

Business Privacy & Data Protection Policy

General Background to GDPR

The General Data Protection Regulation (GDPR) applies from 25 May 2018. **Many of the GDPR's main concepts and principles are similar to those in the Data Protection Act (DPA) 1998.** For further information you may refer to the **Information Commissioner's Office (ICO)** website.

GDPR applies to the processing of PERSONAL data. However, we apply many of its principles to both our CORPORATE/CLUB customers as well as our interfaces with INDIVIDUAL MEMBERS on behalf of our clubs.

Note we have several policies which address distinct yet related areas:

- Business Privacy & Data Protection Policy
- Privacy & GDPR Policy for Smart Club Cloud Users
- Website User Policy
- Security Policy

The first two policies aim to clearly outline how and why we collect, manage and process data in fulfilment of our corporate privacy obligations and the GDPR Accountability Principle. They also describe security levels and instances where data is shared or processed by other parties. Note, all of our policies are working documents which will continually be amended in line with regulations and any changes in our procedures.

Data Management & GDPR at Smart Club Solutions

There are various implications of GDPR depending on whether your company is a 'processor' or a 'controller'. Given the diverse range of services which we provide we can be one or other or both, but in the vast majority of cases our clubs are controllers, the data owners, and we assist with certain areas of processing or the facilitation of processing. Our clubs, as controllers determine the purposes and means of processing personal data. GDPR compliance is based on how the controller (the user, or in our instance, the club) decides to use the data. Our solutions can assist and facilitate greatly in GDPR compliance and effective data management. Our Data & Service Agreements with individual clubs will outline further the records we maintain and process and how much of the **GDPR duty of care and effective implementation comes down to the club's (the controller's) implementation** of its data management activities.

Quality Service to our Customers: Data on your Club

Under the GDPR definition, data management relating to our own company business-to-business operations sees us acting **primarily as a data 'controller' of business information rather than personal data.** We implement high standards of professional integrity and privacy when it comes to dealing with our Customers. In order to achieve quality levels of administration, operations, customer service and communications it is essential that we maintain an up-to-date secure database of relevant information on each of our clients.

As of May/June 2018, we are contacting each of our clients to inform them of the information which we hold at present and to advise them that they must contact us immediately to inform us of any relevant changes. They will also be made aware of our revised policies as will (where relevant) any members who use our Smart Club Cloud solution. This is particularly important with changes in personnel or officials responsible for club finances. Our clubs consent to us storing relevant general club contact information as well as contact information for relevant club officials and representatives

whose details we require in order to deliver an efficient service as part of our operations as a service provider and as a contractual necessity to deliver on our service.

Any change in this contact information must be communicated to us by the club's Data Protection Officer as detailed in our Data & Service Agreement with the Club. Any individual may request that their data be removed at any stage. In the event that a Data Protection Officer leaves his/her office then the club must inform us of its new appointee.

The Club's Data Protection Officer will also be responsible for informing us of relevant administrators or individuals at the club who should have access to the club's membership database. The DPO should also inform us of any changes to this list of individuals – additions or removals. At present (May 2018) we are in the process of refreshing consents from clubs and revising our Data and Service Agreements.

Example information which we maintain includes:

- Address and contact information for the general club
- Names and contact details of key individuals/officials as club representatives

Such information may be maintained in our own internal databases or in systems/solutions related to our company operations such as (online) accounting/invoicing solutions (eg. Freshbooks) or payment processing services such as GoCardless.

We backup records remotely on secure servers which are managed by us and our service providers in the UK. Personal information that we store or transmit is protected by security and access controls, including username and password authentication, two-factor authentication, and data encryption where appropriate.

Depending on the nature of the solution which we have provided to an individual club, we may have to process or share data on the club itself or individual club personnel or indeed members. We will seek appropriate consents within our agreements with the club, who in turn will also inform their members and seek approval/consent from their members in order to deliver the desired solution/outcome/service for that member. Such explicit consent to the club may not be required if the action is in the interest of the member by virtue of being a member, or **if the member's compliance is a 'contractual necessity' in order for the club's service to function.** These types of scenarios are outlined below, mainly including third party integrations and occasions **where we need to access the club's membership database.**

What member data do we hold in our Cloud and how secure is it?

Our grounds for retaining and processing data relating to the Club are outlined in section 1. In relation to the clubs members, while the burden of duty will more often fall on the club as the data owner, there are occasions where it is relevant for us to have a legal basis for processing data or facilitating the processing of data.

Depending on the nature of the solution which we have provided to an individual club, we may have to process or share data on the club itself or individual club personnel or indeed members. We will seek appropriate consents within our agreements with the club, who in turn will also inform their members and seek approval from their members (or implied by virtue of interest of the member) in order to deliver the desired solution/outcome. These types of scenarios are outlined below, mainly **including third party integrations and occasions where we need to access the club's membership database.**

The vast majority of our clubs host their Smart Membership database. Our Smart Club Cloud enables members to carry out a range of secure financial transactions online. Such transactions are processed by other reputable third party payment processors, so the only sensitive member

information actually held in our Cloud is the following: Firstname, Surname, Date of Birth and Email. This information is required to assist login verification and to match transactions with the relevant member in the club database. No bank account or card details are stored in the Cloud. Indeed, such information is only entered and live for the period of the transaction by the payment processor. Our Cloud database is hosted in AWS and has firewall rules that only allow access from our office IP address and the AWS server which hosts the Cloud site and API. All web communication is over https and SQL server communication is done on an encrypted pipe. Personal data is passed to third parties for certain integrations as outlined below. AWS backs up the Cloud database on a daily basis. You may consult our full [Security Policy](#) for further technical information.

How and why we process/share data in our Cloud with Third Parties

While we may host and/or may backup your club data, Smart Club Solutions does not access (unless requested by the club) or share data with any other party. However, elements of our Smart Club Cloud solution involve third party processing of members data or club data:

- Cloud 1: Stripe Payments Platform: One of our Cloud options whereby members can carry out club-related transactions online. Members complete their transaction on a secure site and we do not have access to their bank information which is processed via Stripe Payments.
- Cloud 2: Realex Payments / Bank Internet Merchant Account: Similar to the previous point, the **member's bank information is processed via the secure Realex Payments portal and we do not have access to such information.**
- GoCardless: where a club signs up to a payment plan with us. Under this scenario, club financial information is processed by GoCardless and is not visible or held by Smart. There will be a direct agreement between the club and GoCardless.
- ClubManager365.com: We also integrate with relevant providers of complementary software in order to enhance the overall solution for our clubs and members. One such integration at present is with ClubManager365.com for online booking at our tennis clubs. The joint **processing here is actually between the club's membership database and the online booking partner** so the data management should be covered by your club policy.
- Other third party solutions: We will update this document with any additional third party integrations at the appropriate time.

We will review any contracts which from time to time we may have in place which involve sharing data with other companies and we will generate appropriate documentation to demonstrate compliance.

When might we **require access to a Club's membership data?**

There are 4 scenarios when we might have sight of or need to access membership data at a club:

- Club database setup: When we work with the club on the initial setup of their Smart Club Solution. Membership files are deleted from our Server when we have finished the import.
- Smart Card Personalisation: We provide an inhouse card printing service. In addition we occasionally use third party card printers. When using third party print services we seek prior confirmation that the purge all data upon completion of the print job and that they do not copy or share any information. Only upon receipt of this agreement will any details be sent to the relevant print bureau. Data will be purged once cards have been delivered to client and client confirms acceptance.
- Hosting, Support & Training: we may need access to your data when a Club requires support. The majority of the time all access to the data will be through an online service such as Teamviewer, so the data does not leave the Club server. On occasions we may need to transfer a backup of the data to our server for testing purposes, upon completion of which the data will be purged.
- Backup: we may need to retrieve information upon request from you club if they use are remote backup service.

How does Smart Club Backup manage club data and how secure is it?

Many of our clubs avail of our secure Online **Backup solution**. **Under this arrangement all of a club's data is backed up securely once every 24 hours to a secure server located in England.**

We will only request access to this data upon request by the club and this is only likely to happen in the case of **any emergency where there is a risk of loss of data on the club's local server.**

All communications between Smart Backup Server and your local Server are transported in a 128-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (internet), potential eavesdroppers have no knowledge of what has been exchanged.

All of your files are first zipped and encrypted with your defined encrypting key before they are sent to Smart Backup server. To everyone but you, your files stored on the Smart Backup server are no more than some random files with random content.

The encrypting key used to encrypt your files resides only on your computer and is known only to Smart Club Solutions, although we can provide this to you if necessary. Currently, the algorithm that we are using to encrypt your files is Advanced Encryption Standard (AES), with 256-bit block ciphers.

You may consult our full [Security Policy](#) for further technical information.

Including Smart Club Solutions in your Membership Terms & Agreements

We have an agreement with you as a Club (new Data and Service Agreement coming soon), under which we agree to deliver an effective membership management solution. We do not have to ask your members directly to opt-in to avail of our solutions as the club is our customer and you have already signed your members up to receiving our service. In GDPR terminology, you are the **'controller'** of the personal data to be processed.

However, we would advise you to include reference to our service within your own terms and agreements with members. You may seek explicit consent from your members to opt-in to certain communications and services, or it may be implied that that members agree to such services by virtue of becoming a Club member and in line with the successful delivery of club services – it is part of your **contract with the member and it is in the member's** interest. The basis of agreement is up to you, the club, to decide upon.

So, in summary and without repeating all of the above information, you may wish to include reference to the fact that:

- Smart Club Solutions delivers a Membership Management solution to your club.
- This solution may on occasion involve Smart Club Solutions having sight of membership data (eg. to setup the initial database, to assist in support or training enquiries, to print membership cards).
- This solution may on occasion involve Smart Club Solution processing or facilitating the processing of membership data and some of this may be by third parties (eg. online payment processing, online booking, personalisation of smart cards).
- The Smart Club Solution is critical to efficient and effective club operations and membership co-operation is taken as given once members join the club; or, you may include this information in a more general agreement/policy which members must accept upon joining the club.
- Members can find out more about the Smart Club Solutions Privacy Policies at the Smart Club Solutions website (Business Privacy & Data Protection Policy; Privacy & GDPR Policy for Smart Club Cloud Users).

How can our Smart Club Solution assist with your GDPR compliance?

The new regulation impacts greater on the responsibilities of the club than it does on Smart Club Solutions, and to this end our solutions can assist your club in meeting its GDPR requirements. We are **providing the tools for you, the 'controller'**, to effectively manage your membership data and carry out your **GDPR obligations but we are not the 'owner' of the data and it is up to the club to implement and use the database and related solutions in a professional manner.**

A Smart Club Solution can assist your club in becoming GDPR compliant but ultimately it will be down to the Club to ensure that it meets its obligations under GDPR.

Here are just some of the ways we can help:

- Our Membership database (and Members Cloud) equips club administrators with extensive features for comprehensive data management. The standard fields as well as the ability to create additional tick box criteria and user defined drop-down menus empower club managers and administrators to record all relevant data against each member.
- The Smart Club Cloud for Members enables clubs to ask members to register online, and within the data collection, explicitly record member permissions/agreements linked to key criteria and policies.
- Members can log-in to amend their settings and preferences (eg. opt-out) in our Cloud and clubs can report of any changes via our Cloud reporting features.
- Members can also view and update some of their personal information held in the club database.
- Reporting features enable you to report on such items as member preferences, members who have not opted-in, etc. while communications features enable you to send tailored messages to those specific individuals as a group.
- Our Cloud registration enables parents to register their children online with a club and express their preferences in terms of communications and acceptance of policies.

Target Clubs & Direct Marketing

We may gather information on target clubs or companies as part of our market research and business development planning.

We may seek to qualify key decision makers by phone or via communications in social networks such as LinkedIn.

If they are to be added to a database for email communications, we will firstly gain explicit permission to do so from the relevant individual.

Anyone may provide their personal details to us at any time on the Contact Us page on our website, or via direct communication by meeting, email, phone or social networks. In the event that a potential customer (or other interested party) communicates firstly with Smart, then they will be deemed to be interested in a reponse/correspondence/communication, their details will be retained and, given following appropriate opt-in, we will continue to communicate with them in a timely manner until such time as they advise that they are no longer interested in communications from Smart. Individuals may inform us of their wish to unsubscribe in writing by letter or email, via the contact form on our website, or via the unsubscribe links within some of our emails. They may also unsubscribe by phone. See also our [Website User Policy](#).

Data Retention

We retain information on all current and previous customers (clubs) to enable us to provide an efficient service and a solid backup of information in the event of a historic enquiry. Such information will include records in our own customer database and historic email communications.

Note, such information is held under the club's record and not that of any individual.

We also retain information on enquiries from clubs expressing (potential) interest in our solutions. Such information is also retained with a view to professional business development, relationship development, and quality of service. Where an individual informs us that they no longer represent a club then they may request that their details are withdrawn.

We do not retain information on individual members at our clubs as this is the clubs data. Our Smart Club Cloud demands that certain limited member details are stored by us and these are outlined above. **From time to time we may need to access the club's membership database or facilitate the processing of member data and such instances are detailed above (support, card printing, etc.)** including details of when we purge such data. See our [Privacy & GDPR Policy for Smart Club Cloud Users](#).

General

Communication of Privacy Policy

When we sign-up or collect data from our clubs we inform them of how we store, process and use their information as part of our Data and Service Agreement. Relevant policies are also communicated to our Cloud users under our user agreement and are available to view via our Website. We also advise our clubs on relevant information which they should make available to their members when implementing a Smart Club Solution but, again, these communications are the responsibility of the club.

Data Security & Breach Notification

As the majority of our clubs host their own data, the risk of a data breach is borne mostly by the club. However, we do continually monitor our Cloud (payment platform) for any unwanted activity and in the event of such an occurrence we would immediately inform relevant parties be that club, member, integration partner or possibly ICO if the implications were significant (eg. likely to cause significant personal distress, damage to reputation, cause financial loss, identity theft or breach of confidentiality). Our integrations partners will also inform us immediately should they identify any threats to data security.

Privacy & Protection by Design

Our company operations and procedures as well as our software solutions are developed with a view to general data protection, security and GDPR compliance, both for our company as well as for our Clubs. We continually monitor our inhouse club data while ensuring that data protection is at the forefront of new development and any integrations under consideration (where, for example, we would complete privacy/protection impact assessments during specification and testing in partnership with the relevant 3rd party).

International Markets & GDPR

GDPR applies from 25 May 2018 across all European Union markets. This includes the UK, despite its plans to leave the European Union. As we are a registered company in the UK, our lead supervisory authority is the ICO. Any integration partners we work with are also based in the EU. While at present all of our customers are based within the UK and Ireland, we will make any future international customers (if any) aware of their obligations under GDPR if they deal with EU citizens. GDPR imposes restrictions on the transfer of personal data outside the European Union but it is extremely unlikely that this will affect our operations.

Privacy: Rights of the Individual

The majority of the following points are the responsibility of the Club as the controller but clubs and individuals have the right to request what information we hold on them, correction to/removal of this information, prevention of direct marketing, prevention of automated decision-making and profiling and data portability (from controller). Under GDPR clubs have 30 days to reply to a SAR (Subject Access Request) and we would also apply this timeframe. We reserve the right to refuse or charge for requests that are manifestly unfounded or excessive. Your club controls your data and you should contact them if you wish it to be verified, amended or removed. Members can also log-in to amend their settings and preferences (eg. opt-out) in our Cloud and clubs can report of any changes via our Cloud reporting features; Members can also view and update some of their personal information held in the club database.

GDPR & Personal Data of Children

With a view to managing our club data for efficient company communications and operations, we have no reason to hold any personal data related to children.

In relation to clubs using our solutions to manage data relating to children, each club will have its own rules in relation to child age verification and policies re. parental consent for data processing, communications, etc. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger than clubs **will need to get consent from a person holding 'parental responsibility'**. **To this end, our** Cloud registration enables parents to register their children online with a club and express their preferences in terms of communications and acceptance of policies.

Data Protection Officer (DPO) & Policy updates

We have a DPO responsible for continually monitoring developments in this field and updating our policies, practices and development plans in line with our company and customer requirements. Our policies may be updated from time-to-time in line with regulations and/or changes in our products or practices.