CLUB DEVELOPMENT

GDPR Guidance (January 2018)

This briefing note provides advice and guidance for tennis venues in complying with the GDPR changes that will affect how venues collect and use data.

LTA BRITISH TENNIS

GDPR Guidance for Tennis Venues

The General Data Protection Regulation (GDPR) will take effect in the UK, and across the EU, on 25 May 2018. The GDPR and existing data protection law applies to organisations regardless of size. The basic structure of data protection law will remain the same after May 2018 however the introduction of the GDPR has implications for tennis venues of all sizes and structures.

Tennis venues hold and use the personal data of individuals (mainly details of their members and employees i.e. names, addresses, phone number, email address, date of birth). Organisations that hold personal data and use and determine how this data is used are known as '***data controllers***'.

Individuals will continue to have rights which must be observed by tennis venues (as data controllers). However the compliance burden will increase significantly and venues should prepare themselves for this prior to 25 May 2018.

This guidance note looks at what all venues should be doing now, as a minimum, and the changes that venues may need to make in order to comply with the GDPR.

1. Do I need to register as a data controller?

Under current data protection legislation some organisations were required to register with the body that administers data protection law in the UK (Information Commissioner's Office or ICO). Registration will be abolished by GDPR but organisations will still have to pay a fee – to help to fund the work of the ICO. Some exemptions are likely to continue to apply. The fee structure and the process for how the fee is paid are yet to be finalised. You should look at the ICO website for updates regarding this. If you are currently registered and are due to renew, you should do so until the new system comes into place. Even if you are exempt from the new fee, you must still comply with the GDPR.

2. Identify a compliance lead within your venue

Certain types of organisation 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 your management team is aware of the venue's data protection obligations and that this is a significant compliance issue which requires careful attention and resources. This applies both now, in preparation for the change, and going forward.

3. Act now, don't wait!

There is no grace period after May 2018 and the ICO have been taking a harder line in enforcement and emphasising the rights of the individual, so don't delay in beginning to address these changes.

4. Do not get distracted by Brexit

The GDPR will come into force in the UK and across Europe in May 2018 and it is not expected that the UK will make any substantial changes when the UK leaves the EU.

5. 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, available on its website (ico.org.uk: **here**).

- ***Existing Guidance***: There is a helpful two-page GDPR summary called '***12 steps to take now'***, and a longer overview document on the ICO website.

- ***Programme of Future Guidance:*** The ICO has given some indications of further guidance which data controllers can expect to see. The ICO has added a page to its website called '***Guidance: what to expect and when'***, which it has promised to update as new GDPR guidance is planned and published by the ICO and by other bodies.

6. Auditing your venues personal data usage

It is recommended that your venue conducts a 'mini-audit' of the personal data that your venue holds and uses, and why. This is something that a club secretary, or someone who knows the whole organisation reasonably well, could prepare. We suggest logging audit results in a matrix, which can then act as a reference document for any compliance efforts. The LTA have produced a ***GDPR Data Audit template*** that can assist you in carrying out this audit. In the audit you should address questions such as:

- ***On what types of individual 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?*** If you are relying on consents, how did you obtain them? What form of wording was used? Will those consents be valid under the GDPR?

- ***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 either the ICO asks or an individual who you hold data on asks.

7. Identify gaps in your knowledge & areas of vulnerability

Much of this should follow naturally from a mini-audit / review: once undertaken, it will probably point to remedial steps or seeking advice from appropriate professionals, but at least you will have a clearer idea of where the key threats to your venue lie.

8. Watch out for & get to grips with key changes

The following are new or changing concepts you will need to get used to:

- ***Transparency*:** Venues will need to provide much fuller information when they first collect personal data from 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 will need to be substantially upgraded and should be brought clearly to the attention of existing players, members and other individuals whose data is processed (i.e. used) by the venue.

- ***Consents from individuals for using their personal data - tougher rules***: Any club which makes use of customer and member lists for direct marketing and/or fundraising should plan on reviewing (and quite possibly upgrading) consents, wherever it relies on them, over the remaining period up to May 2018. The ICO are taking a more rigorous approach to enforcement of existing rules with fines issued to leading charities for fundraising practices and to major retailers for their direct marketing to customers. For example, opt-in consent is likely to be needed for email direct marketing and real care is needed over any 'prospecting' of potential members or supporters.

- ***Processing or using personal data without consent*:** tougher rules will apply here too. You can in some circumstances use an individual's personal data without gaining their consent to do this. You must have what is called a "legitimate interest" to do this. If what you are doing is broadly reasonable having regard to the individual's interests, legitimate interests may be available and allow you to avoid seeking consent, if you provide clear information to the individual, most obviously through a privacy policy. This is a complex area and care should be taken before using personal data without the individual's consent.

- ***Subject access rights (and other new or expanded rights)*:** the period for compliance with an individual's right to request copies of the data you hold on them will be reduced from 40 days to one month. You will no longer be able to charge an individual for this.

- ***Accountability***: You will have to be able to demonstrate your compliance with the data protection principles. Keeping records of privacy policies and consent language and procedures will be important.

- ***Security breaches***: The general rule will be that 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. And where the breach is likely to present a high risk to particular individuals, they should be notified directly. You should develop good data security systems and practices as a priority.

- ***Data processors***: Where you sub-contract data processing out to a third party (e.g. a payroll services provider or even a volunteer), care is needed –you need to be confident they will hold your data securely and you also need contract guarantees from them.

- ***Data Protection Officers:*** GDPR requires organisations engaged in more complex data processing (particularly of for example health data) to appoint a data protection officer with specific responsibilities (and skills). This is unlikely to be necessary for most tennis venues but should be checked.

- ***Sanctions and enforcement***: Sanctions under GDPR will be increased - including raising the

ICO's current maximum fining powers from £500,000 to a maximum 20 million euros or four per cent of annual global turnover, whichever is higher. However, the ICO has stated that fines will be used proportionately.

This note is a general summary of the law. It should not replace legal advice tailored to your specific circumstances.