Journey after 25 May GDPR Deadline- Real Life Questions

Questions

We want to market a new course to people who have undertaken a previous course. They took the previous course pre GDPR. What are our options?

If the training course is similar and the participants have informed you in the past not to contact them about future courses then as a sporting establishment and data controller under the data protection law you cannot contact them.

However, if you have informed them that the course they undertook to become a coach is reliant on them keeping these qualifications or credentials up to date and you detail this in your course application form then you could rely on lawful grounds under Article 6,1(b) of the GDPR - performance of a contract/agreement (e.g. course agreement) if you are carrying

out operations to inform them their course credentials are out of date and/or there is a new course they need to undertake as you have updated the course material again you can rely on Article 6,1(b).

If you want to carry out direct marketing by electronic means or by direct mail you need to follow the Privacy Electronic Communications Regulations. Wait to see our blog at the end of September on how to market lawfully.

If you want to keep them updated on sporting courses you could use the ‘soft opt-in’ approach, especially if the course is similar to that undertaken in the past.

Your privacy notice and course agreement need to detail this type of operation and give them a clear option to say 'NO'.

What do we do now?

a) update your course forms,
b) have a clear opt-out if they do not want to be kept informed unless it is a requirement to remain as a sport provider and/or coach
c) update your privacy notice
d) if you have young adults or children marketing operations should not take place until a record of the 'responsible' person (e.g. parent) consent has been obtained.

Do clubs need to provide consent forms for players/coaches. The players and coaches have different relationships with the club, what should we do?

A club is a data controller as they obtain and use the information of people who take part in club activities. The club determines the use of the person's personal information (e.g. use, sharing, retention, security). Being a participant in the club entails being supplied with a privacy notice detailing who you are, how you will use, share, retain and secure their personal information. Where a child is involved a 'responsible' person's (e.g. parent) consent must be obtained and recorded. If a participant is taking part in a club they will complete a club membership form and on this, you should have a privacy notice which you take them through at point of application. In it, you will detail the lawful grounds you will rely on to obtain and use their information, for example Article 6,1 (b) of the GDPR - performance of a contract/agreement (e.g. membership form/agreement). Where you want to use the information for marketing, you need to obtain consent if you intend to market to them electronically or by direct mail. Unless you follow the reply under question 1 above.

As a club we engage with schools and they sometimes arrange and facilitate the competitions in the first set of games. As a club we may take over the competition at a regional round stage. At this point we will not normally know what teams have qualified until the regional stage. What do we now need to do to be compliant with DP law?

A club may engage with an educational establishment (e.g. school) and together you run sporting competitions/events at a local school level. The school is a data controller and the sporting club may be a joint data controller if they are determining the use of the sporting participants' personal information alongside the school. If the club is not determining the use of the personal information and is only using the data under the instructions of the school, then the club is a data processor acting on the instructions of the school as the controller.

This is very important to understand as it establishes roles and responsibilities. There should

be an agreement in place between the club and school detailing the use, sharing operations, security and obligations to be adhered to ensure compliance with the data protection law. This agreement will reference who is responsible to obtain and record the consent of the 'responsible' person (e.g. parent). When obtaining consent, it should be supported by a privacy notice detailing who, what, when and how personal information will be used, shared, retained and secured, when the school obtain and use the personal information and when the club will. This is normally part of an annual parental consent notice. What the club needs to ensure is that this notice details when the club alone become the controller of the data and how the parent/child can exercise their 'rights' under the law.

As a club we run sporting events for under 15-year olds. As part of these competitions, images/video of the players may be taken by the club. From whom and how do we obtain and record consent?

A club would need, again at the point of entering into the joint relationship with the school, to ensure the agreement with the school clearly indexes the consent notice and details controllers and processors as discussed in point 2 above. But the club will also need to obtain written recordable consent for taking, retaining and sharing photographs and videos. This will include where the photos and videos will be posted. If the photos/videos are to be posted on any form of social media, search engine or website, the 'responsible' person needs to clearly understand where and for how long. They need a privacy notice detailing the young person/child's 'rights' and how to exercise these rights.

As a general rule if the 'responsible' person (e.g. parent) consents to having their child's image/video obtained, processed and uploaded by your club directly or via the school, consent can be gathered once but you as a club need to have a record of this. This can be by a statement in your educational sporting agreement with the school. As long as the school confirms to you that they have consent, then this would cover you and others in using the one consent, rather than asking at every event and rather than having to put up posters stating photographs/video or streaming is taking place and how the 'responsible' person can ensure their child is not captured. A good practice approach would be to have staff or photographers wearing clothing which can be noticed. Having a link to your privacy notice and that of school is again a good approach to ensure compliance and transparency.

Our club does not have a photography/video or live streaming policy, what should we do?

As part of the General Data Protection Regulation, you are required to have proper governance controls (policies and procedures) in place to inform staff, volunteers, coaches, board members etc what the club's process is to ensure compliance and the practices all have to follow to implement good data management and protection. These policies are key documents as a club will be capturing a lot of young people and children's' personal information (image and name). You can view our SRA GDPR Toolkit and contact your national governing bodies who may hold template documents they are willing to share. Top tips: As a data controller if you are taking photograph images either at your events and shows you need to have:

a) Posters stating images are being taken and have a point of contact to obtain a copy of any image taken where the person is the main focus
b) Have in your privacy notice how, when, why you will take images, how long you will retain, use, share and secure the information.
c) How an individual can exercise their rights to access, object and request images to be erased. If posted on 'information societies' e.g. social networks/search engines/websites,

how they can exercise their right 'To Be Forgotten'.

Therefore, the organisation running the event needs to ensure, via posters, that they make the attendees aware of who the photographer is, and individuals should have the option of not being photographed. Permission should certainly be sought before photographs are used for publicity/marketing. Be extra aware of photographing children.

Always seek written parental permission before taking a photograph, using a picture, sharing it on social media such as Facebook or Instagram, even in private groups. The new regulations are quite rightly very strict regarding children's data.

What are the basic training information we should supply in our club in regard to GDPR?

You need:
- Photograph procedure
- Privacy notice
- Consent form
- Poster
- Retention period agreed
- Professional photographer agreement and destruction notice

As a club, do I treat coaches as third-party suppliers if they are acting on our instructions and running our events, and should the club have an affiliation agreement in place?

An affiliate is a separate company/person, e.g. an independent contractor/club/coach. However, another company may affiliate through ownership. This ownership does not mean total control. An affiliate agreement can be entered into by any type of business and affiliating with another organisation is a good way to ensure compliance with data protection law, to promote and deliver sports through local clubs and increase general membership and/or grow the sport in general.

An affiliate agreement is a contract between two or more parties: the host, maybe a club, engaging a school/another club/event organiser as an affiliate to run their events. The club should in these circumstances enter into an affiliate agreement with them to ensure compliance with the law, promote sport and leisure services. If the third organisation is not only affiliated to run events, sports and competitions for the club but is running their own events then a separate approach by both parties needs to take place to ensure data controller and processor roles are clearly established.

If the club is acting as a data processor for the member body running events under the member body's instructions, then it is the member body as a data controller which will be responsible under the affiliate agreement.

Local committees which act as coaches to promote a club's regional events and local events will not sign up to an affiliate agreement but should agree a code of conduct, sign up to a constitution and abide by the club's committee handbook and rule book.

If we engage a coach to run training, competitions and events should we be registered with the Information Commissioner's Office?

If a club engages a coach for the purposes of developing and running the club's sport sector provisions locally, they will be a processor acting on the instructions of the club. The data processor should carry out a self-assessment using the ICO assessment toolkit on their website. They would only need to register with the ICO if they meet the criteria as a data controller. However, if in their own right they promote and deliver their own coaching services unrelated to the club then a self-assessment has to be carried out using the online tool for micro-SMEs.

Our club wants to use an online survey tool such as Survey Monkey to enable our participants to enter competitions. What should we consider?

The new data protection law states a person has a right to know where their data will be held and if it is held in an organisation outside the EEA then proper security controls and compliance with the EU Data Protection Law must be adhered to by the international company. The club will need to verify that the overseas company is GDPR compliant.

A clear, open and transparent privacy notice needs to detail your organisation and/or others with whom you have entered into a partnership, and who and how they will hold the data, as well as how they and you will keep this data secure. You will need to detail how they can exercise their rights, for example the right to access their records if held by a third party. You can only pass on club members' information if you record a lawful basis and/or, in the absence of these, if you obtain the consent of the individual. Most sites such as Survey Monkey have GDPR privacy notices and they have signed up to the currently recognised data protection privacy shield showing they adhere to the EU data protection requirements. Each club needs to carry out their own self-assessment on providers to ensure compliance.

The Right to be Forgotten - When someone asks to be forgotten, is the club allowed to keep some of their personal information, for example a record of their qualifications?

When does the right to erasure, to be forgotten, apply? Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose for which you originally collected or processed it;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

The right is not absolute and only applies in certain circumstances. as noted above. If the club has outlined in its retention policy, then the retention can continue as long as you have a lawful basis for the personal and special categories of data (see Article 6 and 9 of the GDPR). The club still needs to inform the individual of their decision within a month of receiving the objection. The Right to Be Forgotten relates to Information Societies (e.g.

search engines and social media). If an individual wants that data erased, you need to make every endeavour to meet this request.

Our club wants to collect and use personal and special categories of information for statistics - What are our GDPR responsibilities?

There are two approaches to statistical information. You need to know where the information derives from and from where you have collected this at source in an anonymised manner. You will then need to record a lawful ground under article 6 e.g. for the performance of your membership agreement, the organisation will obtain personal identifiable information and use this for statistical and monitoring purposes but only to create anonymised reports.

Using the example of a national championship race which creates a list of indefinable runners by name and membership number it allows their times and where they were placed to be recorded. This would be permissible as it would be expected by the member/runner as part of their membership. They would expect their club to have retained this against their personal member records and as long as you have put in your privacy notice that this information will be used in anonymised reports for statistical purposes and these anonymised reports will be shared, the club would be processing data lawfully.

The club need to ensure the identifiable data set is secure/locked down and separate. This identified report has been used as a starting point and it is paramount it can never be reconnected to the anonymised report and/or re-connect. If you do not keep it separate, then you cannot state the statistical report was anonymised. Note Digital Economies Act states it's an offence for anonymised data to be deemed anonymised if it can be re-engaged to identify the living individual.

What is the difference between a Mandatory Data Protection Officer and Voluntary?

The GDPR and the Data Protection Act 2018 both outline the requirements on an organisation for having a Data Protection Officer or not. The GDPR under Article 37 details the criteria and exemptions and Articles 38 and 39 detail the tasks. What is important is to determine if you need a Mandatory or Voluntary by answering the questions under Article 37 and recording your responses and reasoning behind your decision. There is no definition of volume of data or what a core activity is as each organisation and sector is different. As long as you can demonstrate your assessment and reasoning for your decision then that will hold you in good stead. However, you need to ensure when making your decision if you go down the voluntary route you will be required as a data controller or processor to apply the full obligations in Article 38 and 39 "tasks".

As a club we collect medical information and we know this is deemed - Special Category Data. What do we need to do to obtain and use this data?

As a club and data controller you may collect medical information if you can record a lawful ground under Article 9 of the GDPR.

If you cannot record one of these grounds and one ground from Article 6 then you will need to seek consent from the individual or 'responsible' person if it relates to a child or young person. Normally this type of information is collected for the purposes of participants taking part in sporting activities and the club or class has to carry out a health and safety risk assessment or to manage H&S or legal obligations to ensure a person is fit and healthy to take part in the sport. In addition, the collecting of this information may be to ensure the club or class meet their personal liability insurance. All of these are examples you can rely on to request this information. Putting this into practice, it would be reasonable to expect an

instructor/coach to be able to ensure the safety of the players and the others within their control during a sporting event. The instructor/coach needs to know that the individual can carry out an activity safely. If the instructor/coach is in any doubt, they can ask the individual to prove otherwise. Which could include seeing a medical certificate in some circumstances.

As part of collecting this information a privacy notice has to be supplied, informed and understood before collecting the information. The data has to be managed in line with the six principles including the security of the information under Principle 6 to ensure it is adhered to.

As a club can we create "Banned Lists" - I want to understand what our legal obligations are once we have decided to ban someone for a safeguarding matter and what are our obligations are to share this information and when we cannot not?

Safeguarding is covered in Schedule 8 of the Data Protection Act 2018. This is a complex area which brings into force not only the GDPR but the Human Rights Act, Police and Child Protection Act, amongst others. An assessment must take place on a case by case basis and all information should be kept strictly confidential. How and what information is shared is not specified and would need to be decided upon by relevant senior bodies in the club and where applicable by discussing this with your NGB if you have adopted their safeguarding policies.

We would also recommend you seek legal advice as a club to ensure compliance with the law and the protection of children, young adults and vulnerable people. Creation of an Indicator List ‘Ban List' again needs to be created in line with law and the ICO's Information Sharing Code of Practice. These are just a few examples which need to be recorded as part of your safeguarding data protection impact assessment (DPIA). A DPIA should carried out as this would be deemed a new form of processing which may have a high impact on the individual to whom the indicator relates to.