



PRIVACY & SECURITY

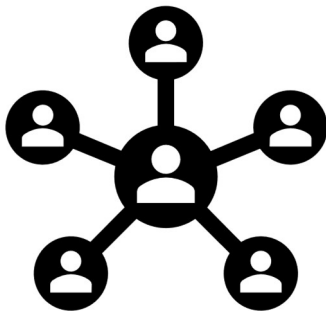
For Customers
April 2025

OVERVIEW

Life Fitness' privacy and security program is an integral part of our business operations. We have a dedicated team responsible for privacy and security to ensure protection for:

- Life Fitness information assets including Halo Fitness Cloud, our exercise and equipment management platform
- Facility owner/operation ("Facility") customer and member data
- The underlying technology and infrastructure of Life Fitness environments

Access to customer and member data is restricted to authorized parties who have been vetted by risk assessments, regulated by data controls, and bound by contractual agreements.



As a connected fitness company, we've established mature competencies in:

- Threat monitoring, response, and proactive cyber defense capabilities.
- Our data privacy and controls align with industry recognized security frameworks such as the NIST CSF and ISO 27001.
- Requiring our third-party partners, suppliers, distributors, and agents ("Partners") to maintain appropriate privacy and security hygiene to protect the data they process on behalf of Life Fitness.
- Maintaining our compliance with data privacy laws such as the General Data Protection Regulation ("GDPR"), U.S state privacy laws including the California Consumer Protection Act ("CCPA"), as amended.

SECURITY ECOSYSTEM



Cyber Defense and Incident Response

Life Fitness utilizes a 24x7 staffed security operations center to monitor and respond to cyber threats against our enterprise and exercise platform environments. Security controls are deployed throughout to automatically detect and mitigate attacks. Back-up systems are designed and tested to restore timely access to data in the event of an incident.



Secure Software Development

An iterative security analysis is performed during each phase of the software development lifecycle, using both dynamic and static testing services. Access to base code repositories is restricted to authorized personnel which are required to use strong authentication to access.



Vulnerability Management

Scanning for vulnerabilities on all systems is performed during the design, pre-production, and post-production release of those systems. Ongoing weekly scanning is performed to ensure any new vulnerabilities are discovered and mitigated in a timely manner.



Compliance and Risk Management

Life Fitness aligns with the NIST Cybersecurity Framework and has deployed policies, standards, and processes to meet framework guidelines. Sustained compliance is regularly monitored and evaluated including penetration and vulnerability testing and third-party risk assessments.



Privacy and Security Controls

Controls and practices commensurate with industry best practices are deployed to all facets of the Life Fitness enterprise and exercise platform to ensure adequate data security and a strong posture against cyber-attacks. These include user authentication, access restrictions, encryption of Halo Fitness Cloud data and other personal data as appropriate, and event logging,



Training and Awareness

The security training and awareness program includes quarterly newsletters and phishing simulations to keep employees educated on security threats. Onboarding and annual security training is mandated for all employees and additional in-depth training is provided to select functions.

COMPLIANCE WITH DATA PROTECTION LAWS AND REGULATIONS



Part of the Life Fitness privacy and security program includes meeting requirements set forth in data protection laws, including the General Data Protection Regulation (EU and UK).

Strategy and Governance Framework

Life Fitness has established a privacy committee which serves as the governing body for managing privacy matters. Internal and external privacy officers are appointed as well as are external legal counsel for data privacy compliance and guidance purposes.

Policy Management

Life Fitness has both internal and external privacy policies, as well as information security policies and standards which determine how we incorporate GDPR and privacy considerations into our business practices.

Data Lifecycle Management

Life Fitness conducts data mapping activities annually to ensure the latest PII location and cross-system transfer information is inventoried and mapped. Additionally, Life Fitness requires data retention or anonymization based on business processing, legal, and commercial needs.

Data Privacy Training

All company personnel receive online training dedicated to GDPR as well as data protection and privacy requirements to ensure a privacy and security aware culture.

Transmission and Storage

Life Fitness deploys encryption, usage monitoring, and malware defenses to protect data during transmission and in storage based on the nature and purposes of the processing.

Individual Rights Processing

Life Fitness provides individuals the ability to **opt-out** of data collection and marketing, request to obtain data collected about them, and/or remove data using our publicly facing data subject request process as required by data protection laws.

Privacy by Design

As part of the Life Fitness compliance framework, a privacy by design policy is implemented to ensure all new or existing projects receive proper data protection impact assessment.

Cross-Border Data Transfer

Where required by law, we maintain data protection agreements, standard contractual clauses, or other approved methods for cross-border transfers of personal data. In compliance with GDPR, we also have standard contractual agreements in place between Life Fitness US, UK, and EMEA affiliates.

Data Processor Accountability

All data processor engagements are subject to a mandatory third-party risk assessment and governed by written contracts covering legal requirements including data use and disclosure restrictions, technical and organizational security measures, notice of security incidents, and cooperation with Life Fitness in responding to data subject requests.

THIRD-PARTY MANAGEMENT



Life Fitness is committed to supporting its Partners as they strive to adopt and follow data protection best practices that guide Life Fitness. Generally, these best practices include, but are not limited to:

- ✓ A risk and vulnerability management program
- ✓ Incident response and breach notification processes
- ✓ Adherence to privacy regulations and practices
- ✓ Operational backup, restore, and business continuity plans
- ✓ Company-wide security and phishing awareness training
- ✓ Personnel screening, termination, and transfer processes
- ✓ Encryption at rest and in transit for data and assets
- ✓ Secure software development practices
- ✓ Identity governance and strong access control
- ✓ Security threat monitoring and controls
- ✓ Implementation of security policies, standards, and procedures
- ✓ System configuration and maintenance processes
- ✓ Alignment to industry recognized security frameworks
- ✓ Third party risk assessment processes

CONTACT US

For questions about this information please contact your Life Fitness representative or email us at privacy@lifefitness.com.