General Data Protection Regulation (GDPR)

The GDPR applies to personal data - this is any information relating to an identifiable person who can be directly or indirectly identified.

It contains explicit provisions that require internal records of processing activities to be maintained. Documentation is a new requirement under the GDPR. There is an obligation to ensure (and demonstrate) that what is done with people's personal data is in line with the GDPR.

Processing activities must be documented in writing - can be paper or electronic - and it must be in place by 25 May 2018.

The club must have a valid lawful basis in order to process personal data - this is not new, but there is more emphasis on being accountable for and transparent about the lawful basis of processing.

There are six available lawful bases for processing, set out in Article 6 of the GDPR. The only two which could apply to the club are 'consent' and 'legitimate interests'. The Information Commissioners Office (ICO) says:

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

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.

With consent individuals have full control and responsibility for their data, including the ability to change their mind as to whether it can continue to be processed. With legitimate interests the club keeps control over the processing and takes responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted effect on them. The legitimate interests are that the data is necessary for the running of the club and the data is used in ways people would reasonably expect and which have a minimal privacy impact.

The ICO says it's important to get the lawful basis right first time. If you find at a later date that your chosen basis was actually inappropriate, you cannot simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.

Because of the size of the club using consent as the lawful basis could cause all sorts of problems if people withdraw consent, and also problems with keeping track of who has consented to what. The EBU is using legitimate interests and is providing guidance and information to clubs based on clubs using legitimate interests too.

To use legitimate interests the club needs to produce a limited interests assessment. The EBU has provided a template for this and a completed version for the club is on a separate document.

Main points from the EBU guidance:

- all information we collect relating to members (and visitors) is 'personal data'
- only committee members or club managers should have access to members' records. Passwords should be changed whenever roles are filled by new people. (Note that on Pianola access is not by password, it is by an individual being given specific permissions by ticking a 'role' box on their member record – if that individual no longer takes that role, the tick is removed and they can no longer access data)
- committee members' details should only be displayed on websites if they have specifically agreed to this
- clubs should not issue lists of telephone numbers etc without specific agreement from the people on the list
- access to the club's My EBU should be restricted to committee members and the password should be changed whenever any of them change. Scorers can be marked as such on EBU records and can then upload results using their personal EBU log in (not a problem for us as we upload results using Pianola)
- do not have data in more places than is necessary. Only the primary database (which for the club is Pianola) should contain full information and be secured appropriately. Only the minimum amount of essential information should be stored in other places such as scoring programs
- the club needs a privacy notice and must take all reasonable measures to ensure that members are aware of it. So it must be issued to all members by email or post and displayed on the website and the notice board. The EBU has provided a template and a completed version for the club is on a separate document
- the club needs a new application form. The EBU has provided a template and a completed version for the club is on a separate document

The club is a Data Controller with regard to its own data, and is a Data Processor on behalf of the EBU, to whom they send members' contact data and game results.

Pianola (and Bridgewebs if any member data is held on it) are data processors.

Data Controllers and Data Processors need to have contracts see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts.

The EBU is waiting for templates of these contracts to be made available by the ICO and they will need to be adopted as soon as they are, as the club is a data processor for the EBU.

Pianola has said they will be providing a contract. Bridgewebs says they are working on a contract and privacy notice. They are also amending the website, but seem to be basing everything on consent – see Bridgwebs website http://www.bridgewebs.com/cgi-bin/bwol/bw.cgi?club=bw&pid=display_page11 for more details.

GDPR puts specific legal obligations on data processors and they will have legal liability if they are responsible for a breach. However, this doesn't remove liability from the data controller.

Controllers must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met.

There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Pianola is a secure database, only people with specific roles/permissions can access member data, individual members can only see other members' personal data if that member has specifically consented to it by ticking boxes in My Account on Pianola. Information about grades/ranks is available to other members, but can be restricted by people logging into EBU My Account and restricting it.

Alexa Baxter

22 April 2018