GDPR: simplified action list for bridge clubs

Identify who will be responsible for implementing the new regulations within the club. This could be one person, or two or more working together.

Decide which role within the club will have the main responsibility in future for ensuring that the club discharges its obligations under the GDPR – e.g. the Chairman – and who will answer any questions or requests about data held on members – e.g. the Membership Secretary. Ideally, it should be possible to contact these people through a role-related email address such as memsec@anyclub.com, but if not, you will need to give their contact details on your website.

Compile – and keep! – a list of what personal data is held by your club, how it's stored, who has access to it and how it's protected. Consider limiting access where appropriate, e.g. scorers don't normally need to know anything more than the names and EBU numbers of members, and can upload results through their own "MyEBU" area rather than having access to that of the club.

Identify any external data processors – e.g. Bridgewebs, the EBU itself – and make sure that you have appropriate clauses on personal data included in your contracts with them. The EBU will shortly be providing guidance and assistance on the preparation of such clauses.

Produce and publish a privacy policy, based on the EBU template but using the information from the previous steps to amend it where necessary. The privacy policy should be circulated to members and also available on your website. It will need to be reviewed and updated from time to time.

Review any listings of personal data which are not absolutely required to run your club – e.g. membership lists containing email addresses/phone numbers – and either cease to compile them, or seek explicit consent from each member whose personal data is included.

Review data retention: decide how long you need to keep data after someone has left the club, and set up a process for deleting personal data once it is no longer required.

Strengthen all passwords used to protect personal data and make sure they are changed as necessary, particularly every time someone who knows a password stops carrying out the role for which they needed it. Passwords should be at least 8 characters and should contain at least one of each of: both upper and lower case letters, a number, and ideally a symbol.

Decide how the club will deal with data breaches and subject access requests. A written summary of the agreed procedure should be included in the guidance note described below.

Prepare a short guidance note for everyone who has access to members' personal data, explaining what they need to know and do to comply with the Regulations. This should include all committee members, scorers, and TDs, plus others with limited access for particular purposes, such as those who organise matches or co-ordinate host lists. Make sure the note covers security (preferably encryption) for any data downloaded to memory sticks, laptops or personal computers or otherwise kept in homes rather than at the Club. It should also remind recipients to avoid common data breaches: for example, we should normally use "bcc" when circulating emails, avoid putting membership application forms with personal data on club noticeboards, etc.

Ask all recipients for a signature to say they have read the guidance note and formally agree to abide by its contents.

Prepared by Sandra Nicholson (Summertown BC, Oxon), April 2018