CLUBSYTEMS – MEMBER DATABASE

GDPR - Security Overview

Created: 09/04/2018

The GDPR becomes enforceable from 25 May 2018, this notification is designed to assist users if asked about the security in place for Club Systems hosted products.

ClubV1 (and all our cloud software) is hosted in Microsoft Azures Northern Europe region.

Microsoft has been leading the industry in establishing clear security and privacy requirements and consistently meeting these requirements. Microsoft Azure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2.

As well as country-specific standards, such as Australia IRAP, UK G-Cloud and Singapore MTCS. Rigorous third-party audits, such as by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate.

We protect your data in the following ways:

1) **Encryption** - We use an industry standard level of SSL certification to secure data, the SQL database secures your data by providing encryption for data in motion with Transport Layer Security (TLS) and for data in use with Transparent Data Encryption (TDE).

2) **Firewall and Rules** - To help protect your data, firewalls prevent access to the ClubV1 database until we specify which computers have permission using firewall rules. The firewall grants access to databases based on the originating IP address of each request.

3) **Authorization / Authentication** - Authorization refers to what a user can do within an Azure SQL Database, and this is controlled by our user account permissions. As a best practice, we grant users the least privileges necessary.

4) **Dynamic Data Masking** - We hide some columns to limit sensitive data exposure by masking them to non-privileged users.

5) **Key Vaults** – We use Key Vault for storing secrets like passwords or API keys,

6) **Additional security** - We offer all ClubV1 clubs an option, to use a 'PIN' in conjunction with the Username and Password to ensure an additional level of security preventing unauthorized access to the Software by any user or other party.

7) **Passwords** - Passwords are hashed using unique salts and key stretching to make cracking more difficult.

Along with protection, we also use proactive monitoring in the form of:

1) **Auditing**

Auditing tracks database activities by recording database events to an audit log. We are able to understand ongoing database activities, as well as analyse and investigate historical activity to identify potential threats or suspected abuse and security violations.

2) **Threat detection**

Threat Detection complements auditing, by providing an additional layer of security intelligence built into the service that detects unusual and potentially harmful attempts to access or exploit databases. We are alerted about suspicious activities, potential vulnerabilities and SQL injection attacks, as well as anomalous database access patterns.