GDPR Guidance (March 2018):
Frequently Asked Questions

This briefing note provides some answers to frequently asked questions arising as Venues prepare for the coming into force of GDPR on 25 May 2018. It is intended for initial and general guidance only and Venues must rely on their own review of this area and seek legal advice where required. Registered Venues can contact BASeLine (on 0344 571 7986) who will be able to assist with general queries that Venues may have on GDPR (you will need to quote the following membership number: X1232KC79BB5).

What is GDPR?

The General Data Protection Regulation is a new, European-wide law that replaces the Data Protection Act 1998 in the UK. The main principles of data protection law will remain unchanged however GDPR places greater obligations on how organisations handle personal data. It comes into effect on 25 May 2018 and is regulated in the UK by the Information Commissioner's Office (ICO).

What information does GDPR apply to?

The GDPR applies to "personal data", which means any information relating to an identifiable living person.

Does GDPR apply to our Venue?

It is very likely that GDPR will apply to your Venue. It applies to any company, charity or other organisation which "processes" any personal data. "Processing" includes the collection, holding, use, sharing and even deletion of personal data. If your Venue carries out any of the above it will be a "controller" under GDPR (unless you are doing this on behalf of someone else). Examples of personal data a Venue is likely to process include staff, volunteer, Venue officer data and member data.

GDPR will apply to the Venue whether or not the Venue needs to register/pay a fee to the ICO (see registration section below).

Each controller is responsible for their own processing of personal data. Non-employed coaches may be separate controllers under GDPR.

What are the main requirements of GDPR?

The Venue must comply with the Data Protection Principles, a set of rules for the handling of personal data. The Data Protection Principles require that personal data is:

- processed *lawfully, fairly and transparently;*
- *adequate, relevant and no more than is necessary;*
- *accurate and kept up-to-date; and*
- *processed securely.*

What does lawful processing mean?

"Lawful processing" means that the Venue must have a "lawful basis" for processing. There are six lawful bases for processing personal data: consent, necessary for the performance of a contract, legal obligation, vital interest, public task and legitimate interest. To determine which lawful basis is most appropriate a Venue must consider the type of personal data and how it is being processed.

The most well-known lawful basis is obtaining the consent of the individual. Consent must be very clear and freely given and individuals must be able to withdraw consent at any time.

Venues, like other organisations and businesses, do not necessarily need consent to process personal data relating to staff, volunteers or members or even other individuals whose data they hold. The alternative grounds for holding and using personal data are often more appropriate and more flexible – provided the Venue's use of the data is sensible and reasonable and individuals have been made aware of it via the Club's privacy policy (more on this below). Venues should not always seek to rely on consent as sometimes consent is not appropriate, particularly as it can be withdrawn at any time. Venues may wish to look at the alternatives: further ICO guidance can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

The LTA has prepared example consent wording that Venues may wish to consider using as a starting point.

What are the alternatives?

There are two main alternatives to getting consent that may be useful where the Venues reasonably needs to use personal information:

1. the processing is necessary for the performance of a contract (e.g. an employment or a membership contract) with the individual. This is likely to cover much of the processing that the Venues carries out; and
2. the processing is necessary for the legitimate interests of the Venue or a third party. When relying on legitimate interests a Venue will need to ensure that they balance their interests against those of the individual. The processing must be necessary for the Venue's reasonable activities and have a minimal impact on the privacy of the individual. The Venue should keep a record of the process it has followed. "Legitimate interests" should cover most reasonable, day-to-day processing of personal data which falls outside the "necessary for performance of a contract" basis – for example retaining a reasonable amount of information about an individual after s/he has ceased to be a member; or perhaps sharing Venue officer information with another Venue for good reasons.

Venues should note that "legitimate interests" and "necessary for the performance of a contract" cannot be relied on in some cases: for example (1) processing of "special category data" (such as health data) and criminal conviction data; and (2) the use of personal email addresses for direct marketing. Personal data in these categories is more closely protected. In these cases the Venue may need consent, or to find an alternative lawful basis.

For example, a Venue may be able to rely on "legitimate interests" for membership administration (instead of needing consent) however any email direct marketing from the Venue to the member will require the member's consent to this type of communication. A member can withdraw consent (and the Venue would have to stop sending marketing emails), but s/he cannot stop the Venue relying on "legitimate interests" without a good reason so the Venue will continue to be able to chase such a member for unpaid invoices, for example. See below for more comments on direct marketing.

Other examples where consent may be appropriate are as follows:

- sharing data with third parties where this is not strictly necessary (perhaps with a sponsor or with other members) – there is a good case that this should be subject to consent, and be genuinely optional for the individual concerned; and
- publishing home contact data of members on websites; or publishing images of individuals (particularly children) on websites or in brochures.

"Legitimate interests" and "necessary for the performance of a contract" with the individual are likely to allow a Venue to process a member's data for the bulk of its purposes, provided the Venue is transparent about this in a privacy policy provided to the member. The Venue can then seek consent for other activities such as email direct marketing, sharing of contact details with third parties, posting of images on websites etc. which are genuinely optional.

The LTA has produced sample wording below which a Venue can use on, for example, a player registration form to summarise what it does with personal data, signpost the individual to the Venue's privacy policy for more detail and seek consent where required. We suggest considering some form of wording, on any data collection form, explaining how that data may be used and signposting the fuller privacy policy.

Thank you for completing this registration form. Your personal data will be processed by the Club for the purposes of club and membership administration and to facilitate your participation in [competitions etc.]. Further details are available in our privacy policy which can be found HERE.

We would also like to send you by email details of offers, membership deals and ticket opportunities. Please tick here if you would like to receive such emails. INSERT TICK BOX.

You may wish to use members' data for other optional uses as set out above and may need to obtain consent to do this. If you wish to do so then you will need to tailor the wording accordingly.

What about direct marketing?

As mentioned above, a Venue may need consent to send direct marketing by email – even to its own members. This is because direct marketing is regulated not just by GDPR but also by the Privacy and Electronic Communications Regulations (PECR). These say that an organisation sending direct marketing by email to personal email addresses (e.g. @gmail.com) must have the consent of the individual, or

alternatively meet a complicated test called "soft opt-in". However, due to its complications, many venues may not wish to rely on it and therefore we have not set out the requirements needed to fulfil it here.

PECR only applies to email and SMS direct marketing (and, in a different way, to phone direct marketing). You are likely to be freer to send direct marketing to a lapsed member by post, relying on your "legitimate interests" again. But you should include an opt-out opportunity in every mailing and you should not continue such marketing indefinitely.

What does fair and transparent processing mean? What is a privacy policy?

GDPR requires the Venue to be very open and clear with individuals about the "processing" which it undertakes (regardless of the lawful basis for processing the data). The Venue will need an updated privacy policy which sets out how the Venue processes personal data. The Venue will need to provide the privacy policy to all relevant individuals – if possible before 25 May 2018. The LTA has prepared a template privacy policy for a Venue's internal purposes (staff, volunteers etc.) and one external-facing privacy policy that Venues can use as a starting point to set out what personal data it collects, what it uses it for, what "legal basis" it is relying on, how long it will keep it for and what individuals' rights are. Preparing and making these policies available is an important part of GDPR compliance.

When should updated privacy policies be used and sent to members, staff, volunteers and Venue officers or other relevant individuals?

A Venue's updated privacy policy must be made easily available to each relevant individual e.g. via a prominent link when any prospective or new members sign up for membership and sent to existing members, staff, volunteers and Venue officers before or around 25 May 2018.

How do GDPR rules differ for children?

The ICO is clear that children are entitled to particular protection under GDPR, because they may be less aware of the risks involved. So the same rules apply, but Venue should make sure they are very clear when communicating how children's data will be used and, in particular, in any language used to collect consent. The law remains unclear as to the age at which a child should be treated as an independent person for data protection purposes: this should probably be treated as 12 or 13, but having regard to the particular child and his or her understanding of the situation. Up to that age, personal data should be collected from the parents and (where consent is required) consent obtained from them. Venues can use the consent wording set out above but may need to amend this slightly so that it clear that consent is being collected from a parent in respect of the personal data of their child. The ICO offers specific guidance on this: see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/.

What records should Venues keep?

GDPR emphasises the need for Controller organisations (here Venues) to be able to demonstrate that they have complied with data protection law. This means Venus should keep records of privacy policy text in place from time to time (even after it may have been changed) and have evidence of consents having been obtained (and when) where the Club has relied on consent. GDPR also requires Controllers to document their thinking about, for example, whether legitimate interests applies and to be able to evidence that they have thought about the privacy implications for individuals of particular uses of their personal data.

How long can the Venue keep personal data for?

A Venue must only keep personal data for as long as is necessary for the Venue's reasonable purposes. There is some flexibility around how long it can be kept. For example, Venues can retain member and employee data for a period after membership has ended or employment has terminated so that it has relevant documentation if that member or employee makes a legal claim against the Venue.

What does GDPR say about data security? What about data security breaches?

A Venue must ensure that it takes measures to secure the personal data that it processes. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Venues can find more guidance in the security section of the ICO's Guide to GDPR here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

Another particular aspect of GDPR is that certain types of data security breach must be reported to the ICO within 72 hours of the Venue becoming aware of it. This may include any hacking of data; any inadvertent loss or mis-publication of data on a website and even any serious interruption to data services. You are required to notify the ICO of data security breaches where it is likely that such breach will affect individuals' rights and freedoms. In addition, where the breach is likely to present a "high risk" to any particular individual (for example if his/her financial or special category data has been compromised), that individual must be informed as well. These rules underline the need to appoint a suitable individual as a data protection manager (discussed in more detail below). The ICO's breach notification guidance is here: https://ico.org.uk/for-organisations/report-a-breach.

What rights do individuals have under GDPR?

Individuals have the right under GDPR to know what a Venue is doing with their personal data. In addition they have the following specific rights:

- Right to request access to their personal data (commonly known as a "data subject access request"). They have the right to receive a copy of the personal data that the Venue holds on them.
- Right to request correction of their personal data. A Venue may need to correct any incomplete or inaccurate information that it holds.
- Right to request erasure of their personal data. An individual can ask a Venue to delete or remove personal data where there is no good reason for it continuing to process it.
- Right to object to processing of their personal data in certain circumstances.
- Right to request the restriction of processing of their personal data in certain circumstances.
- Right to request the transfer of their personal data to another party.

The most significant is the right of subject access: an individual can require a Venue to provide all personal data held by the Venue on him/her, within a month, and without charge. There is no particular form which has to be followed and relevant staff should be trained to recognise them and get them to the Venue's data protection manager quickly so that there is plenty of time to assess them and deal with them. There are some limited exemptions but the Venue may need to ask officers and staff to check and disclose material from private email accounts.

Do we need to appoint a Data Protection Officer (DPO) at the Venue?

This is unlikely to apply to most Venues given the amount and type of personal data that they will be processing however Venues should ensure that they have considered this. Venues can find more guidance in the DPO section of the ICO's Guide to GDPR here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/.

Does the Venue need to register with the ICO?

If a Venue is registered under current law, it is likely it will continue to need to register and pay a fee under the new rules. If a Venue is not currently registered, it should consider the ICO's guidance on registration to assist in determining if the Venue needs to register (there is an exemption for not-for-profit organisations only carrying out very limited data processing) which can be found here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/02/new-model-announced-for-funding-the-data-protection-work-of-the-information-commissioner-s-office/.

What else does a Venue need to do?

Venues should:

- allocate responsibility for data protection to an individual (and relatively senior) member of staff, as "data protection manager": avoid the term "data protection officer" (using the term may result in the Venue being caught by the requirements around DPOs). For larger Venues it may make sense to put in place a small group of senior staff members whose teams are particularly affected (e.g. membership, IT, HR);
- send that individual on some training;

- ensure that person has a good idea of the data processing undertaken by the Venue, and has carried out some kind of audit before 25 May 2018 so that the Venue has assessed what issues might need dealing with;
- ensure that the Venue, and the person responsible for data protection specifically, is ready to deal with any data security breach or any exercise by an individual of his/her rights; and
- ask this person to keep good records of privacy policy wording used, consents (where applicable) and any other relevant information related to processing of personal data.

Does my Venue need a data processor agreement with ClubSpark?

The LTA is aware that many Venues make use of Clubspark. We will be sending out a further communication to Venues relating to Clubspark. However, in the meantime, each venue does not need to physically sign a data processor agreement (like the template provided by the LTA) with Sportlabs to cover a venue's use of ClubSpark. The terms and conditions of use of ClubSpark which the venues accept will contain the necessary data processing provisions.

What will happen if the Venue does not comply with GDPR?

Failure to comply with GDPR may attract enforcement action from the ICO. In serious cases the ICO may issue fines. The ICO also provides guidance to controller organisations like the Venue. It recognises that this is a complicated area of law and has stressed that its priority is helping smaller businesses to meet the law rather than penalise them for breaching it.

ICO Guidance

The ICO recognises that data protection compliance is a significant burden for smaller organisations. What the ICO wants to see is that smaller organisations are taking data protection seriously and making efforts to understand the personal data they hold and process. It has set up a Small Organisations section on its website and this provides a portal into various resources all of which are intended to explain both the existing and the new data protection rules. The section can be found here: https://ico.org.uk/for-organisations/business/.

It has also set up a dedicated advice line for small organisations. More details can be found here: https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/.

What happens if the Venue engages someone else to carry out data processing on its behalf?

If the Venue wants a third party to process the personal data that a Venue holds on its behalf it must make itself comfortable that the third party has sufficient data security arrangements in place and have a written contract in place with this third party to ensure that the third party acts only on the instructions of the Venue. Anyone other than an employee of the Venue will be a third party. An example would be if a Venue engages a third party to carry out its payroll administration.

The LTA has produced a template data processing agreement that Venues can enter in to with third party service providers.