DATA PROTECTION

Information for Clubs & County Associations

July 2018

ENGLAND squash

Data Protection Guidance Note

This guidance note gives an overview of how the General Data Protection Regulation 2016 ("GDPR") and the Data Protection Act 2018 (together, the "Privacy Laws") apply to clubs and county associations. It also suggests a series of steps to be taken to help them comply with these laws.

By way of background, the GDPR, an EU wide data privacy regulation, came into force on 25 May 2018 and repealed the UK Data Protection Act 1988. In parallel to the GDPR, the UK government passed the new Data Protection Act 2018 which essentially adopts the same standards as the GDPR. It also modifies and supplements certain aspects of the GDPR which Member States are permitted to under GDPR.

Key Elements

The Privacy Laws

- Regulate the way personal data is processed by both data controllers and data processors
- Provides stronger protection for special categories of personal data and criminal convictions and offences related data
- Requires data controllers to comply with seven key data protection principles
- Requires certain organisations to pay a fee to the Information Commissioner's Office ("ICO") in respect of their processing of personal data
- Requires some organisations to appoint a Data Protection Officer
- Gives broader rights to individuals to whom the personal data relates (data subjects)
- Increases the potential fines applicable to data protection breaches

Most clubs and county associations will be processing personal information relating to their members, customers, employees, suppliers etc. and will therefore need to comply with the Privacy Laws.

In addition to the guidance set out in this note, England Squash recommends that clubs and county associations read the helpful guidance provided by the ICO, the independent authority set up to uphold data protection laws in this country. The ICO's website can be found here: http://www.ico.org.uk.

Personal data
The definition of personal data is now broader under the new Privacy Laws. Personal data means any data relating to an identifiable natural person who can be directly or indirectly identified, in particular by reference to an "identifier". These "identifiers" cover the types of information one would expect to be personal data (e.g. name, email address, contact information etc.) and now also include things such as location data and online IDs (such as IP addresses and cookies).

Processing
"Processing" covers virtually any use which can be made of personal data e.g. collecting, storing, using and destroying it.

Data controllers and data processors
A data controller determines the purposes for which, and the manner in which, any personal data are processed. A data processor on the other hand, processes personal data strictly in accordance with the instructions of a data controller.

It is possible that an organisation can act both as data controller and a data processor in different contexts. It is also possible that two organisations can act as data controllers in relation to the same data. It is important to note that unlike under the previous data protection regime (Data Protection Act 1998), data processors are now directly responsible for certain obligations under the Privacy Laws and can therefore be subject to enforcement and penalties, and data subjects may also bring claims directly against a processor.

Special categories of personal data
These types of data were previously referred to as "sensitive data" and consist of information relating to the racial or ethnic origin of a data subject, his/her political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data and data about an individual's health, sex life, or sexual orientation.

Clubs and county associations can only collect and use special categories of personal data (e.g. in respect of special dietary needs, health declarations on booking forms etc.) where additional criteria have been fulfilled. The most straightforward means to ensure compliance is to obtain the individual's consent before collecting their data. This can be done via a consent capture included within the data protection notice referred to below. Please also see the section below on consent requirements.

Criminal convictions and offences data
The processing of this type of data was previously dealt with in the same way as sensitive data under the Data Protection Act 1998.

Separate rules now apply to this type of data, which require both a processing condition to be met (as referred to below in respect of "lawfulness, transparency and fairness") and either the processing to be carried out under the control of an official authority (e.g. the police) or, in respect of clubs and county associations (e.g. DBS checks relating to coaching candidates), where the processing is permitted under Member State law.

In this regard, the Data Protection Act 2018 sets out the grounds for which this data may be processed and sets out certain protections which must be put in place. This might require the implementation of what is termed an "appropriate policy", setting out, amongst other things, how the club or county association will ensure compliance with the data protection principles when processing this data. For the duration of the processing of the data, and for six months thereafter, the club or county association must also ensure the policy is retained, reviewed and kept up to date and made available to this ICO if requested.

The seven data protection principles

Data controllers must comply with the seven key data protection principles listed below, whenever they are processing personal data.

1. **Lawfulness, transparency and fairness** – requires a data controller to:
    a. satisfy at least one "processing condition" when processing personal data. These include explicit consent, necessity for performance of a contract with the data subject, necessary for compliance with a legal obligation, or necessary for a legitimate interest. The relevant processing condition will need to be explained to the data subject (which can be done in a privacy policy).
    b. There is an additional list of "processing conditions" for special categories of personal data (as referred to above in this note). These are far more restrictive than for other types of personal data, and in most instances, will require explicit consent.
    c. An increased amount of information needs to be given to data subjects, and this must be presented in a clear and concise manner and be appropriate for the specific audience. Ordinarily, this information would be included within an online privacy policy or hard copy privacy notice put up in a clubhouse for example.
2. **Purpose Limitation** – personal data should be collected for specific, explicit, legitimate purposes and shouldn't be processed in a manner incompatible with those purposes.
3. **Data Minimisation** – personal data should be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.
4. **Accuracy** – personal data must be accurate, up to date and amended or deleted if it is not.
5. **Storage Limitation** – personal data must be retained for no longer than is necessary to achieve the purposes for which it was collected.
6. **Integrity and Confidentiality** – personal data should be stored in a secure and confidential way. Data breaches will need to be reported to the ICO as soon as the controller is aware and no later than 72 hours after the breach, unless it can be demonstrated that the breach is unlikely to result in risk to individual. If the breach is likely to result in high risk to individual, the individual must be notified without undue delay.
7. **Accountability** – data controllers must continuously assess risk, implement appropriate policies and procedures and keep them under review as to their suitability and effectiveness.

In addition to these key principles, there are other obligations which need to be complied with in different circumstances. These relate to, without limitation, record keeping, data subject rights, overseas transfers of personal data and engaging third parties to process data.

The Privacy Laws also require data protection compliance to be a fundamental part of the design of any systems, products and services which process personal data, as well as throughout the duration of such processing activities. Controllers are also required to implement technical and organisation measures to ensure that, as a standard, only personal data necessary for the processing purposes are processed e.g. internal training, encryption methods, robust policies and procedures.

Consent
Consent is much harder to obtain lawfully under the new Privacy Laws. The new laws require consent to be "unbundled" (so separately obtained for different uses of data), given freely and on an informed basis and with an affirmative action (such as a signature or an opt-in tick box). Pre-ticked consent boxes are expressly prohibited under the Privacy Laws. The individual also has the right, in most circumstances, to withdraw their consent and this right must be made clear to the individual at the time of collecting the consent. Children under 13 cannot give consent for online services and will always need parental or guardian consent.

For marketing purposes, an individual's explicit consent is required. As expected, marketing covers the sale of products and services but also the promotion of aims and ideals. This means that the rules around consent for marketing will cover not only commercial organisations but also not-for-profit organisations. On such basis, it is best practice for clubs and counties to obtain the consent of individuals before marketing (via phone, SMS or email), even if the relevant communication is not actively promoting goods or services but rather latest news or updates. Individuals should also be given an easy way to opt-out of such communications on each occasion and if an individual decides to opt-out, they should be promptly removed from the relevant marketing list.

If the organisation wishes to share personal data with third parties for the purpose of that third party's own marketing (such as a local sponsor), it will need to disclose the specific names of those organisations when seeking the individual's consent.

Notification to the ICO/payment of fees
The Data Protection Act 1998 required controllers to have an ICO notification, which required the payment of an annual fee and an online confirmation of the processing activities of the relevant organisation.

This process has been changed under the new laws. The obligation to pay a fee to the ICO is now set out in the Data Protection (Charges and Information) Regulations 2018 and this obligation replaces the requirement for data controllers to notify ICO of their data processing activities.

There are three tiers of annual fees, which aim to reflect the risk profiles associated with different types of processing activities. Certain exemptions do apply, so if the club or county is unsure whether it is required to pay (or how much it might be required to pay), the ICO has a helpful self-assessment tool which can be found here: https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

If the organisation currently has a data controller notification in place, the obligation to pay does not apply until the notification expires. The ICO will write to the organisation before this expires to confirm what is required. The ICO will use the information which they currently hold on the organisation to decide what tier applies. If the organisation disagrees with the assessment, it must contact the ICO.

If the notification has recently expired, the ICO will deem the organisation to fall within the highest fee tier, unless the organisation confirms otherwise.

If the club or county has never previously registered with the ICO, it will need to do so using the following link: https://ico.org.uk/registration/new

It is important to pay the fee to avoid ICO fines (which can be up to £4,350).

Data protection officers (DPO)
An organisation (whether a processor or controller) is required to appoint a DPO if it:

- Is a public authority or body; or
- Undertakes regular and systematic monitoring of individuals on a large scale; or
- Processes sensitive categories of data on a large scale; or
- Processes data relating to criminal convictions/offences; or
- Considers appointing a DPO is necessary following its own internal risk assessments.

A DPO must have expert data protection knowledge (with reference to the type and complexity of processing carried out by the organisation) and must act independently (although it can be an internal appointment).

Data Subject rights
Several data subject rights existed under the old regime but are simply being enhanced under the new laws, including subject access requests, the right for data to be corrected and the right to object to direct marketing.

There are a few new rights being introduced, namely:

i. the right to be "forgotten" (requiring organisations, when requested, to delete data which is being processed unlawfully);

ii. the right to restrict processing (meaning the controller cannot process the data further until the individual has explicitly consented or other limited exemptions apply);

iii. the right to object to certain other types of processing, including processing based on legitimate interests of the controller; and

iv. data portability, which requires the controller to be able to transfer personal data to the individual in a commonly used and machine readable format so it can be transferred to another controller (or where practical, directly from one controller to another).

The administration involved in dealing with data subject requests is likely to increase, particularly given that organisations will now have one month (in most cases) to respond to the relevant request rather than the previous 40-day period. Therefore, it is crucial to start thinking about how these new deadlines will be met within the organisation. England Squash would recommend clubs and country associations familiarising themselves with the new framework relating to individual rights and putting in place practical policies for dealing with any requests.

Disciplinary Cases
Where personal data is being used in the context of a disciplinary hearing or procedure, the same data protection principles set out above shall also apply. Importantly, clubs and county associations will need to establish a lawful ground for processing personal data used as part of such hearing or procedure.

Where the personal data is not classed as "special category" data, this will most likely be the legitimate interests of the relevant club or country association (but will need to be assessed on a case by case basis). Where special category data or data relating to criminal convictions and offences is relevant, additional conditions will need to be met (which may include putting in place an appropriate policy to deal with such processing, as referred to above in the "criminal convictions and offences data" section), and an additional processing ground must be established. This might include the new "standard of behaviour in sport" condition (which relates to the protection of integrity in sport, and which can be found in the Data Protection Act 2018, Schedule 1, Part 2, paragraph 28 www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted) or where the processing is necessary for the establishment, exercise or defence of legal claims.

Seven practical steps towards compliance

1 **ALLOCATE** responsibility within your organisation

Compliance responsibilities will naturally fall to those officers, staff and volunteers of clubs and county associations who come into contact with personal data such as: the club secretary; membership secretary; webmaster; bookings officer and the events secretary. It's suggested that where a formal DPO appointment is not required, that clubs and county associations designate an appropriate individual or group of individuals to assist their club or county association with data protection compliance.

2 Decide whether your organisation needs to **PAY A FEE** to the ICO.

3 **AUDIT** forms, IT systems, website, internal processes and agreements.

It is helpful to undertake an internal data audit, which broadly seeks to identify exactly what personal data your organisation holds across all functions of the business (e.g. HR, finance, members, coaches, suppliers, business contacts etc.) and the methods used for collection (e.g. membership applications, entry forms, staff contracts, website enquiries, CCTV), what the data is used for, where the data is stored, who it is shared with, and what legal grounds are relied upon for processing the data. This process should also identify any data which is no longer relevant or is out of date.

4 **IMPLEMENT** outcomes of audit.

This might involve:

1. Updating your organisation's privacy policy, to set out details of your processing activities in line with the information requirements under the Privacy Laws.

2. On forms where data is collected, draw attention to the privacy policy and make a copy easily accessible. We set out below an example data capture form which could be used on a membership application form:

EXAMPLE DATA PROTECTION NOTICE

The information which you provide in this form and any other information obtained or provided during the course of your application for membership will be used solely for the purpose of processing your application and if elected to membership, dealing with you as a member of [insert name of club]. Your information will be handled in accordance with our privacy policy which can be found here – [INSERT LINK]. Please note that the information you have provided will be shared with certain third parties listed in our privacy policy, including England Squash, the governing body for squash in England, for the purpose of enabling England Squash to activate and manage your England Squash membership.

Your data will not be shared with any third party for marketing or commercial purposes without firstly obtaining your explicit consent.

If you give your consent below we will include your contact details in our membership handbook which will be available to all members. You will be able to withdraw your consent at any time by contacting us.

☐ *I am happy for my contact details to be included in the [insert name of club] membership handbook*

- Additional consent opt-ins may be required for optional data sharing with third parties for marketing purposes (as referred to above in respect of "consent") or where you are collecting special categories of personal.
- Implement internal policies relating to data retention/deletion, data breach reporting, security (including in respect of staff devices) and the handling of data subject requests.
- Reviewing and updating staff contracts and staff handbook (if applicable
- Implementing or updating contracts with suppliers who process personal data on your organisation's behalf to ensure the data provisions are compliant.

5 **CLEANSE** from your organisation's systems any data which is no longer needed or is inaccurate.

6 **TRAIN** officers, staff and volunteers on how to handle personal data in accordance with the new laws.

7 **THINK DATA PROTECTION** for all new initiatives to ensure you understand what risks are involved from a data protection perspective and how to comply with the new laws in relation to such initiatives.

Penalties
Finally, it is important to mention penalties.

The potential penalties under the Privacy Laws have significantly increased from those under the Data protection Act 1998:

- €10,000,000 or, if an undertaking, up to 2% of total worldwide annual turnover of the preceding financial year (whichever is higher). This applies to breaches which are less serious in nature, for example failure to put in place an adequate processor agreement or to implement appropriate technical and organisational measures appropriate to the risk.
- €20,000,000 or, if an undertaking, up to 4% of total worldwide annual turnover of the preceding financial year (whichever is higher). This is reserved for more serious breaches of the fundamental principles of data protection, but does cover a significant number of the obligations set out in the Privacy Laws, including a breach of the data protection principles and data subject rights.

In the event of any breach, factors such as the severity and scale of the breach, whether the breach was intentional, whether the infringer has co-operated with the ICO and whether there was any financial gain from the breach will certainly be considered.

Businesses which carry out "high-risk" processing activities (e.g. call centres and direct marketing companies) will most likely be the target of any ICO enforcement action and large-scale fines. However, clubs and county associations should still think carefully about compliance, not least from a reputational point of view.