MILLS & REEVE

ENGLANDGOLF

England Golf

Briefing for Clubs & County Bodies: The EU General Data Protection Regulation

December 2017

Introduction

Golf Clubs, County and Governing Bodies will process individual personal data in nearly all their activities. This includes data about employees, volunteers, players, members, website/app users and more.

If you hold information that could be used to identify a living individual (such as contact details sent in via a Membership Application Form, booking enquiries sent via a website or transaction details recorded in the club shop) then you will need to consider the impact of data protection legislation on how you handle that information.

Whilst data protection law has been around for decades, the law is being refreshed and enhanced via the new General Data Protection Regulations (the "GDPR"), which come into force across all EU member states on 25 May 2018.

Golf bodies should therefore be operating in full compliance with the GDPR as at 25 May 2018. This briefing will give an overview about what that compliance should look like.

Let's start with the key principles.

GDPR Key Principles

Principle 1: **Use data fairly, lawfully and transparently**

Personal data must always be processed fairly and lawfully and with transparency at the forefront of all processing.

Further info: This is the top requirement to be aware of, requiring you to ensure you have a solid and documented justification for how you use personal data (for example, keeping a record of consent from the individual that they are happy to receive promotional material from the Club). We've given it its own section and separate examples below.

Principle 2: Purpose Limitation

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

Example: You place all the contact information you receive from members, visitors, volunteers indiscriminately into a single database and send all public mailings to those contacts. You have not complied with the 'purpose limitation' principle. When you collect someone's contact details to make a course booking or a coaching appointment, you should not *automatically* add that person's details to a mailing list – you would need a separate confirmation from the individual to use their details for that purpose (though this could be done at the same time).

Principle 3: Data minimisation

Personal data must be adequate, relevant and limited to what is necessary for the purpose for which you collect it.

Example: Your Membership Application Form requests details of an individual's ethnicity. Unless you can demonstrate that this information is *necessary*, it would not comply with the 'data minimisation' principle to request this.

Principle 4: Accuracy

Personal data must be accurate and, where necessary, kept up to date.

Example: One of your members emails you to tell you that they are moving to a new address. You update the contact details you have and ensure that no further communications are posted to the old address. You also remind members as part of an annual mailing that they should contact you if there are any changes to the details you hold about them.

Principle 5: Data retention

Data must be kept in a form that permits identification of individuals for no longer than is necessary.

Example: You are holding membership records from several years ago that identify individuals whose membership lapsed with no further contact. . Unless there was a good reason to keep these, this would breach the requirement to keep personal data only for as long as necessary. The majority of records

should be deleted from the system once the membership lapses (or a reasonable time afterwards to allow for reinstatement if requested).

Additional Example: You are holding entrant information from an Open Competition that was held 5 years ago. This has value as a historical record for the Club and, on that basis, you retain the key information (e.g. entrant name, handicap, result) but remove information that is no longer necessary or relevant (e.g. address, contact details).

Principle 6: Data security

Personal data must be processed in a manner that ensures appropriate technical and organisational security of those data.

Further info: This means staying abreast of developments in information security, and ensuring that security measures (such as restricting access rights, patching known system flaws and providing staff training) are applied within your organisation. Where an organisation's computer systems are hacked, or data is leaked or lost, it is usually as a result of a failure to meet this obligation.

Example: You have an excel spreadsheet of current and prospective members details which you use to grow the Club's membership. That spreadsheet should have IT access rights in place to ensure only authorised people can view then information on there. Additional protections (such as encryption) should be added if it is emailed externally and care should be taken that the spreadsheet is not lost or misplaced.

Additional example: A member of your HR team has access to a database containing employee payroll information. To assist their working day they print a portion of that information for review. The printer is communal and, because it's taking an age to print, the employee goes to a separate room to make a cup of tea. The information prints and is viewable to anyone who approaches the printer – this could easily result in a breach of the sixth data protection principle.

Lawful Processing

Golf organisations will need to ensure that their reasons for handling personal data align with one of the lawful purposes for processing allowed under the GDPR.

The key question to ask is: *"why am I allowed to use this information?"* For standard personal information such as names, addresses, handicaps, contact details and membership numbers, the answer should be one of the following:

- you have an individual's consent, evidenced by a clear affirmative action, establishing freely given and specific agreement to the processing

> ***Example***: You need consent to sign a member up to receive promotional material from the Club and for other products or services they might be interested in. You inform the individual about who their data will be passed to and how they might be contacted so that the individual can agree to the specifics. You then ask the member to tick a box to confirm their 'clear affirmative consent' to receive the mailings. (When you do rely on consent, the requirement for a clear affirmative act means the individual must take deliberate action to opt in).

- the processing is necessary for performing a contract the individual is party to

> ***Example***: Using someone's contact and payment details to complete a course booking. Without their details, the transaction could not be completed and therefore you are justified in using their details for the purpose of making the sale/booking.

- you are complying with a legal obligation

> ***Example***: You are required to run DBS checks on volunteers who will undertake activities working with child golfing groups. You need to provide information about the individuals to the Disclosure & Barring Service to do this. You do not need their consent, but you do need to inform them that you are undertaking the check and that you are doing so in order to comply with your legal requirements.

- the processing is necessary in order to protect the vital interests of the data subject or of another natural person; and

> ***Example***: A volunteer working on the course collapses and emergency services are called. The volunteer's personal details will need to be provided to the emergency services in order for them to retrieve his medical information to protect the 'vital interests' (the key health situation) of that individual.

- you are pursuing legitimate interests, except where those interests are overridden by the individual's rights

> ***Example***: You email volunteers periodically to see if they are available to provide support on specific dates or at events. The Club will have a legitimate interest in locating available

volunteers, and this outweighs the privacy rights of the volunteers, who will have an expectation that they will be contacted.

'Sensitive' Data

Some data falls into special categories where extra caution must be taken. These are highly sensitive categories of personal data, such as data about an individual's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- health; and
- sex life or sexual orientation.

There are enhanced rules in respect of such data, requiring additional justification for processing. Relevant justifications include: receiving explicit consent from the individual; where the information has already been made public by the individual; or where it is a medical/health emergency.

Example: Your Club's buggy policy requires confirmation of a medical condition before allowing the use of buggies in certain situations. In order to receive such information lawfully, the Club will need to obtain the explicit consent from the individual to record their health information – meaning a documented consent, evidenced by a clear affirmative action (such as a signature confirmation), establishing freely given and specific agreement to the processing.

A note on Consent

As shown above, golf organisations will not always need consent to process personal data under the GDPR. Consent is *one* way of lawfully processing personal data, but is not suitable for all situations. Under the GDPR consent can always be withdrawn, so it is important that you assess carefully whether you do need to rely on consent, or whether there is a more appropriate lawful basis for processing.

Example: Clubs may be required to disclose information regarding their members to England Golf - so that England Golf can provide the full benefits of membership. This would not require the consent of the individual, as it is necessary for the fulfilment of the membership contract. In addition, England Golf requires personal data regarding club members, such as name, gender and year of birth in order to monitor and run the central database of handicaps (CDH). England Golf has a legitimate interest in receiving handicap information, which will typically outweigh an individual's privacy interests regarding handicap information. Where these grounds apply, consent would not be required. What you are required to do is to tell individuals about the disclosure and the reasons behind it, so they can take an informed decision over whether or not to proceed with membership on that basis.

Additional example: You would not wish to seek consent from an individual to record a booking transaction, as if, once the booking was made, the individual *withdrew* their consent for you to use their details then you would be left without a record of the booking. A better basis for processing someone's data for a course booking is that it is necessary to fulfil your booking contract with the individual golfer.

Whatever lawful basis you plan to rely on, you will need to tell individuals your justification for processing their personal data, so documenting this, and communicating it, is important. The next section looks at how this should occur.

Privacy Notices

The GDPR requires organisations to provide information to individuals about the processing of their data in a concise, transparent, intelligible and easily accessible way, using clear and plain language.

This is most commonly achieved through a notice provided to the individual, known typically as a privacy or data collection notice. Some examples of what you should provide include:

- **Identity and contact details** of the data controller (the organisation responsible for the processing of personal data) and any data protection officer.
- The **legal basis** for the processing (including any 'legitimate interests' relied on).
- **Recipients**, or categories of recipients of the data, including details of any proposed data **transfers outside the EU**.
- **Retention period** for which the data will be stored (or the criteria used to determine that).

- The existence of the **individuals' specific rights** over their data (e.g. the right to access data and, if processing is based on consent, the right to withdraw that consent – see next section).
- The **right to complain** to a supervisory authority (which, in the UK, is the Information Commissioner's Office).
- If there will be any **automated decision taking** – together with information about the logic involved and the significance and consequences of the processing for the individual.

Example: Your Membership Application Form should include the elements listed above in the form of a Privacy Notice, which the new member will read (and should ideally confirm they have read) prior to submitting their personal information to make the application.

Additional example: When making a one-off course booking for a non-member, a Privacy Notice should be provided at the time the visitor provides you with their details. That Notice should explain, amongst other things, how their data will be used, if it will be transferred anywhere, and what rights the individual has over their personal information.

Individuals' rights

Alongside the increase in governance obligations, the GDPR provides some enhanced rights for individuals. For example, the right for individuals to access their personal data through a **"Subject Access Request**" is altered so that personal data must, in general, be provided without charge and within a shorter timeframe of one month.

Example: A Member contacts you concerned that his personal details have been forwarded by the club and he is now being contacted by a number of golf clubs trying to attract him with membership offers and he does not recall providing consent for this. He requests that you provide him with the personal data that you hold on him, as well as confirmation of any transfers of that data outside the club. Under the GDPR, you should aim to provide this information within one month of the request.

There are also the following enhanced rights:

- **Right to object**: Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing; and processing for purposes of scientific/historical research and statistics.

- **Right to rectification**: This allows individuals to require an organisation to rectify any inaccurate personal data about him/her without undue delay and to, where appropriate (in the context of the processing), have incomplete personal data completed.

- **Right to erasure**: This allows individuals to request their personal data is erased without undue delay in certain situations, including where the personal data are no longer necessary in relation to the purpose for which they were collected/processed; or a data subject withdraws his/her consent and no other legal ground for processing applies.

- **Right to restrict processing**: This allows individuals to, in certain circumstances, require the organisation to restrict its processing to storage only.

- **Right to data portability**: This enables individuals who have consented to the processing of their data to ask for a copy of that personal data in a structured, commonly used format so that it can easily be transferred to another data controller.

Getting GDPR right first time

The emphasis throughout the GDPR is on transparency and accountability. Golf organisations should be prepared to be open and accountable to individuals with all processing of their information, by complying with the principles set out above.

Record keeping becomes all-important, and organisations are required to maintain a record of processing activities under its responsibility. The record should mention:

- the name and contact details of the controller and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- any transfers of personal data to a third country or an international organisation;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures in place.

Example: You should prepare a Data Protection Policy document and allocate responsibility to a member of your organisation to be the point of contact for data protection matters. The Policy should contain as a minimum the information outlined above, including the overall purpose of the processing (e.g. for administration of the activities of the golf club) and the categories of personal information (e.g. "contact details of members, visitors, staff and personnel"; "handicap information of players"; "health information required in accordance with Buggy Policy"). Be specific and informative where possible, to comply with the requirements of transparency and accountability.

And it helps to get it right first time. Under the GDPR, you are required to notify **security breaches** to the ICO without undue delay and, where feasible, within 72 hours of awareness (unless the breach is "unlikely to result in a risk to the rights and freedoms" of data subjects – this is a judgment call that will need to be documented as part of the breach response). Notification should also be made to the affected data subjects, without undue delay.

Example: A mailing is inadvertently sent out to the entire club mailing list that contains a spreadsheet record of buggy bookings and the health details of members who have booked buggies. You are unable to successfully recall the email and you realise there were no password protections in place in the spreadsheet, therefore you consider that this situation may result in a high risk to the rights and freedoms of the individuals concerned. You notify the Information Commissioner's Office and the affected individuals without undue delay.

Under the GDPR, any data subject that has suffered damage as a result of an infringement of the GDPR will have a right to claim compensation for that damage from the infringing organisation.

The maximum level of fine for non-compliance with most obligations under the GDPR will be €20 million, or 4% of worldwide turnover if that is greater. This is a significant increase on the current maximum and is intended to ensure data protection compliance moves up the risk agenda for many organisations.

There is much more to cover regarding the GDPR that falls beyond the scope of this briefing. We have included below some practical steps to take now to assist in preparation for the legislation, and further information can be found at www.ico.gov.uk.

GDPR: practical steps to take now

- Analyse what personal information your organisation collects (for example member, visitor, employee and volunteer information) – and what the source of this information is. Is it the individual direct? Or from some other source such as a previous club?
- Review how this data is used (which might be for bookings, marketing, employment or administrative purposes) and cross-check those activities against the permitted conditions for processing, asking: *why am I allowed to use this information?*
- Check employment contracts, membership documents and privacy information provided to employees, volunteers and members, and ensure you are giving sufficient detail about what personal data you will process and why.
- Review internal data protection policies and consider whether they ought to be updated.
- Review who in your organisation has access to records containing personal data and determine whether it is necessary for everyone who currently has access to retain it.
- Make relevant staff and personnel aware through providing data protection training focused on GDPR compliance.
- Ensure that contracts that require personal data to be transferred to another organisation – which happens where you use a cloud-based software system, for example – are GDPR-compliant.
- Review the existing procedures you have for dealing with breaches, taking into account: (1) the framework e.g. are the right people involved, both to take decisions and to undertake technical activities to try to minimise the scale of breach and consequences on data subjects?; (2) the practicalities e.g. how are they going to be contacted if a breach is discovered at 5.45pm on a Friday or midday on a Sunday?
- Review internal processes for complying with individuals' rights. In particular, ensure standard responses to subject access requests inform individuals about their other rights.
- Check the ease with which data can be easily accessed, exported and/or restricted if relevant requests are received.