GDPR Guidance

ENGLAND HOCKEY

The General Data Protection Regulations (GDPR) will come into effect on 25 May 2018 to replace the Data Protection Act 1998 (DPA). Compliance is mandatory for all clubs and associations including committees and working groups (hereinafter referred to as 'clubs') in their capacity as either data controllers[1] and/or data processors[2] and applies to all personal data (electronic and hard copy).

**This document is intended to assist by providing a brief overview of Clubs' immediate and future obligations under GDPR. Further reference must be made to the GDPR, ICO guidance[3] and approved Sports Recreation Alliance (SRA) templates*

In simple terms:

- **Review the data held and conduct a compliance risk assessment[4] - what do you hold and why?**
- **Tell members what you are doing with their data**
- **Get their consent to use if for each purpose other than essential use to make the activity happen**
- **Keep their data secure**
- **Delete their data when you no longer need it**

TOP TIPS TO PREPARE FOR GDPR

Process: understand the journey that personal data takes through your club. What information do you collect and is it necessary? What do you tell people when you collect it? On what legal basis have you collected it[5]? Where and how do you store that data? What do you do with it? When is it deleted? This will allow you to identify any areas of risk.

Awareness: ensure that all persons responsible for the collection, processing or storage of data are aware of the changes (including third parties) and know who to speak to should they receive a subject access request[6] (SAR) or in the event of a breach.

Policy: ensure policies and procedures are in place to reflect the changes under GDPR.

Communication: Transparency is key. Make sure you tell people at the point of collection, why you are collecting their data, what you intend to do with it and when it will be deleted. Review consents currently relied upon. Confirm with all parties including third parties that they are GDPR complaint.

---

[1] Those who control and own the data
[2] Anyone who processes data on behalf of a data controller
[3] Including but not exclusively '12 Steps' and 'Getting Ready for the GDPR'
[4] SRA Compliance Questionnaire is a useful tool
[5] You may wish to consider 'Consent' and 'Legitimate interest' but further reference should be made to the ICO Guidance
[6] See EH FAQs at Enclosure 1

DATA PROTECTION PRINCIPLES (largely unchanged from the DPA 1998 making transition easier):

Data must be:

- Used fairly and lawfully
- Used for limited and for specified circumstances
- Used in a way that is adequate, relevant and not excessive
- Accurate
- Kept for no longer than absolutely necessary
- Handled according to people's data protection rights
- Kept safe and secure
- Not transferred outside the European Economic Area (EEA) without adequate protection

KEY CONSIDERATIONS:

Data processing: People will require more information when collecting data (see '**process'** above). This should be set out clearly in your Privacy Notice (see link for England Hockey approved template). Approved partners (Club Buzz, Pitchero, SportLomo and Teamer) will be taking steps to ensure GDPR compliance. You must check that unapproved systems are GDPR compliant e.g. organisations appointed to run Club websites. For assistance in drafting contracts with businesses you may send out your data to, see link for the SRA Data Processing Agreements template. You must make people aware of where you will be sending their data and seek their '*consent*' to do so.

Providing you are using people's personal data in a way that is consistent with the running of the Club e.g. sharing phone numbers with captains, keeping records of red and yellow cards etc., this is a '*legitimate interest'* and should not present any data protection issues providing that this is set out clearly in a Privacy Notice when they join, which they have access to. Should you wish to use their data in a way which is not in the '*legitimate interest'* of running the Club e.g. for marketing emails for sponsors, explicit, positively given '*consent'* for a specified purpose must be given.

- **Consent must be explicit, positively given for each separate use and expressed in simple easy to understand terms, avoiding legal jargon. Consent can be refused and can be withdrawn at any time**

Data storage: Stored data must be accurate and securely stored. For electronic data (Word documents and Excel spreadsheets) you may wish to consider encryption if not held on a secure system, particularly if you are sending this data around your club.

- **People's right to rectification of data can be exercised at any time and must be actioned within 1 month**
- **Individuals can also request information held about them in the form of an SAR, which must be actioned within 1 calendar month and cannot be charged for[7].**

Data retention: Data must be stored for no longer than is necessary.

- **People's right of erasure of data can be exercised at any time**

[7] See GDPR guidance for exceptions. Be aware of exemptions from disclosure.

Data breach: The ICO must be notified of a data breach (including loss of any personal data) within 72 hours, notifying the ICO of the nature and extent of the breach, likely consequences and measures taken or to be taken. Careful consideration must be given as to whether the individual should be informed and only where there is a high risk to the rights and freedoms of the individual should this be done (this consideration and the decision should be recorded).

Children: Children **under the age of 13** must have a parent or guardian consent on their behalf. Privacy Notices for children should be set out in simple, plain English.[8] Please see link for Sport and Recreation Alliance's Child Friendly Privacy Notice template.

Special category data and criminal convictions: Particular care must be taken when processing and storing such data, as there are additional measures to be taken[9]. Special category data is for example information about a person's race, politics, sexual life etc.[10]. Advice should be sought if unsure.

Failure to comply: The fines have increased and breaches could result in a fine (at the highest end) of in excess of 20Million EUROS or 2% of your global annual turnover.

Of note: you will no longer be required to register with the ICO as a data controller.

ENCLOSURE:

1. Frequently Asked Questions

[8] The Data Protection Bill states that Children over the age of 13 do not require consent of a parent or guardian. However, the Data Protection Bill is yet to be passed. Therefore continual reference to the ICO Guidance must be made to ensure currency and compliance.
[9] Direct reference should be made to ICO Guidance when processing such data.
[10] A full list can be found in the GDPR.