Southsea Tennis Club - General Data Protection Regulation (UK GDPR) guidelines

The Data Protection Act 2018 is the **UK's** implementation of the General **Data Protection Regulation** (**UK GDPR**)

Data Protection Lead.

Although there is no specific requirement to assign an individual, the Membership Secretary is primarily responsible for data management as the personal data retained for STC is held in ClubSpark, and the Membership Secretary manages the data in ClubSpark.

All UK GDPR questions should consequently be directed to the Membership Secretary. Southsea.tc@gmail.com

Data Retention and Auditing

It is STC policy to retain Members details within the LTA ClubSpark facility and not on its own data storage areas. This ensures that the data is protected as ClubSpark is UK GDPR-compliant and ensures that there is only one set of data thereby reducing the risk of data synchronisation issues.

Name, email address and phone numbers are kept in the Club's Gmail account, this is so that we can contact you with club related business and notifications.

Members' data is only retained for the current membership year. Membership details for previous years are archived within one month of the commencement of the new membership year.

Members are all sent a link that enables them to modify or delete personal individual fields that they are not happy with within the ClubSpark facility.

The Membership Secretary deletes records of members that have left the club and reviews the club membership validity on an annual basis.

As STC is a voluntary organisation, the only records retained are membership records.

Personal Data Usage

Membership details are only retained for recording membership purposes.

Details are not shared with any other organisation or individual.

ClubSpark UK GDPR Compliance

ClubSpark is hosted on Microsoft Azure, which runs in geographically dispersed datacentres that comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored, and administered by Microsoft operations staff that have years of experience in delivering the world's largest online services with 24 x 7 continuity.

In addition to datacentre, network, and personnel security practices, Microsoft Azure incorporates security practices at the application and platform layers to enhance security for application developers and service administrators.

Security for the Hosting Environment

The Microsoft Azure platform environment is composed of computers, operating systems, applications and services, networks, operations and monitoring equipment, and specialised hardware, along with the administrative and operations staff required to run and maintain the services. The environment also includes the physical operations centres that house the services and which themselves must be secured against malicious and accidental damage.

Key Architecture Design Points

The Microsoft Azure platform is designed to provide "Defense in Depth," reducing the risk that failure of any one security mechanism will compromise the security of the entire environment. The Defense in Depth layers include:

- Filtering Routers: Filtering routers reject attempts to communicate between addresses and ports not configured as allowed. This helps to prevent common attacks that use "drones" or "zombies" searching for vulnerable servers. Although relatively easy to block, these types of attacks remain a favourite method of malicious attackers in search of vulnerabilities. Filtering routers also support configuring back-end services to be accessible only from their corresponding front ends.
- Firewalls: Firewalls restrict data communication to (and from) known and authorized ports, protocols, and destination (and source) IP addresses.
- Cryptographic Protection of Messages: TLS with at least 128 bit cryptographic keys is used to protect control messages sent between Microsoft Azure datacentres and between clusters within a given data center. Customers have the option to enable encryption for traffic between end users and customer VMs.
- Software Security Patch Management: Security patch management is an integral part of operations to help protect systems from known vulnerabilities. The Microsoft Azure platform utilises integrated deployment systems to manage the distribution and installation of security patches for Microsoft software.
- Monitoring: Security is monitored with the aid of centralised monitoring, correlation, and analysis systems that manage the large

amount of information generated by devices within the environment, providing pertinent and timely monitoring and alerts.

- Network Segmentation: Microsoft uses a variety of technologies to create barriers for unauthorised traffic at key junctions to and within the data centers', including firewalls, Network Address Translation boxes (load balancers), and filtering routers. The back-end network is made up of partitioned Local Area Networks for Web and applications servers, data storage, and centralised administration. These servers are grouped into private address segments protected by filtering routers.

STC ClubSpark Management Access

The Membership Secretary manages who has authority to review the data on ClubSpark, and reviews that the access is correct and limited to appropriate committee members on a 6-month basis.

Details Relating to Children

All child details are linked to the record of a parent, and communication with children is carried out through the parent. All children are linked through the Parent nominee and that parent can review and amend/delete those child records.

Email Addresses

The primary day-to-day communication with members is through email facilities, using the following email account:

southsea.tc@gmail.com

Consent is reached with members to ensure that they are happy for their email addresses to be utilised for this purpose.

The Club Chairman appoints who controls these distribution lists and reviews them on an annual basis.

Social Media Controls

The club utilises the following social media facilities to inform and promote club activities:

- Facebook
- Instagram
- Twitter

Facebook and Twitter are actively listed in the EU-US privacy shield as UK GDPR compliant platforms. Instagram is owned by Facebook and hence covered under its parent umbrella.

Individual or group members photos may be uploaded onto these platforms, but the postings will not include details such as names to protect individuals' identities.

Before images are used on the website or Social Media channels, permission will be sought by the Social Media Controller. Any images kept by the club will only be used for this purpose and not made publicly available without permission.

Any person requesting a photo of themselves to be removed will contact the Social Media Controller, who will ensure that the photo is removed within 48 hours of notification.

The Social Media Controller will review the platforms on a half yearly basis, and entries that show people no longer associated with the club will be removed.

Complaints and Subject Access Requests

Any UK GDPR issues that are received are to be logged in the following spreadsheet on the Team Room:

> STC/General Admin and Work Areas/UK GDPR/UK GDPR Issues List

Details to be included in this facility include:

- UK GDPR Issue number
- Date Received
- Concerned Party
- Assigned Resolver
- Issue Raised
- Resolution Actions
- Date Resolution Agreed

Confirmations of resolutions should be uploaded into the UK GDPR directory in the Team Room.

13 April 2021