Genius Sports

Technical & Organisational Measures (TOMs)

Classification: External
Version: 2.0

Overview

Genius Sports understands the requirements for maintaining the security of personal data that our customers, personnel, suppliers and other third parties share with us. When developing, designing, selecting and using systems and processes that are involve the processing of personal data, we take steps to ensure that we fulfil our data protection obligations to secure personal data. These are summarised in the following Technical and Organisational Measures (TOMs), provided in compliance with Article 32(1) of the GDPR.

Genius Sports maintains the majority of production environments within Amazon Web Services (AWS), or Microsoft Azure. We operate a shared responsibility model with these providers whereby areas of responsibility for security are divided between Genius Sports and the providers. As such, we take necessary steps to ensure they adopt high standards of security and compliance with adequate technical and organisation measures in place. See further details of the AWS shared responsibility model and AWS Compliance Centre, Azure shared responsibility model and Azure Compliance Centre.

1 Organisational

Our strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling Privacy and Security related risks through the establishment and maintenance of an ISO 27001 aligned Information Security Management System (ISMS).

We operate a dedicated internal Information Security department, working closely with our Privacy department to operate the ISMS in a manner that ensures that appropriate security measures are in place to protect personal data and maintain compliance with all applicable privacy laws and regulations. In addition, we maintain Executive level security and privacy committees, providing top management support, strategic direction, and overseeing the maintenance of our ISMS.

Genius Sports has an Information Security Policy, Privacy Policy and further related policies which define our requirements for the protection of information and systems. Policies are subject to periodic review and approvals by Senior Management prior to release. All employees are required to comply with our Information Security Policy, and non-compliance can result in disciplinary action.

2 People

We maintain confidentiality agreements with our employees, customers and relevant third parties, prohibiting the disclosure to unauthorised third parties of any confidential data related to Genius Sports and of our customers. Background checks are conducted against our employees, the level of checks is dependent on role and level of access to data.

Our employees and relevant contractors are provided with Information Security awareness training upon joining Genius Sports and further training is provided on a regular basis throughout employment to ensure awareness is maintained.

3 Vendors & Suppliers

Suppliers who require access to data and systems must go through our procurement process and are subject to security and privacy due diligence and must likewise implement appropriate technical and organisational measures to be authorised as a Genius Sports supplier. We enter into personal data processing agreements, including EU Standard Contractual Clauses and UK International Data Transfer Agreements, with suppliers who process personal data on our behalf. Depending on the sensitivity of data that a supplier may have access to, we may stipulate additional security requirements in our terms of agreement.

4 Physical Access Control

Genius Sports' infrastructure and applications predominately operate in the Cloud using reputable third-party providers (AWS and Azure) who are responsible for the securing the hardware, software, networking, and facilities that run our Cloud services. This includes ensuring the physical and environmental protection of their Data Centres.

Where a customer prefers on-premises hosting, we will provision services from our third-party managed UK Data Centre. Our data centre provider operates high performance and secure connectivity to ensure the protection of data, this includes ISO 27001 and SOC 2.

We may store non-customer personal data in our offices, such as employee, contractor and supplier records. In such instances, we maintain physical security controls to restrict access to only authorised individuals. This includes access-controlled areas and locked storage holders and CCTV monitoring.

We allow remote working for certain roles at Genius Sports and have implemented various measures to ensure the protection of data in such scenarios. This includes the enforcement of a Remote Working Policy, use of a VPN for connections to our network, and the deployment of Mobile Device Management (MDM) solutions to ensure security policies are applied to end user devices, including Bring Your Own Devices (BYOD) mobile devices. The use of BYOD is subject to compliance with our BYOD Policy and application of device controls to restrict information access.

5 Logical Access Control

Genius Sports' policy is to provide access to data and systems based on least privilege basis. This is implemented through various measures including:

a. Use of identity and Access Management tools to control the secure authentication and authorisation.
b. Enforcement of a Password Policy requiring complexity, password rotation, and multiple factor authentication, unless approved by exception.
c. Prohibition of credential sharing, unless approved by exception.
d. Secure storage of credentials in encrypted vaults such as password managers and secrets managers.
e. Encrypted connections to our systems and services processing personal data, including VPN access to critical network resources.
f. Collection of system access logs.
g. Access provisioning subject to strict approval procedures to ensure access is appropriate.
h. Access rights of employees and external party users to data and systems adjusted or revoked upon change or termination of their employment, contract or agreement.
i. Personal data encrypted in transit and at rest. This includes encryption of databases, servers, user devices and communication.
j. Segregation of access to data, including separation of development and test environments from production systems, and network segmentation.

6 Security in Design & Development

During development of processes and technology we focus on security and privacy by design and by default. Security and privacy risks are considered in the early stages of a project or product's development. Our Security and Privacy teams are consulted to ensure that potential risks are identified, and privacy principles are adopted to sufficiently mitigate any risks and data processing complies with relevant laws and regulations. Our design principles include:

a. Ensuring the minimum amount of personal data necessary is collected and processed.
b. Retaining data for a limited period of time.
c. Only using data for the purposes for which it was collected.
d. Ensuring that we have a legitimate reason to process the data.
e. Ensuring that processing is transparent and fair.
f. Employing data masking, pseudonymisation and/or anonymisation where appropriate.
g. Encryption of data in transit and at rest.
h. Secure authentication and authorisation controls to restrict access.
i. Enforcing appropriate data retention and backup policies.

Genius Sports incorporates information security requirements into the development, acquisition and deployment of new systems. We operate a Secure Software Development Lifecyle (S-SDLC), supported by secure development policies and training. Our SSDLC framework comprises:

a. Requirements: assessing potential security and privacy risks, and setting requirements to mitigate risks.
b. Design: reviewing the secure and privacy compliant design of systems.
c. Development: analysing code in development to ensure it adheres to secure coding guidelines.
d. Verification: testing to ensure the original design and requirements are satisfied.
e. Post-deployment: ongoing maintenance of security controls, monitoring and regular testing.

7 System & Network Security

Genius Sports employs various security technology to detect, prevent and respond to security events and threats that may exist in our infrastructure, applications and end user devices. Our network infrastructure is protected using endpoint detection and response (EDR) technology, firewalls, Cloud Security Posture Management (CSMP) solutions, and are subject to regular security patching and testing.

The security of corporate end user devices and BYOD is managed using Mobile Device Management (MDM) solutions which ensure devices have the necessary security policies and controls applied such as encryption, patching, and deployment of anti-virus protection.

8 Resilience

Genius Sports maintains measures to ensure the resilience of our data and processing activities. Our systems and environments hosted by third party Cloud and data centre providers benefit from the high levels of availability and redundancy provisioned by the third parties. For our remaining infrastructure, we have built in backup and redundancy capabilities to facilitate the continuity of services in the event of disruption.

We maintain frequent, secure backups of essential data, software and systems, with the aim of ensuring recoverability of operations and preventing the loss of personal data. Backups are stored in secure remote locations and retained in accordance with our retention policy. Recovery and restoration processes are regularly tested for effectiveness.

Sufficient redundancy has been built into our information processing facilities to meet our availability requirements. Our Cloud infrastructure is hosted across different geographic regions using multiple parallel instances and leveraging load balanced automatic failover capabilities. We conduct regular testing of redundant systems to ensure the expected failover from one component to another.

9 Monitoring & Response

Genius Sports operates an in-house global Security Operations Centre (SOC) utilising Security Incident and Event Management (SIEM) technology to monitor and respond to threats across our devices and infrastructure. We also receive security intelligence feeds from various channels including the UK's National Cyber Security Centre and specialist industry feeds to enrich our threat monitoring capabilities.

Upon identification of an incident or event, our incident response procedures will be invoked to ensure the effective response and mitigation of incidents. Our procedures are designed to minimise the impact of security incidents, restore normal operations as quickly as possible, and prevent similar incidents from occurring in the future.

Incidents are immediately triaged and assigned a priority to determine the applicable timescales for response, as well as the type of internal and external communication required. This includes the notification of relevant incidents to affected customers and regulators without undue delay and in compliance with applicable laws and regulations.

10 Compliance

Genius Sports maintains an assurance framework comprising a four lines of defence model to ensure the continued effectiveness and improvement of our security measures, and compliance with laws and regulations. This includes auditing of controls by our Internal Audit team, as well as external auditors such as ISO 27001 certifying bodies. Our infrastructure and applications are independently security penetration tested to look for any vulnerabilities that may impact the integrity, confidentiality or availability of data and systems.