Harper Macleod LLP

Data Protection for Sports Governing Bodies

An introductory guide

Driven to deliver

Harper Macleod LLP

INTRODUCTION

This Guide is intended to be a comprehensive and bespoke guide to the key compliance issues arising under the Data Protection Act 1998 for SGBs.

The Guide considers the full life-cycle of personal data within an SGB from its collection / creation through to its ultimate destruction.

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 within SGBs. It is structured in a manner that allows the user to go to the relevant content immediately without the need to read the entire Guide and includes high-evel 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 sportscotland expert resource should they require more detailed and specific advice on Data Protection matters.

GET IN TOUCH

If you have any questions about the contents of this Guide, or would like to find out any more information, please don't 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 DPA

WHAT YOU NEED TO KNOW ...

- The Data Protection Act 1998 (the "DPA") requires your SGB, as data controller, to handle personal data held in electronic files and within highly structured paper files in a responsible manner.
- The DPA applies to all activities undertaken by your SGB in relation to personal data.
- Your SGB will process a range of sensitive personal data, including health data, in relation to athletes, employees and others involved in your sport.

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

A data controller is the person who determines the purposes for which and the manner in which any personal data in its possession is processed. SGBs are the data controllers 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 DPA is a data processor, who processes personal data on behalf of a data controller. Where, for example, payroll administration or the marketing function of an SGB is outsourced to a third party, that third party will usually be a data processor of any personal data that it processes in providing that function to the SGB. While the DPA does not apply directly to data processors, it requires data controllers to pass on data security obligations to data processors.

Data is information that is held on computer or, indeed, 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. For example, if an SGB's employee files are stored alphabetically by name, and the information on the files is stored in random or even chronological order regardless of subject matter, this would not amount to a relevant filing system, as the searcher would have to leaf through the file to find specific information. However, if the files were 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 identifiable and living individual. The courts have

narrowed the scope of the definition of personal data to cover only data which focuses on individuals and not just any data which mentions individuals by name, although there has, more recently, been a move away from this, with the courts favouring the former definition. 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 DPA contains additional rules in relation to the processing of sensitive personal data, which consists of data relating to:

- racial or ethnic origin;
- political opinions;
- health;
- sexual life;
- religious and other similar beliefs;
- trade union membership; and
- criminal records.

The administration of emergency medical treatment on the field of play is an example of the processing of sensitive personal data by an SGB and others involved in the same (the personal data being processed relates to the athlete's injury, condition and health).

Processing of personal data covers any activity carried out by an SGB from the collection or creation of personal data through to its ultimate destruction.

2. NOTIFICATION

WHAT YOU NEED TO KNOW ...

- The DPA requires your SGB to notify your data processing activities to the Information Commissioner's Office (the "ICO").
- The annual fee ranges from £35 to £500, depending on the size and turnover of your SGB.
- Failure to notify to the ICO is an offence.
- Your SGB may be exempt from notification to the ICO, provided that the tests set out in the DPA are satisfied.

The DPA requires data controllers to notify their data processing activities to the regulator for DPA in the UK, the ICO. The notification process has been significantly streamlined recently and involves completion of an online questionnaire (taking no more than 15 to 20 minutes). The notification fee ranges from £35 to £500 per year, depending on the size and turnover of the SGB.

The DPA contains exemptions from notification, the most relevant of which for SGBs is the exemption that applies to bodies or associations not established or conducted for profit. SGBs are generally not for profit organisations but any profits that they do make should be used in furtherance of their purposes (subject to the

requirements of their constitutions).
In order to benefit from this exemption, SGBs must ensure that:

- they only process personal data of individuals for the following exempt purposes: (i) establishing or maintaining membership of the SGB; or (ii) providing or administering activities for individuals who are either members of the SGB or have regular contact with it;
- they only process personal data of individuals who are either past, existing or prospective members or have regular contact with the SGB for the above exempt purposes;
- the personal data processed by SGBs is the name, address and other information in connection with: (i) eligibility for membership of the SGB; or (ii) other matters the processing of which is necessary for the exempt purposes;
- they do not disclose personal data to any third party, except with the individual's consent or where it is necessary for the exempt purposes; and
- the personal data must not be kept after the relationship between the SGB and the individual ends, unless and only for so long as it is needed for the exempt purpose.

Obviously, if an SGB chooses to take advantage of this exemption, it must recognise that it will be significantly limited with regard to:

- the purposes for which it may process the personal data that it holds;
- the individuals on whom it may process personal data;
- the types of personal data that it can process;
- who it may share personal data with (unless the consent of the relevant individuals has been obtained); and
- how long it may retain any personal data that it processes.

Whether an SGB is required to notify is ultimately a decision for the SGB, as it is difficult to provide a view in the abstract, given the diverse purposes for which and individuals on whom SGBs may process personal data. If an SGB is confident that it meets the above requirements then it need not submit a DPA notification to the ICO or indeed inform the ICO that it falls within the scope of the exemption. It is always open to SGBs to make a voluntary DPA notification to the ICO if they so wish. Moreover, if the scope of an SGB's data processing activities changes over time, it must continuously review whether it is still able to take advantage of the exemption and, if so, immediately submit a notification to the ICO – failure to do so is a criminal offence.

A further exemption from notification applies in relation to those SGBs who do not process electronic personal data. If an SGB only retains paper records then it is not required to make a DPA notification.

An exemption from notification does not, however, result in exemption from application of the DPA to the SGB; SGBs must ensure that they comply with the DPA in all of their data processing activities.

3. DATA PROTECTION PRINCIPLES

WHAT YOU NEED TO KNOW ...

- Your SGB must comply with the eight data protection principles ("the DPPs") contained within the DPA 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 destruction.

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

- personal data is processed fairly and lawfully;
- personal data is obtained only for specified and lawful purposes and not processed for incompatible purposes;
- personal data is adequate, relevant and not excessive in relation to the purposes for which it is processed;
- personal data is accurate and, where necessary, kept up to date;
- personal data is not kept for longer than is necessary;
- personal data is processed in accordance with the rights of data subjects under the DPA;
- appropriate technical and organisational security measures are taken to prevent unauthorised or unlawful processing, accidental loss of or destruction or damage to personal data; and
- personal data must not be transferred outside the European Economic Area ("EEA") (which comprises the EU Member States and Norway, Iceland and Lichtenstein) unless the destination country ensures an adequate level of data protection.

The following sections consider some of the DPPs in detail as they apply to SGBs.

4. FAIR AND LAWFUL PROCESSING

WHAT YOU NEED TO KNOW ...

- It is fundamental that your SGB complies with the fair and lawful requirements of DPP 1. It is the most complex of all of the DPPs.
- Fairness requires your SGB to be upfront and open with individuals as to how your SGB intends to use their personal data. This information can be provided in the form of a data protection statement within your SGB membership application forms, internal corporate policies and on your SGB's website.
- DPP 1 is engaged in a number of circumstances, including: when your SGB processes membership applications; collects athlete performance data; recruits employees; takes photographs and video at SGB events; obtains personal data from children; collects third party personal data; and shares personal data with member clubs and sportscotland.
- It is important that your SGB considers in advance all of the purposes for which it will use collected personal data. Failure to do so could result in your SGB exceeding the scope of the data protection statement and such personal data being used in breach of the fairness requirements of DPP 1.
- Your SGB must also consider the other DPPs when complying with DPP 1. For example, failure to limit the personal data collected may breach DPP 3 as well as DPP 1.
- DPP 1 is complex in practice and presents a high-risk DPA compliance area for your SGB.

DPP 1, requiring fair and lawful processing of personal data, is the most important of all of the DPPs. Processing will clearly not be fair where the data subject is misled or any pressure or inducements are applied when collecting personal data.

For example, it is unlikely that the fairness requirement will be met by an SGB if data subjects are not informed that their personal data is to be used for a particular purpose, for example, collecting health data for the purposes of administering emergency medical treatment on the field of play or collecting performance data via the use of wearable technology for coaching and training purposes.

DPP 1 also requires SGBs to provide certain information to data subjects, which may be provided within a data protection statement and must include:

- the identity of the SGB;
- the purposes for which the SGB will process the personal data; and
- any additional information which is necessary to ensure that the processing is fair in

the circumstances.

Examples of purposes which are relevant for SGBs to include within their data protection statements include:

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

When is fair processing relevant?

The fair processing requirements of the DPA are relevant to SGBs in the following circumstances:

- processing membership applications;
- administering emergency medical treatment on the field of play;
- obtaining consent to doping control and submitting samples to UKAD;
- collection of athlete performance data using either video recording or wearable technology;
- 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;
- processing volunteers' personal data;
- disclosing personal data to third parties;
- handling children's personal data and managing issues of parental consent;
- obtaining consent to video and photography 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.

At the stage of collecting personal data, SGBs should do the following with regard to each DPP:

- DPP 1 – SGBs must act fairly and openly by specifying who they are and confirming that they will collect personal data from the individual when the individual, for example, completes a form on the SGB's website;
- DPP 2 – SGBs must specify the purposes for which they will use the collected personal data and confirm whether any disclosures of such personal data to third parties is envisaged;
- DPP 3 – SGBs must only collect as much personal data as they need for a particular purpose and must not collect excessive personal data;
- DPP 5 – SGBs may specify how long they will keep collected personal data;
- DPP 6 – SGBs may set out how individuals may access their personal data held by the SGB;
- DPP 7 – SGBs must only collect personal data in a secure manner. If personal data is collected online, SGBs must use secure servers and ensure that their websites are not susceptible to denial-of-service attacks. Collected personal data must also be retained by the SGB in a secure manner; and
- DPP 8 – if SGBs intend to send collected personal data to countries outwith the EEA, for example, for the purposes of entering their athletes into competitions, the SGBs must specify this at the time of data collection. This

information must include details of the countries to which such personal data may be sent and a confirmation of the fact that the SGB will take appropriate measures to protect the personal data post transfer.

The above information can be provided within a data protection statement on the online and offline forms on which individuals are required to provide their personal data. The statement can be included above the point at which the individual signs the form or clicks "I accept" or "Submit". In the online context, the data protection statement can be supplemented by an online privacy policy.

In order to ensure fair 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 data protection statement and must continue to process personal data for the purposes specified in that statement at the time of data collection;
- DPP 3 – SGBs must ensure that the personal data that 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;
- DPP 6 – SGBs must respect individuals' rights on an ongoing basis by providing access to personal data upon request;
- DPP 7 – 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; and
- DPP 8 – SGBs must continue to respect the DPA requirements on transfers of personal data outwith the EEA on an ongoing basis. This will link back to what the individuals were informed of at the time of data collection. Transfers may only take place to those countries of which the individuals were informed at the time of data collection.

In the event that an SGB wishes to use collected personal data for a different purpose that is not compatible with the purposes initially notified to the individuals in the data protection statement, then the SGB must provide a new data protection statement to the individuals concerned and give them an opportunity to object to any new processing purpose.

An SGB must keep an audit trail of the data protection statements which individuals have seen and accepted. This reduces the risk of using personal data for a purpose that is incompatible with the purposes notified to the individual.

Schedule 2 and 3 Grounds

In addition to providing the information contained in the data protection statement, the DPP 1 requires SGBs to justify their processing of personal data with reference to one or more of the grounds listed in schedule 2 to the DPA. One or more of the grounds listed in schedule 3 to the DPA must also be satisfied where an SGB is processing sensitive personal data.

Schedule 2 grounds include:

- the SGB has obtained the consent of the

individual to the processing of the personal data;

- the processing of the personal data is necessary for the performance of a contract to which the individual is a party or for taking steps at his/her request before entering a contract. This includes performance of the SGB's obligations under the contract of membership;
- the processing of the personal data is necessary for compliance with a legal obligation other than an obligation imposed by contract. This covers compliance with any conditions imposed by **sport**scotland or statutory requirements;
- the processing of the personal data is necessary to protect the vital interests of an individual. This covers situations where, for example, personal data requires to be disclosed by an SGB to third parties in life or death situations, such as disclosure of medical records to overseas doctors for treatment purposes in the event of athlete injury on the field of play; and
- the processing of the personal data is necessary for the purposes of the legitimate interests of the SGB or a third party to whom personal data is disclosed by the SGB and such processing is not unwarranted by reason of prejudice to the rights or freedoms or legitimate interests of the individuals concerned. If an SGB needs to use personal data for the purposes of its legitimate activities then the SGB may use the personal data, provided it is satisfied that any harm to the individuals concerned is minimal and justified by the SGB's legitimate interests in the use.

Schedule 3 grounds include:

- the SGB has obtained the individual's explicit consent to the processing of the personal data. Explicit consent is different to the consent required under schedule 2. The consent must be more informed in that the SGB should highlight the risks of the processing to the individual and the consequences of granting consent;
- the processing of the personal data is necessary for performing a legal obligation in connection with employment i.e. the SGB requires to use the personal data for the purposes of complying with its responsibilities under employment law;
- the processing of the personal data is necessary to protect the vital interests of the individual – this is similar to the schedule 2 ground;
- the processing of the personal data is necessary for legal proceedings in which the SGB is involved. These include proceedings in connection with athlete conduct / disciplinary issues and employment tribunal; and
- the personal data relates to racial or ethnic origin and is necessary for the SGB to monitor equal opportunities.

Collecting third party personal data

The collection of third party personal data refers to the situation where an individual provides the personal data of another individual to an SGB for and on behalf of that individual. Ensuring compliance with the DPA's fair processing requirements in this context can be challenging for SGBs. It is a high-risk data processing activity, involving considerable reliance by the SGB on the individual providing the personal data to furnish the individual subject of the personal data with the SGB's data protection statement to ensure the SGB's compliance with the DPA's fair processing requirements.

The SGB should require the data provider to confirm his / her capacity in these situations by,

for example, including an appropriate section on the form into which the personal data is inputted. In some situations, the SGB may require evidence of proof of relationship between the third party and the data provider, which may extend to the SGB contacting the third party for confirmation that the data provider has authority. This is particularly the case in guardianship situations. SGBs should also be prepared to handle objections to the processing of personal data from the subject of the personal data should the subject dispute the data provider's authority to act on his/her behalf.

Photography and videos

Photographs and video contain the sensitive personal data of the subjects of the image and the footage, as they invariably give rise to information regarding the religious beliefs and / or ethnic origin of the subject. The subject may be an athlete wearing a turban or a skull cap.

In order to process such personal data, SGBs should seek the explicit consent of individuals. A record of such explicit consent should be retained for audit trail purposes.

Personal data sharing between member clubs and SGBs

The key issue is whether the member club can share personal data with the SGB. This depends on the data protection statement that the member club has provided to its members and if this allows for such sharing. SGBs should therefore ask for a copy of any such data protection statement prior to engaging in such data sharing.

When the member club's personal data is transferred to the SGB, the SGB must provide the members with a data protection statement setting out the purposes for which it will process the members' personal data. This must be when the SGB first processes the personal data unless:

- provision of the data protection statement would involve a disproportionate effort; or
- processing by the SGB is necessary for compliance with a legal requirement to which it is subject.

Effective risk management

Data protection statements, both off and online, are key. SGBs must ensure that notices are future-proof. This involves the SGB thinking ahead about the purposes for which it will use the personal data. This is important because SGBs cannot exceed the scope of the fair processing notice.

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

Moreover, in the event that an individual objects to the processing of his / her personal by an SGB, the SGB must always respect and record such objections. The recording is important from the point of view of ensuring that personal data in respect of which an objection has been expressed is not reused by the SGB.

5. DATA RETENTION IN SPORT

WHAT YOU NEED TO KNOW ...

- Your SGB cannot hold personal data indefinitely and for longer than it needs to.
- The DPA does not set out how long personal data may be kept for.
- Your SGB must come to a view based on 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 may be considering implementing an electronic document management system (eDMS) involving the conversion of paper records into electronic form. While eDMS has obvious benefits, your SGB may experience difficulties in proving that an electronic version of a paper record is authentic and has not been altered in the conversion process.
- Your SGB should consider putting in place a records management plan and a 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 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 DPA 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 data controller, as follows:

- DPP 1: the data protection statement provided by the SGB could specify the period for which personal data will be retained;
- 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;

- DPP 6: SGBs should retain their records containing personal data in such a way that they can readily comply with their obligations under this principle efficiently. In other words, they can access their personal data and respond to subject access requests within the statutory 40 day timescale; and
- DPP 7: 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 DPA. SGBs may wish to retain such personal data in anonymous form, if possible, which would mitigate the risk associated with complying with the DPA;
- end of relationship – once an individual has withdrawn from membership of an SGB or is no longer an employee and is not actively involved in the sport, the SGB may wish to consider whether it is appropriate to continue holding on to 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).

Electronic Document Management Systems

Organisations are increasingly looking at ways of reducing their data footprint by converting paper records into electronic form by scanning and holding them within eDMS. The original paper record is often then destroyed.

While eDMS have the benefit of reducing the amount of physical personal data held and making paper records more accessible in digital format, SGBs may experience difficulties from an evidential point of view should such records be required for the purposes of any proceedings in which the SGBs are involved.

Generally, the courts require the "best evidence". In other words, the courts require the original document as proof of, for example, the existence of a contractual relationship between an SGB and one of its suppliers or members. If an SGB has implemented an eDMS and has disposed of the original document as part of that process, the SGB must prove to the court that the document on the eDMS is identical to the original and has not been altered in any way. In order to do so, the SGB may comply with the British Standards Institute Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. The Code describes how to prove that a digital image of a hard copy document is authentic and has not been tampered with since being converted into electronic form. Key to this is the maintenance and retention of detailed audit trails, which set out the complete life cycle of the document from when it was originally scanned into the eDMS, accessed by users of the eDMS and communicated to third parties by, for example, e-mail or other file-sharing facility. If an SGB is able to demonstrate that a scanned version of a signed paper membership application form is identical to the electronic version via the use of such audit trails then the courts will likely accept the eDMS version, although this is not absolute, as compliance with the Code only increases the evidential weight of the electronic document and is not conclusive in itself.

British Standard (1008) on Evidential Weight and Legal Admissibility of Electronic Information also contains similar provisions.

Records management

While the DPA, in particular DPP 5, does not require SGBs to do so, one means of managing the records of an SGB effectively is to have either or both of a records management plan and records management policy. While these are generally creatures of Freedom of Information legislation, both documents can be a useful internal guidance tool on the maintenance and destruction of an SGB's records.

A records management plan will set out: who is responsible for records management within the SGB; a mind map of the personal data held by the SGB; how audit trails are maintained by the SGB; the vital records held by the SGB which contain personal data essential for the operation and business continuity of the SGB; 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 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, an SGB may either archive or delete it.

Personal data should only be archived in the event that an SGB still needs it. This is because the DPA 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 data processor and the SGB, as data 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.

Data retention and risk management

If an 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 damage / distress to 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 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, an 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 retention policy in practice; and
- securely delete out-of-date or irrelevant personal data to reduce the risk of claims of DPA breach post personal data deletion.

6. SECURE DATA PROTECTION IN SPORT

WHAT YOU NEED TO KNOW ...

- Your SGB must put in place physical and technical measures to protect the personal data that it holds against certain risks, including 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.
- 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 7

The DPA requires SGBs, as data controllers of personal data that they process, to put in place "appropriate technical and organisational measures … 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 2014 edition – a relatively inexpensive security measure. A risk-managed approach should be adopted and SGBs should respond to specific risks that they have identified;
- nature of personal data to be protected: SGBs should accord more protection to sensitive 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;
- resulting harm which may arise from breach: if breach of the DPA 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;
- effectiveness of existing measures: if SGBs have experienced a DPA breach or an audit has identified weaknesses within the existing infrastructure then additional measures should be taken to secure personal data; and
- reliability of staff: the security of personal

data ultimately depends on those who process personal data on behalf of SGBs, including staff and contractors. SGBs must therefore demonstrate that they carry out sufficient due diligence on their staff and contractors relative to the role performed. For example, staff handling personal data relating to children and vulnerable adults must be subject to appropriate disclosure 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 top of the Information Commissioner's list when it comes to enforcement action against data controllers, with the largest fines to date being imposed in the data security context.

In order to mitigate the risks of breaching the DPA'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 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 "data security champions" 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 appropriate to their grade and involvement with personal data;
- restrict access to the network to authorised users only, who should have unique user names 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 damage or distress could be caused to individuals 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.

7. RIGHTS OF INDIVIDUALS

WHAT YOU NEED TO KNOW ...

- Your SGB must recognise the rights that individuals have against your SGB.
- In particular, your SGB must provide access to, and a copy of, any personal data that it holds on individuals upon the request of such individuals.
- Your SGB may charge an administration fee of up to £10 for dealing with requests and must respond within 40 days.
- Caution must be exercised to ensure that third party personal data is not inadvertently disclosed when responding to a subject access request.
- Your SGB should consider the exemptions from the subject access right contained within the DPA in order to restrict the disclosure of confidential commercial information from disclosure to the individual requestor.

The DPA confers a number of rights on individuals in relation to personal data held on them by SGBs, as data controller. The most important of these are the following.

An individual has a right, on making a request to an SGB, to be informed whether personal data of which he is the data subject is being processed by or on behalf of that SGB and, if so, the individual also has a right to:

- a description of the personal data held, the purposes for which it is being processed and the recipients or classes of recipients to whom the personal data may be or has been disclosed; and
- 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).

The DPA provides that, in order to meet these obligations, a copy of the personal data in

permanent form must be provided (for example, in hard copy or on disk).
A subject access request must:

- be addressed in writing to the SGB;
- 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 40 days from 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. SGBs may charge an administration fee (up to £10) for responding to a subject access request.

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 DPA provides that, if it is not possible to edit or delete the third-party data, the SGB need not comply with a subject access request unless the third party concerned has consented or it is reasonable in all the circumstances to comply without such consent. The DPA sets out a list of factors in assessing reasonableness in these circumstances, including:

- obligations of confidence owed by the SGB to the third parties;
- steps taken to obtain the third party's consent; and
- any express refusal of consent by the third party.

Where the third party personal data is confidential or sensitive, it is unlikely that disclosure will be reasonable.

The subject access right is subject to certain exemptions. These include, for example:

- the disclosure of confidential references – an SGB may exempt a reference that has provided in connection with an individual where that reference was given in relation to education, training, employment or to the appointment to an office;
- negotiations with the data subject – if an SGB is in negotiations with an individual in relation to the handling of a claim that the individual has made against an SGB, the SGB need not disclose personal data relating to that claim to the extent that disclosure would prejudice such negotiations; and
- management information – personal data relating to management planning and forecasting is exempt, provided that disclosure of that personal data would prejudice the SGB's activities.

SGBs must comply with their obligation to provide information in intelligible form by supplying the individual with a copy of the information in permanent form, unless the supply of such a copy is not possible or would involve "disproportionate effort". The requirement to provide the personal data in intelligible form does not require an SGB to simplify the personal data it holds or re-write it in a manner that is understandable; rather, an SGB is required to provide, for example, an index of acronyms or internal terminology to assist in understanding. An 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.

Individuals have a limited right to require an SGB not to process their personal data where such processing causes, or is likely to cause, the individual or anyone else unwarranted substantial damage or distress. This may be because an individual is concerned that an SGB's approach to data protection matters is likely to compromise the individual's personal data to his/her detriment due to, for example, inadequate data security.

Individuals also have a right to prevent processing of data for direct marketing purposes, even where consent has been previously given.

The DPA includes rights in relation to processing that involves automated decision-making. At any time by written notice, an individual may require an SGB to ensure that no decision significantly affecting him/her is based solely on the automated processing of his/her personal data for the purpose of evaluating matters relating to him (such as work performance, creditworthiness, reliability or conduct). An individual is entitled to be given an explanation as to how any automated decisions taken about him have been made. This right arises where any automated processing is the sole basis for a decision which significantly affects the individual. In this case, he will have the right to be informed by the SGB that the decision was made on that basis and to require the SGB to reconsider or take a new decision on another basis.

8. DATA 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 then that third party will be the data processor of such personal data for the purposes of the DPA.
- The DPA requires that your SGB enter into a written contract with the data processors imposing the DPP 7 data security requirements on the data processor.

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

The SGB must also enter into a written contract with the data processor which requires the SGB to act only on instructions from the data controller, and to comply with obligations equivalent to those DPP 7 imposes on the SGB with regard to security measures, outlined above.

9. INTERNATIONAL TRANSFERS OF PERSONAL DATA

WHAT YOU NEED TO KNOW ...

- Your SGB must comply with the requirements of DPP 8 when engaging in international transfers of personal data.
- It is likely that your SGB will be involved in international transfers of personal data when its athletes participate in international competitions.
- Uploading photographs to your SGB's website is an international transfer of personal data for the purposes of the DPA, provided that the website is accessible outwith the EEA.

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 staff contact details.

DPP 8 regulates transfers of personal data. Personal data must not be transferred to a country outwith the EEA 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. In almost 20 years of the underlying EU Data Protection law being in force, the European Commission has made few adequacy determinations. 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 EEA.

However, where the destination country does not ensure an adequate level of data protection, SGBs have a number of options. Firstly, they can either undertake a self-assessed determination of adequacy. This involves analysing the legal and regulatory regime in operation in the destination country and coming to a view as to whether there is adequate protection in place. This is a high-risk approach, as the analysis involved is complex and would ultimately require local solicitors to be engaged if it is to be undertaken appropriately.

Secondly, SGBs may enter into one of the model contracts approved by the European Commission or the ICO. These model contracts must be entered into as they are with no modifications.

Finally, SGBs may rely on one of the exemptions to DPP 8 contained within the DPA. These include, for example, where the individual has consented to the transfer – the data protection statement can be a useful means of obtaining consent in these circumstances.

10. CHILDREN AND DATA PROTECTION IN SPORT

WHAT YOU NEED TO KNOW ...

- While the DPA does not include specific rules in relation to handling children's personal data, your SGB must exercise caution in processing such personal data.
- 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 fair processing of such images in accordance with DPP 1, your SGB must be open and upfront within parent consent and data protection statements 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.
- In the event that a child seeks to enforce his / her DPA 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.

Fair processing and the first DPP

Fair processing under the first DPP 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 data protection statements, which is appropriate to the level of understanding of the target audience. This

involves SGBs in 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 data protection statement 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 and / or data protection statement. 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. Section 66 of the DPA provides that persons of 12 years of age and above are presumed to have general understanding to be able to exercise their DPA rights. On that basis, it is recommended that when SGBs deal with persons under the age of 12 in the course of their activities, they should seek explicit and verifiable parental consent. Persons between the age of 12 and 16 years are more aware, engaging and able to understand the consequences of their actions. But it is risky to assume that a person of 13 years of age automatically possesses sufficient capacity to make decisions on DPA 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 data 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 e-mail 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 e-mail to the parent and requests a response from the parent by e-mail;
- the SGB telephones 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 DPA applies to all photographing and filming carried out by or on behalf of SGBs, SGBs must seek the child and the parent's written consent to the capture of the child's images in this manner. The consent statement must comply with DPP 1, 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 requirements of DPP 7 have already been outlined, above. In order to comply with that principle in the children's 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, e-mail, e-mail 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 DPA rights

DPA rights 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 DPA rights on behalf of children.

In the event that a third party seeks to enforce DPA rights on behalf of the child, an SGB will require to obtain evidence of authority to act; otherwise, there is a risk that an SGB has failed to comply with DPP 6 in that it has not processed personal data in accordance with the rights of the child.

If a child seeks to enforce his / her rights against an 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 sensitive 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 his/her 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 Privacy and Electronic Communications (EC Directive) Regulations 2003 require that such communications must not be sent by an 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 data protection statement 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. Similar considerations regarding consent arise in this context as they do in connection with the requirements of the DPP 1. Parental consent may be necessary in order to comply with the requirements of the Regulations.

As noted above, the DPA 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.

11. ENFORCEMENTS, SANCTIONS & REMEDIES

WHAT YOU NEED TO KNOW ...

- An aggrieved individual may enforce the DPA 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 £500,000 for serious DPA breaches.
- The courts may award compensation to an aggrieved individual for breach of the DPA by your SGB.
- The DPA also creates a number of criminal offences of which individual officers and members of staff of your SGB could be guilty in the event that personal data is used in an inappropriate manner. This includes selling membership databases to a third party without the authority of the SGB.

The ICO is responsible for enforcing the DPA. The ICO will only intervene in the event that the individual is unable to obtain redress from the SGB. The individual may also enforce his/her rights against an SGB in the courts.

An individual has a right, where he believes himself/herself to be 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 DPA. 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 DPA, the ICO may serve an SGB with an enforcement notice, requiring the SGB to comply with the DPPs.

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 £500,000) for serious contraventions of the DPA. Before doing so, the ICO must be satisfied that the contravention was serious and was of a kind likely to cause substantial damage or substantial distress, and that the SGB either:

- deliberately contravened the DPA; and
- knew or ought to have known that there was a risk the contravention would occur, and that it would be likely to cause substantial damage or distress, but still failed to take reasonable steps to prevent it from happening.

Individuals are entitled to compensation from SGBs for damage or distress caused by any breach of the DPA. Compensation can only be awarded by the courts and not by the ICO. To date, very few claims for compensation have been made. Where actions have been brought, the courts have made it clear that compensation is only available to an individual who suffers damage by reason of a data controller's contravention of a DPA requirement. Where no damage is caused by that contravention, no compensation will be payable.

An individual can obtain a court order for the rectification, blocking, erasure or destruction of data held by an SGB which is inaccurate, and the court may also, where it considers it reasonably practicable, order an SGB to notify third parties to whom incorrect data has been passed of the rectification, blocking, erasure or destruction.

Breaches of certain rules give rise to criminal offences on the part of SGBs, for example, breach of the obligation to notify or inform the ICO of any changes to registerable particulars. It is also an offence to fail to comply with an information notice, an enforcement notice or knowingly to make a false statement in response to an information notice.

The knowing or reckless obtaining or disclosure of personal data without the consent of an SGB is, subject to certain limited defences, an offence, as is selling or offering to sell data so obtained or disclosed. This would occur where, for example, an employee leaves an SGB and proceeds to sell the personal data of members of the SGB (without the SGB's consent) to a third party to be used by that third party for its own purposes. A new offence, that of enforced subject access, will come into force later in 2015. This applies where an SGB requires, as a condition of employment, prospective employees to provide the SGB with a copy of their criminal records by making a subject access request to the Police.

Aside from legal sanctions, failure to comply with the DPA 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.

12. EXEMPTIONS

WHAT YOU NEED TO KNOW ...

- The DPA 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 DPA contains a number of exemptions from the DPPs and other parts of the DPA, 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.

Harper Macleod LLP

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