personal data and that SGB has shared the participant's personal data with an English sports governing body then the SGB should inform the English sports governing body to ensure the participant's personal data is accurate.

SGBs have one month to responds to requests from individuals exercising their rights under the Data Protection Legislation and it is possible to extend this time period by two months for

5. Processors

What you need to know...

- If your SGB engages a third party to provide services to the SGB and such services involve the processing of personal data on behalf of your SGB, as a controller, then that third party will be the processor of such personal data for the purposes of the Data Protection Legislation.
- The Data Protection Legislation requires that your SGB enters into a written contract with the processor and includes a list of requirements that must be included.

It is control rather than possession of personal data that is the determining factor for the purpose of the application of the Data Protection Legislation. Where personal data is processed on behalf of a SGB by another party, for example, a supplier, the SGB is required to ensure that the processor has implemented the necessary security measures in relation to such personal data.

The SGB must also enter into a written contract with the processor which requires the processor to:

- process the data only on the documented instructions of the SGB as controller;
- ensure that persons authorised to access the data are subject to a duty of confidentiality;
- take the measures required by the Data Protection Legislation relating to security;
- not engage another processor unless specifically without prior specific or general written authorisation of the SGB and notifies the SGB of any intended changes to sub-processors. Sub–processors shall be subject to the same obligations under a written contract with the processor and the processor is fully liable for any breaches by any sub-processor;
- assist the SGB with technical and organisational measures and in responding to requests from individuals under the Data Protection Legislation;
- deletes or returns the personal data to the SGB at the end of the contract (at the SGB's discretion) and deletes existing copies unless the processor is under a legal obligation to retain such personal data; and
- provide any information required by the SGB to demonstrate compliance with the processor's obligations under the Data Protection Legislation and contributes to audits conducted by the SGB.

The contract between the SGB and any processor must also set out the following:

- subject-matter and duration of the processing;
- nature and purpose of the processing;
- type of personal data and categories of individuals involved; and
- obligations and rights of the SGB and processor.

6. Data retention in sport

What you need to know...

- Your SGB cannot hold personal data indefinitely and for longer than it needs to.
- The Data Protection Legislation does not set out how long personal data may be kept for.
- Your SGB must come to a view based on statutory legal requirements, best practice in the sector and the costs and risks associated with keeping personal data for longer than is required.
- Anonymisation of personal data should be considered as a means of keeping data as long as possible.
- Your SGB should put in place a data retention and records management policy, which sets out roles and responsibilities for data retention within your SGB and destruction arrangements.
- When personal data has reached the end of its retention period, your SGB must review the personal data and either archive or destroy it. While the latter is simple to achieve with paper records, it is more difficult in the case of electronic files.
- Your SGB must take care to dispose of IT assets containing personal data securely.
- Keeping personal data for longer than is necessary exposes your SGB to a number of risks and may result in breach of the DPPs.

DPPs and data retention

DPP 5 provides that personal data processed by SGBs for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The Data Protection Legislation does not set out specific retention periods, but all DPPs have retention implications, which SGBs must consider when determining the retention periods of personal data of which they are the controller, as follows:

DPP 1: the privacy notice provided by the SGB should specify the period for which personal data will be retained or the criteria for determining the period for retaining personal data;
DPPs 3, 4 and 5: these DPPs require that only relevant, accurate and up-to-date personal data is processed that is not kept for longer than is necessary for the purposes for which it is processed; and
DPP 6: SGBs should have a records management policy that sets out how personal data is managed and handled by the SGB, particularly in relation to the secure disposal of personal data.

Determining retention periods

The period for which SGBs retain personal data can derive from a number of different sources:

- legal requirements – specific laws may require personal data to be retained for particular periods of time, for example, health and safety legislation and employment law, which require certain records to be retained for periods between 2 and 40 years;
- sector or best practice guidelines – guidance available within the sports sector may require SGBs to hold on to personal data for specific periods;
- current and future value of the personal data to the SGB – if the SGB's interests are likely to be prejudiced by the personal data being disposed of too soon then it may consider retaining the personal data for an extended period to protect against such prejudice arising;
- costs, risks and liabilities associated with retaining personal data – if retaining the personal data would involve having in place expensive archive facilities or disk storage or would give rise to prejudice to the individuals to whom the personal data relates (for example, there is a significant risk that inaccurate, historic and irrelevant personal data relating to individuals could be processed by the SGB to the detriment of the individuals concerned) then the SGB may favour disposal of the personal data to reduce such risk;
- ease or difficulty of ensuring that personal data is accurate and up-to-date – if it is difficult for the SGB to ensure that the personal data is accurate and up-to-date, the SGB may decide to dispose of the personal data in order to reduce the risk of processing inaccurate, out-of-date personal data;
- purpose for which it was obtained – if the purpose for which the SGB obtained the personal data has been fulfilled or is no longer relevant then the SGB may consider that it no longer needs the personal data;
- historical, statistical or research purposes – SGBs may retain personal data for such purposes, provided that they continue to comply with the Data Protection Legislation. SGBs may wish to retain such personal data in anonymous form, if possible, which would mitigate the risk associated with complying with the Data Protection Legislation;
- end of relationship – once an individual has withdrawn from membership of a SGB or is no longer an employee or is not actively involved in the sport, the SGB may wish to consider whether it is appropriate to continue holding on to all of some of the personal data of that individual; and
- defence of future legal claims – if the SGB requires personal data for this purpose, it should only retain it for as long as it is necessary to defend such claims. Once the risk of a claim arising has ceased because, for example, the period during which a claim may be brought against the SGB has elapsed, the SGB may destroy the personal data that it holds (subject to other legal requirements).

Records management

The means of managing the records of a SGB effectively and demonstrate compliance with the DPPs, in particular DPP5, is to have either or both of a data retention and records management policy. Both documents can be a useful internal guidance tool on the maintenance and destruction of a SGB's records and a data retention policy will be useful to have in terms of the Data Protection Legislation.

A data retention policy will set out who is responsible for records management within the SGBS; retention schedules setting out how long personal data should be retained; and destruction arrangements.

The records management policy will specify: roles and responsibilities for managing records; how audit trails are maintained by the SGB; how records are created within the SGB; requirements relating to storage, management and disposal of records; and monitoring and reporting on general records management issues.

What happens at end of the retention period?

When personal data has reached the end of its retention period, a SGB may review the personal data and either archive or delete it.

Personal data should only be archived in the event that a SGB still needs it. This is because the Data Protection Legislation applies to archived personal data, and SGBs must continue to provide subject access to such personal data and comply with all DPPs in retaining it.

If the SGB decides to destroy the personal data, this is relatively simple to achieve in the case of personal data held in paper format. Difficulties can arise in relation to the deletion of electronic personal data, particularly since such personal data can easily be reinstated post deletion. The key issue is whether deleted electronic personal data is "live" i.e. the SGB intends to reinstate and use it again. If not, the electronic personal data is "put beyond use" and considered deleted.

SGBs must also exercise caution when disposing of IT equipment containing personal data in order to ensure personal data is not accessible post disposal. If the SGB engages a third party for this purpose, the third party is a processor of the personal data and the SGB, as controller, must ensure that the third party puts appropriate security arrangements in place to protect the personal data from loss or disclosure by the third party. SGBs need to ensure that any processors of their personal data have written agreements in place to govern the processing activities (please see section 5 of this Guide for further details

Data retention and risk management

If a SGB retains personal data for longer than required in breach of DPP 5, the SGB exposes itself to a number of risks, including:

- holding on to outdated personal data, which could give rise to a risk of the rights and freedoms of the individuals involved;
- the SGB will need to keep the personal data accurate, which is more difficult when the personal data is voluminous;
- the more personal data is held by the SGB, the more difficult it is to comply with subject access requests as there is more personal data to review;
- risk of breach of DPPs 3 and 4, as the SGB may hold excessive and irrelevant personal data relative to the purposes for which it is held; and
- it is expensive to maintain eDMS and archive facilities and more so when there is a considerable volume of personal data involved.

In order to manage these risks appropriately, a SGB should:

- carry out a data audit and review how long it retains personal data in practice;
- consider the purposes for which the personal data is held;
- establish standard retention periods by reference to the law, industry or best practice;
- follow the data retention and records management policy in practice; and
- securely delete out-of-date or irrelevant personal data to reduce the risk of claims of data protection breaches post personal data deletion.

7. Secure data protection in sport

What you need to know...

- Your SGB must put in place physical and technical organisational security measures to protect the personal data that it holds against certain risks, including unauthorised access, loss and damage.
- Ensure that personal data is only accessible to personnel within your SGB on a need-to-know basis.
- Carry out a data security audit to identify areas for improvement within your SGB. This may range from putting in place a visitor book at reception to improving your firewall and providing training for staff and volunteers.
- Data security is a key risk area. The ICO has imposed the largest fines on organisations in the data security context. Caution is recommended.

DPP 6

The Data Protection Legislation requires SGBs, as controllers of the personal data that they process, to put in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In determining the scope of such measures, SGBs must consider:

- the state of the art and cost: SGBs must look at what is available on the market and the cost of implementing the latest measures. For example, if a 2005 edition of Internet security software is currently being used then this should be updated to the latest edition – a relatively inexpensive security measure. A risk-managed approach should be adopted and SGBs should respond to specific risks that they have identified;
- the nature of personal data to be protected: SGBs should accord more protection to special categories of personal data and children's personal data by, for example, restricting internal access to such personal data and ensuring that disclosures to third parties are appropriately managed;
- any resulting harm which may arise from a breach: if a breach of the requirements would give rise to significant emotional upset to third parties, such as vulnerable adults or children, or significant damage, for example, financial loss through compromise of bank account details, then more stringent security measures will be necessary;
- the effectiveness of existing measures: if SGBs have experienced a data protection breach or an audit has identified weaknesses within the existing infrastructure then additional measures should be taken to secure personal data; and
- the reliability of staff: security of personal data ultimately depends on those who process personal data on behalf of SGBs, including staff, volunteers and contractors. SGBs must therefore demonstrate that they carry out sufficient due diligence on their staff, volunteers and contractors relative to the role performed. For example, staff and handling personal data relating to children and vulnerable adults must be subject to appropriate PVG checks and contractors should equally be required to provide evidence that they have carried out similar checks in respect of their staff.

Effective risk management

Data security is a key risk area for SGBs. SGBs need to ensure that: data is accessible only to authorised personnel within the SGB (confidentiality); personal data is accurate and complete (integrity); and authorised users within the SGB are able to access data when required (availability). Data security incidents are also high on the ICO's list when it comes to enforcement action against controllers, with some of the largest fines to date being imposed in the data security context.

In order to mitigate the risks of breaching the Data Protection Legislation's data security requirements, SGBs should:

- start with simple security measures, such as requiring visitors to sign in upon arrival and wear visitor badges during their visit;
- enforce a clean desk policy and encourage staff and volunteers to put files away in drawers and cabinets (which are capable of being locked) when they are not required;
- secure internal and external doors by electronic key card or fob to ensure that only those with such devices are granted access to buildings in which personal data is stored or, at the very least, restrict access to keys and store keys in locked drawers;
- assign ownership of the data security function to a member of staff who is sufficiently senior and who has support from "designated others" within the SGB;
- implement a data security policy so that staff are aware of the need to exercise caution when handling personal data;
- provide regular and refresher data protection and security training to staff and volunteers, appropriate to their grade and involvement with personal data;
- restrict access to the network to authorised users only, who should have unique usernames and passwords and be required to change their passwords regularly;
- maintain a log of data security incidents;
- carry out a data security audit with a view to identifying areas for improvement and assessing the types of data security measures that could be implemented;
- undertake firewall and penetration testing of the network to minimise the risk of external threats;
- consider how valuable, sensitive or confidential the personal data is and what risks to the rights and freedoms of individuals could be caused in the event of a security breach, particularly children;
- locate servers in locked and separate rooms and limit access to those rooms to IT staff and others who need access;
- keep Internet security software up-to-date in order that the network is protected from the latest threats. Subscribing to security newsletters can be useful in keeping abreast of the latest threats and available countermeasures;
- utilise a well-configured firewall to ensure that the network is protected from intrusions and attacks. This will help identify applications and processes that are running on the network that have not been instigated by the SGB;
- implement suitable security measures for mobile devices to protect personal data "on the move". This may include use of encryption for communications sent to and received from mobile devices and mandatory implementation of VPNs and remote disable / wipe facilities when staff use their own mobile devices in connection with their SGB-related activities;
- advise staff on how they may contribute to providing higher levels of data security by highlighting, for example, the risks involved in posting information about their employment on online forums, such as Facebook; and
- minimise the personal data held. The more personal data that is held, the greater the risk of a data security breach occurring.

8. International transfers of personal data

What you need to know...

- Your SGB must comply with the requirements of the Data Protection Legislation when engaging in international transfers of personal data.
- It is likely that your SGB will be involved in international transfers of personal data when athletes participate in international competitions.

SGBs can be involved in a range of transfers of personal data. These include transfers:

- of medical records in the case of injury on the field of play;
- in connection with competitions to the organisers of the competition and official bodies;
- associated with the broadcasting of competitions (videos and photographs); and
- arising from the posting of personal data on SGBs' websites, for example, photographs of recent events and individuals.

Personal data must not be transferred to a country outwith the EU unless that country ensures an adequate level of data protection. The European Commission is responsible for determining whether a country provides an adequate level of protection. Where the European Commission has made an adequacy determination then SGBs may transfer personal data to that country as if the transfer was taking place within the EU.

However, where the destination country does not ensure an adequate level of data protection, SGBs have a number of options. First, the SGBs can make the transfer subject to appropriate safeguards, and on the condition that there are enforceable data subject rights and effective legal remedies. This involves a complex analysis and would ultimately require local solicitors to be engaged if it is to be undertaken appropriately.

Second, SGBs may enter into binding corporate rules approved by the European Commission or the ICO. These binding corporate rules must be entered into as they are with no modifications.

Finally, there will be certain circumstances where SGBs may transfer personal data where prescribed by UK law. In particular, where data transfers are required for reasons of public interest such as to reduce and / or eliminate doping in sport.

9. Children and data protection in sport

What you need to know...

- The Data Protection Legislation provides that children merit specific protection in relation to their personal data, as they may be less aware of the risks, consequences, safeguards and their rights.
- Your SGB needs to clear as to the circumstances in which it requires to obtain parental consent to the processing of children's personal data. Any such parental consent should be capable of verification.
- Your SGB must take appropriate safeguards when photographing and filming children involved in sporting activities. In order to ensure lawful processing of such images in accordance with individuals' right to be informed, your SGB must be open and upfront within parental consent and privacy notices as to the uses to which such images may be put and to whom they may be disclosed.
- Access to children's personal data within your SGB must be restricted and the security of such personal data must be top priority.
- Privacy notices should be in clear and plain language that children can easily understand.
- In the event that a child seeks to enforce their data protection rights against your SGB, an assessment must be carried out to determine if the child has sufficient maturity and understanding in order to do so. If a parent or third party seeks to do so, evidence of authority to act must be obtained.

SGBs may be involved in the processing of personal data relating to children in the course of their activities. This section sets out the key requirements in this context.

Lawful processing

Lawful processing is important when processing the personal data of children. The SGB needs to be clear as to what personal data is being collected from children and what it will be used for. Clear, simple language should be used within any privacy notices, which is appropriate to the level of understanding of the target audience.

This involves SGBs assessing whether their website is likely to appeal to children – this will be the case for most SGBs that run junior events and competitions. The privacy notices should be prominent and accessible on the SGB's website and on offline and online forms. Further detail can be provided within a privacy policy. SGBs have to be wary of the one of the most obvious difficulties of operating online, namely: are people who they claim to be?

Parental consent

Another issue is that of parental consent. Where a SGB offers online services directly to a child under the age of 12, parental consent must be obtaining before any of the child's personal data. SGBs may wish to obtain parental consent for children under the age of 16 as a matter of best practice.

On that basis, it is recommended that, as a general rule, when SGBs deal with persons under the age under 12 in the course of their activities, they should seek explicit and verifiable parental consent. It is risky to assume that a person of 12 years of age automatically possesses sufficient capacity to make decisions on data protection matters. Indeed, children of similar age can have different levels of understanding and maturity. Assessing the understanding of the child is more important than age. Ultimately, as a controller, the SGB is responsible for determining if parental consent is required in each case. This is not an easy task, and is compounded by resourceful children, who can create email accounts, which appear, on the face of them, to belong to their parents.

It is recommended that parental consent is obtained where the:

- child's name and address will be disclosed to third parties;
- child's contact details will be used for promotional purposes;
- child's image will be published on the SGB's website or social media;
- child's contact details will be made publicly available e.g. SGB website, events results; or
- child is asked to provide third party personal data e.g. parents' contact details.

SGBs must take reasonable steps to verify any parental consent which it has obtained. There are different means of verification:

- the parent prints the form containing the data protection statement, signs and returns it to the SGB by post;
- the SGB sends an email to the parent and requests a response from the parent by email;
- the SGB calls the parent or requires the parent to telephone SGB once the online or offline form has been submitted; or
- the SGB may request information that only the parent would know, for example, the parent's debit / credit card details.

The verification method is a matter of preference for the SGB.

Photographing and filming children

SGBs must take appropriate safeguards when photographing and filming children engaged in sporting activities for the purposes of, for example, the SGB's promotional literature, coaching, training or for recording events in which the children are participating, such as tournaments or summer sports camps.

There are obvious risks of significant damage or distress associated with the capture of photographs and films involving children. These include: inappropriate use of images on Internet; viral dissemination via social media; adaptation of images for inappropriate use; and increased vulnerability to grooming and abuse (where it is possible to pinpoint the child's location). The Data Protection Legislation applies to all photographing and filming carried out by or on behalf of SGBs.

SGBs must seek the child's and the parent's consent to the capture of the child's images in this manner. The consent statement must comply with the Data Protection Legislation, in terms of which SGBs must be upfront about where and how images will be used, for example, online, on social media platforms, or for the purposes of performance monitoring or coaching.

Securing children's personal data

The security requirements of Data Protection Legislation have already been outlined, above. In order to comply with these in a children's personal data context, access to children's personal data must be restricted within the SGB. The devices on which children's personal data is stored must be secured using appropriate passwords and Internet security software. If children's personal data is being disclosed to a third party by, for example, email, email addresses should be checked prior to sending the personal data in order to ensure that the personal data is not sent to the wrong recipient. Ideally, children's personal data should be password protected or encrypted prior to it being transmitted to the recipient.

Enforcing children's data protection rights

Individuals' rights under the Data Protection Legislation can be enforced by the child as the data subject or any person on behalf of child. In practice, it is likely that parents will enforce data protection rights on behalf of children.

In the event that a third party seeks to enforce data protection rights on behalf of the child, a SGB will require to obtain evidence of authority to act. Otherwise, there is a risk that a SGB has not processed personal data in accordance with the rights of the child.

If a child seeks to enforce their rights against a SGB, the SGB must consider whether the child possess sufficient maturity to understand his / her rights, which involves analysing: the child's level of maturity; the nature of personal data (it may not be appropriate to disclose special categories of personal data related to, for example, situations involving abuse to the child, as this is likely to give rise to distress for the child); any duties of confidence owed to third parties (if so, the SGB may risk exposing itself to a breach of confidence action at the behest of the third party if it does not seek its prior consent to the disclosure of the personal data to the child in response to the child's subject access request); the consequences of giving parents access (would this give rise to distress to the child if it relates to a personal matter that the child does not wish to discuss with their parents, for example, a bullying incident involving another member); and the child's views.

Sending communications to children

It is likely that SGBs will wish to send all of their members – including children – promotional communications relating to the SGB's activities, the sport and forthcoming events in which the members may wish to participate.

The Regulation on Privacy and Electronic Communications (the "Regulation") will require that such communications must not be sent by a SGB unless the prior consent of the recipient has been obtained.

It is possible for SGBs to obtain such prior consent by means of the privacy notice provided to members on the membership application form or any other document which the member is required to accept prior to being admitted to SGB membership, provided that the consent statements are separated from any membership terms and conditions and opt-in consent is used.

The Regulation sets down stricter provisions regarding electronic communications to individuals who have had no previous involvement with a SGB, as a controller, for example, where an individual submits their email address through the SGB's website, the SGB should first email the individual with a consent statement to confirm the individual's communication preferences and await a response before sending any email communications to the individuals. In this example, the SGB's website must also have a consent statement which complies with the Data Protection Legislation at the point where the individual submits their email address.

Parental consent may be necessary in order to comply with the requirements of the Regulation.

As noted above, the Data Protection Legislation provides for an absolute right to object to receiving such promotional communications. The child's objections and those of the parent must therefore be respected.

10. Enforcement, sanctions & remedies

What you need to know...

- An aggrieved individual may enforce the Data Protection Legislation against your SGB via the ICO and the courts.
- ICO has wide powers of enforcement, including the power to impose a fine on your SGB of up to 4% of annual global turnover or €20m, whichever is higher.
- The courts may award compensation to an aggrieved individual for breach of the Data Protection Legislation by your SGB.

The ICO is responsible for enforcing the Data Protection Legislation. The ICO will normally only intervenes in the event that the individual is unable to obtain redress from the SGB. Individuals may also enforce their rights against a SGB in the courts.

An individual has a right, where they believe that they are directly affected by the processing of personal data, to make a request to the ICO for an assessment as to whether the processing complies with the Data Protection Legislation. On receiving such a request, the ICO is obliged to carry out the assessment (which may include serving an information notice on the SGB requiring it to provide information to assist the ICO in making the assessment), and to notify the person making the request whether an assessment has been made and of any view formed or action taken by the ICO as a result.

Where it finds a breach of the Data Protection Legislation, the ICO may serve a SGB with an enforcement notice, requiring the SGB to comply with the Data Protection Legislation.
In addition, under certain circumstances, the ICO may (with a warrant from the court) exercise powers of entry, inspection and seizure of documents and equipment. The ICO may also carry out a voluntary audit of entities operating in the private sector.

The ICO also has the power to impose a fine (up to a maximum of 4% of annual global turnover or €20m) for serious contraventions of the Data Protection Legislation.

Individuals are entitled to compensation from SGBs for material or non-material damage caused by any breach of the Data Protection Legislation. Compensation can only be awarded by the courts and not by the ICO. To date, very few claims for compensation have been made.

Aside from legal sanctions, failure to comply with the Data Protection Legislation can result in damaging adverse publicity. Increasingly, any false step in the area of privacy commonly attracts intense media scrutiny, regardless of whether any law has in fact been infringed. This can cause significant damage to the reputation of the SGB concerned.

11. Exemptions

What you need to know...

- The Data Protection Legislation is a strict regime but it contains a number of exemptions to deal with legitimate day-to-day situations, for example, to permit law enforcement activities to take place.
- Your SGB should seek advice on the applicability and relevance of the exemptions to your particular circumstances.

The Data Protection Legislation contains a number of exemptions from the DPPs and other parts of the Data Protection Legislation, including:

- personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes;
- the disclosure of personal data where this is required by law or by court order or the apprehension or prosecution of offenders; or
- personal data processed for the purposes of the prevention or detection of crime.

These exemptions may be useful for SGBs where they receive requests from law enforcement bodies in connection with their investigations.

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

KS/JMc240118