Guidance to Clubs on the Data Protection Act

February 2013 (updated October 2015)

This is part of the RT2020 initiative by the T&RA to help clubs with relevant legislation. All organisations that collect personal data must comply with the law on how data is handled. Real Tennis clubs collect personal data from their members (and employees and sub-contractors) and it is important that clubs are aware of their responsibilities.

The Data Protection Act 1998 (DPA) places a number of obligations on organisations which process personal data. In particular, it regulates how an individual's personal information is processed and protects people from misuse of their personal details.

The definition of personal data is wide; it covers any information through which a person is identifiable. It will include name, address, date of birth etc.

The definition of processing is also quite wide and it covers almost anything you might do with personal data including organising, amending, retrieving, consulting, using, disclosing, deleting and storing it.

There are three main elements to the DPA:

1. Notification - each organisation processing personal data must, subject to certain exemptions, register with the Information Commissioner each year. This is called "notification".

2. Data Protection Principles - each organisation processing personal data must comply with the eight data protection principles:

1. fairly and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;
4. accurate;
5. not kept longer than necessary;
6. processed in accordance with your rights;
7. kept secure; and
8. not transferred abroad without adequate protection.

3. Data Subject Rights – individuals have rights, principally the right of access to the data held about them.

1. NOTIFICATION

The T&RA is exempt from registration as it is a non-for-profit organisation; however, it is still required to be compliant in all other respects. Clubs must check themselves whether they are required to register with the Information Commissioner's Office (ICO). If the club processes any personal data on computer, it may be required to register unless an exemption applies. Failure to notify if required to do so is a criminal offence.

Clubs should consult the ICO's website at www.ico.org.uk which contains a useful online self-assessment guide, or contact the notification helpline on 0303 123 1113 or 01625 545745. Notification is a fairly simple but quite time-consuming process which costs £35 per year. Once notified, notifications must be kept up to date.

Please note that even if you don't need to notify, you still need to comply with the rest of the DPA.

2. DATA PROTECTION PRINCIPLES

Rather than deal with each of the eight Principles, particular risk areas are highlighted below.

(i) Fair and Lawful Processing

For the processing of personal data to be lawful it must be conducted fairly which means that, amongst other things, it must generally be collected with an appropriate level of consent. In order for the consent provided by individuals or their parents/guardians to permit the use of the information you must provide sufficient information so that it is clear for what purpose you require the information (and preferably what things you will not do in relation to the information). This information is often referred to as the specified purpose. In particular, when registering players, it must be clear that although the information is captured by the member clubs, it will also be transferred to the T&RA for competitive and other specified purposes. In this way the consent given is sufficiently informed and effective.

Particular care should be taken by clubs when dealing with the issues set out below:-

(a) **Commercial Use of Data**

Commercial use of contact data may well be "unfair" unless consent is obtained when the data is collected. Therefore, it is important to seek specific consent on forms concerning the use of data and log the individual's commercial use preferences and then comply with them.

There are quite strict rules about sending marketing communications to individuals via email. You should not do this unless you have their consent. The ICO website has further guidance.

(b) **CCTV/Monitoring**

Unless you have a legitimate reason to conduct covert surveillance this should be avoided. If you have CCTV cameras you must have clear signs notifying staff and club visitors of the CCTV. Also please be aware that there is no exemption from notification if you use CCTV cameras.

(c) **Sensitive Personal data**

Sensitive personal data includes information relating to membership of trade unions, health, sexual life, offences or proceedings relating to offences. In most cases in order to process sensitive data it is necessary to have the explicit

consent of the individual concerned. Although there is no prescribed form for the consent, it is certainly advisable to have a written form of consent from each individual who provides, for example, medical information.

(d) **Personal data of children**

Clubs with a junior section will process personal data of children. The DPA does not specify the minimum age at which an individual can act in their own regard and therefore give valid consent. Furthermore, the Information Commissioner has been reluctant to provide specific guidance on this subject. However, as regards the processing of information relating to children in an on-line or web based environment the Information Commissioner has indicated that personal information must only be collected from children with the explicit and verifiable consent of the child's parent/guardian unless the child is aged 12 years and over and it is clear that the child understands what is involved.

There are no specific rules as to what constitutes verifiable consent but it is clear that simply asking the child to confirm that their parents consent by way of a tick box is insufficient. The Information Commissioner has suggested that in many cases it will be necessary to revert to postal communication.

In the case of Clubs, personal details will often be taken from those as young as 7 years and therefore the over 12 years exception would not appear to apply. However, as the information is collected physically by forms produced by the clubs it would be sufficient either for the forms to be completed by the parent whilst present at the club or given to the child who then takes it home for the parent/guardian to complete. This process would be analogous to parental consent forms for school trips. As a precautionary measure the clubs should examine the forms carefully to ensure that these have not been completed by the children themselves.

(e) **Publication of Personal Data**

If personal data is going to be published (for example in a club handbook or on the club website) clear consent is needed by the individual concerned. Particular care should be taken with regard to children's personal details ie their name and address being published especially on a club website and we would not recommend publishing such details for child protection reasons.

(ii) <u>Personal Data must be relevant and not excessive</u>

Care must be taken to avoid holding irrelevant, excessive or inaccurate data. This may not only be in breach of the DPA but cause embarrassment if the individual makes a data subject access request (see below). In particular, personal data held on individuals should be circumspect and accurate and not contain unsubstantiated rumours.

(**iii) <u>Data not to be kept longer than purposes require</u>**

There are a number of obligations that relate to the storage of data for a specific period of time, such as 6 years for HMRC and 12 years for documents signed as a

deed. However, Clubs are under an obligation to destroy information which is no longer necessary for the purposes for which it was collected. It is difficult to set a time limit for destroying information. With regard to medical information and contact information it may be that this information is no longer necessary when a member leaves their club although it would be legitimate to retain contact details if the information had been collected in part in order to supply that individual with marketing information.

(iv) <u>Data must be kept secure</u>

Clubs are under an obligation to ensure that appropriate organisational and technical measures are employed against unauthorised access, accidental loss, damage and destruction of personal data.

In particular, this means ensuring an effective firewall, virus protection etc. as well as password protected access. In addition, physical access to paper and electronic records should be secure.

In relation to the period for which back-ups should be retained, this turns on whether data would be lost if electronic records were otherwise destroyed. However, if paper records of all information are retained then there is no obligation to retain back-ups under data protection provisions.

Working outside the workplace is a particular issue, and home workers and those working while travelling should be issued with guidance about keeping laptops, club paperwork etc secure and confidential.

Where a club outsources any function which involves processing of personal data (including functions ranging from payroll to paper waste collection) it should put in place a written contract with security obligations as required by the DPA.

3. SUBJECT ACCESS REQUEST

This is the key data subject access right which can cause administrative headaches. It is often deployed by individuals when they are in a dispute with an organisation. For this reason, it is always important to bear in mind when data is collected or recorded that it may need to be gathered together at some speed and disclosed in the future.

If you receive a subject access request you must decide taking into account any relevant exceptions, as set out in the DPA, what information needs to be given. You have 40 days to respond and may request a fee of up to £10.

The Information Commissioner has recently given advice on what type of personal data must be disclosed if an organisation receives a data access request. The advice is much narrower than the guidance previously given in the Court of Appeal Durant case which provided that information which must be disclosed is limited to that which affects an individual's privacy rather than merely identifies that person. The new advice can be found at www.ico.gov.uk but the key steps which must be followed when deciding whether to disclose personal data are that data should be disclosed if:

- a living individual can be identified from the data;

- the data relates to the identifiable living individual, whether in personal or family life, business or profession;
- that data is obviously about a particular individual;
- the data linked to the individual provides particular information about that individual;
- the data is used to inform or influence actions or decisions affecting an identifiable individual;
- the data has biographical significance in relation to the individual;
- the data focuses or concentrates on the individual as its central theme rather than some other person; or
- the data impacts or has the potential to impact on an individual whether in a person, family, business or professional capacity.

Particular care must be taken when disclosing information if a third party can be identified from the data. Special provisions apply in such circumstances.

For more information on how to handle subject access requests see www.ico.org.uk.

Conclusion

The key points for Clubs to remember are:

(i) ensure you are registered to process data with the Information Commissioner's Office if you need to be. That said, the exemptions are not particularly clear and you may feel that it is worth registering in any event. And remember that the club will be bound by the requirements of the DPA whether or not it needs to register;

(ii) ensure that forms that are used to collect data include a standard form of wording to ensure that individuals understand what the purpose of the capture of data is and what will happen to that data. Importantly, the form must ensure that all individuals give their explicit consent when they are consenting to the use of their data for commercial purposes or supply information regarding medical conditions. Good evidence of explicit consent is a box ticked on a form; and

(iii) as regards those under 18, it is far easier to ensure that the child's parent or guardian give their consent by completing a paper form rather than differentiating between different ages.