DATA PROTECTION GUIDANCE

This briefing note provides advice and guidance for tennis venues in complying with the data protection legislation when collecting and using personal data.

LTA TENNIS FOR BRITAIN

DATA PROTECTION GUIDANCE FOR TENNIS VENUES

The General Data Protection Regulation (GDPR) took effect across the EU on 25 May 2018 and was retained in UK law following Brexit as the UK GDPR. It, along with the Data Protection Act 2018, sets out the legal and regulatory framework for the safeguarding of personal data that all organisations much comply with regardless of their size.

Tennis venues hold and use the personal data of individuals (mainly details of their members, customers, employees, and volunteers such as their names, addresses, phone numbers, email addresses and dates of birth). Organisations that hold personal data and are the main decision makers of how that personal data is used are known as **data controllers**.

Under data protection legislation individuals have certain rights which must be observed by tennis venues.

This guidance note along with the FAQs note looks at what all venues should be doing in order to comply with their obligations under data protection legislation.

Do I need to register as a data controller?

Under data protection legislation not all organisations are required to register with the body that administers data protection compliance in the UK (the Information Commissioner's Office or ICO). Registration used to be mandatory, but this was abolished by the UK GDPR however organisations that are not exempt still have to pay a "data protection fee" to help to fund the work of the ICO. For details about how the fee is calculated, how you pay the fee, or whether you are exempt, you should look at guidance set out on relevant pages of the ICO's website.

Identify a compliance lead within your venue

Certain types of organisations will need to appoint a Data Protection Officer (("DPO") see section below). Although this is unlikely to affect most tennis venues, you should make sure you identify a compliance lead or team who can take responsibility for your compliance with data protection legislation.

Make use of the ICO guidance

A key role of the ICO is to educate data controllers as to their data protection obligations. We suggest that all data controllers should keep up to speed with guidance from the ICO, made available on its website. You are likely to find the following guidance particularly helpful:

- Guide to the General Data Protection Regulation (GDPR);
- Data Protection Self-Assessment; and
- Right to access personal data.

Map out your venues personal data usage

The first step in ensuring compliance with data protection legislation is to map out what personal data you are collecting, where you are collecting it from, how and why you use such personal data and who do you share it with. This should be information that a club secretary, or someone who knows the whole organisation reasonably well, is

aware of. We suggest using the **Data Protection Map/Audit template** to assist you in carrying out this exercise.

You should also address questions such as:

- **On what types of individuals do you hold and process information?** Staff, members, players, volunteers, suppliers and so on.

- **What nature of information do you hold on individuals? Where does it come from? What do you use it for?** This will vary according to the category of individual. Particular care is needed around health data relating to players or staff and criminal records information.

- **Are those individuals aware of what you are doing with their data, most obviously through a privacy policy or notices when their data is collected?**

- **Do you share personal data with any third parties? If so, what do they use it for, and again do the individuals know?**

You will be expected to know the answers to these questions, and more, when asked by either the ICO or an individual whose personal data you hold.

Identify gaps in your knowledge and areas of vulnerability

This should follow naturally after completing the mapping exercise set out above because, once undertaken, it will probably point to remedial steps or the need to seek advice from appropriate professionals. However, it is far better to know how and where you are exposed so that you can take steps to increase your knowledge and resolve the issues that become apparent.

Key concepts

The following are key concepts that you should be aware of:

- **Transparency:** Venues should provide information about how they shall use personal data as soon as its first collected from such individuals or from other sources. For example, the venue will need to tell individuals about their data subject rights, their right to withdraw consent; and provide information about data retention. Privacy policies should be brought clearly to the attention of players, members and other individuals whose data is processed (i.e. used) by the venue.

- **Consents from individuals for using their personal data for marketing purposes:** Any club which makes use of customer and member lists for direct marketing and/or fundraising should continually review the method for obtaining consent and the validity of consents that have previously been obtained. The ICO take a rigorous approach to parties who carry out incompliant direct marketing with plenty of fines issued since May 2018. For consent to be valid it must be freely given, specific and informed and it cannot be collected in an ambiguous fashion (via a pre-ticked box).

- **Processing or using personal data:** You can only use an individual's personal data if you have a "lawful basis" for doing so. There are six available lawful bases for processing, these are:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

No single basis is 'better' or more important than the others. You must determine your lawful basis before you begin processing, and you should document it. The ICO have a helpful interactive tool on their website that can assist you with determining which lawful basis you should be relying on for each particular purpose that you need to process personal data for.

- **Data Subject access rights:** One right that each individual has, is the right to request copies of the data you hold on them. Whilst this is only one of many rights available to individuals under data protection legislation, it is the one that is most often relied upon, and you should consider enacting a procedure for dealing with such requests. The time frame within which you are required to respond is one month and you are not permitted to charge an individual for this information.

- **Accountability**: You should be able to demonstrate your compliance with the data protection principles. Keeping records of privacy policies, data processing agreements, data sharing agreements, data audit/mapping documents as well as copies of any documentation used to collect consents from individuals is important.

- **Security breaches**: A data security breach (such as actual or potential loss, corruption or theft of data) must be reported to the ICO within 72 hours of you becoming aware of it. Where the breach is likely to present a high risk to particular individuals, they should be notified directly. You should develop and maintain good data security systems and practices as a priority.

- **Data processors**: Where you enlist the services of a third party and as a part of such service the third-party processes data on your behalf (e.g. a payroll services provider) you will need to ensure that the service terms/agreement contains certain provisions to ensure that the personal data shared if provided with sufficient protection by the third party. If you have not entered into a written

agreement, or the agreement does not contain terms detailing the sharing of personal data, you should enter into a specific data processing agreement with the third party on the basis of the template made available on our website.

- **Sanctions and enforcement:** The fines/sanctions that can be imposed by the ICO for noncompliance with data protection legislation are significant – the ICO's maximum fining powers are £17.5 million or 4% of an organisation's global turnover. Whilst the ICO has stated that such fines will be used proportionately, and so far, this has been the case, the potential liabilities that Venues may face for non-compliance means that ensuring and maintaining compliance should be a priority.