Kingsknowe Golf Club

Privacy Policy in Line with new GDPRegulations

In brief, the Club's policy is to be compliant with the new General Data protection Regulations at all times. This is furher explained as follows:

Background:

The law around Data Protection is changing and the new General Data Protection Regulations (or GDPR for short) comes into effect on **25 May 2018.** The new regulations replace the UK Data Protection Act and will govern how organisations use personal data. This is seen as a positive step towards individuals having more control over how their data is used.

Because Club members data (for example name, address, date of birth) is collected, stored, used, shared and deleted, the Golf Club is a classified as a "controller" and "processor" of the personal data of its members, and therefore the new GDPR applies to the club.

The GDPR is mainly concerned with electronic personal data, however, where the club uses paper filing that allows information to be picked from specific criteria, then the GDPR also applies to this paper filing system. Email and any personal data included in emails will be caught by the GDPR.

What the Club will do:

The GDPR includes six data protection principles for the Club to be aware of whenever it is using personal data (for example, signing up a new member, sending an email to a member, etc). the club will adhere to these principles and in order to comply, the club will:

1. Ensure it identifies a lawful basis to process the personal data (from the list set out in the GDPR) and provide a privacy notice to the individual, which tells individuals how the club uses their personal data.
2. Only collect, use and keep personal data for specific purposes – i.e. only use a member's personal data for membership purposes or only use visitors or competitors data for club purposes
3. Only collect, use and keep personal data that the club actually needs.
4. Keep personal data up-to-date where possible.
5. Only keep personal data for as long the club needs it – eg. when a member leaves it will review all the member's personal data held to see whether it is still needed after a specific period of time.
6. Protect personal data and keep it secure.

"Lawful bases" for processing personal data

There is a specific list of "lawful bases" for processing personal data in the GDPR and the Club will identify which one applies before collecting and/or using personal data and this will be communicated to all individuals in privacy notices.

When processing members' personal data (for example, membership fee payments) there will be a "contractual" lawful basis because the Club needs to use members' personal data to comply with the terms of their membership and the Club will only use such personal data for this purpose.

The Club may also be legally required to process members' peronal data for specific purposes eg health and safety. This lawful basis is known as the "legal obligation" lawful basis, and it applies when a controller needs to use personal data to comply with a legal obligation.

The Club will also have a "contractual" lawful basis where employees will have a contract of employment and it will only use employees' personal data to comply with its obligations under that contract of employment. The Club will also need to process employees' personal data for legal reasons under the "legal obligation" lawful basis eg reporting details of employees' income to HMRC for tax reporting purposes.

Another lawful basis is where the Club (or a third party) has legitimate interests for processing personal data. Such legitimate interests cannot be outweighed by the interests of the relevant individual. This might apply where the Club issues newsletters to members / other individuals or communications promoting upcoming events / competitions, which is seen as 'direct marketing'. The Club will make sure that individuals can stop receiving such newsletters or communications if they so decide by contacting the club.

Asking individuals if they consent to the club using their personal data is also a lawful basis under the GDPR and if the Club does not specifically ask individuals for consent where appropriate, then it will use a consent statement that:

- is a clear affirmative action: opt-in rather than opt-out and no pre-ticked boxes;
- is separate from other terms and conditions and not a precondition of signing up to a service;

Where the Club uses social media pages, it is likely that social media websites will have updated privacy policies as the providers will consider that they are controllers.

Finally there is "special category personal data" which is a separate category of personal data under the GDPR and includes data revealing a person's racial or ethnic original; health; sex life or sexual orientation; or religious or philosophical beliefs. The Club currently does not do this but if it decides to process special category personal data, it must have a lawful basis and meet at least one condition for processing special category personal data. There will also be separate conditions in the new UK Act for processing personal data relating to actual or alleged criminal offences, but these are still to be finalised.

Privacy notices

When collecting or receiving personal information from anyone, the Club will issue a privacy notice to the individual whose personal data they are processing. A "Privacy Notice" is a statement by the Club explaining to individuals what the Club doe with personal data. For example, a privacy policy notice will be included in applications for membership, membership renewal forms, booking forms and employment/volunteer contracts. The Club will also put its privacy notices on its website and will provide individuals with the link to the relevant page.

The Club will cover all of its data processing activities in the privacy notices. If for example, it passes membership data or other personal data to the Lothian Golf Association or Scottish Golf Ltd, it will become a controller of that personal data in most cases. The clubs' privacy notice will tell individuals

that the LGA/SGL will receive their personal data and become a controller of it. This could also apply to other third parties.

Rights of data subjects

Individuals (known as "data subjects") have certain rights regarding their personal data under the GDPR. The Club will consider requests from data subjects and provide a response within one month.

Data subjects can ask clubs to:

1. provide a copy of their personal data and information on how the club processes the data
2. correct or complete any incorrect or incomplete personal data held by the club
3. delete all personal data held by the club (only in some circumstances)
4. stop or limit the processing of their personal data (only in some circumstances)
5. provide all personal data in a particular format for their re-use (only in some circumstances)

Data subjects can also object to the Club processing their personal data, which is known as the "right to object". This right only applies in some circumstances – for example, members can object to receiving the club's newsletter and when requested, the club will stop sending the newsletter to the member immediately.

Accountability principle

The GDPR requires controllers to be responsible for and be able to demonstrate compliance with the data protection principles – 'accountability'. There is an exemption for controllers with less than 250 employees and guidance is awaited regarding the scope of this exemption. The Club will however it keep a record of what and how it processes personal data for members, employees, volunteers, and visitors/participants as they do this on a regular basis.

For this, the Club will keep a document recording the following:

- the purposes of processing – for membership, competitions, handicaps etc;
- the categories of individuals and personal data – members, volunteers, etc. and name, address, date of birth, etc;
- the categories of recipients – details of who the club shares personal data with, such as other Golfing Bodies;
- details of any personal data transferred or hosted outwith the EU and safeguards – for example, MailChimp, which has Privacy Shield certification;
- retention periods – how long different records of personal data are kept;
- details of security measures in place to keep personal data secure – for example, passwords, locked cabinets, restricted accounts, etc.

The Club will also keep copies of privacy notices and consent statements so it can evidence that these have been provided to individuals.

Breaches

If the club loses personal data or suffers a data security incident then this would result in a personal data breach. Examples of breaches include: access to personal data by an unauthorised person; sending personal data to the wrong person; or losing computer or mobile equipment containing personal data.

If the breach is severe and could affect individuals (i.e. – risks their rights and freedoms) then cthe Club will notify the Information Commissioner's Office (the ICO) within 72 hours of becoming aware of a breach. The Club will also notify the affected individuals if there is a risk to their rights and freedoms.

Board Action Plan

The process for compliance to GDPR by 25 May is as follows:

- The Board considered a briefing document at its April 2018 meeting and agreed to construct a policy of compliance that commits the club to the requirements of GDPR.
- The policy will be approved at the May Board meeting.
- An action plan of what the club needs to do to be compliant has been worked up into a detailed plan, incorporating the requirements identified in the briefing document. This will be presented to the Board in May for approval and subsequent implementation.
- The office ensure all actions are completed by 25 May.
- The Policy and Action Plan will be updated and as and when required. All updates to policy will be signed off by the Board.
- Policy documents will be available internally on IG and externally on www.kingsknowe.com

END

May 2018