EZ Coach Security Policy: https://www.ezcoachco.com/securitypolicy

1. Introduction
At EZ Coach, we prioritize the security of our users' personal information. This Data Security Policy outlines the measures we have implemented to protect the data we collect, store, and process. Our security practices comply with industry standards and regulatory requirements to ensure that your information remains safe and secure.

For any questions about these terms, please contact us at info@EZCoach.ai.

2. Security and Standards Certification
EZ Coach adheres to recognized security standards and certifications to safeguard personal data, including:

ISO/IEC 27001:2013: International standard for information security management systems.

SOC 1, SOC 2, and SOC 3: Standards for managing customer data based on five trust service principles – security, availability, processing integrity, confidentiality, and privacy.

GDPR Compliance: Adherence to the General Data Protection Regulation for protecting personal data of EU citizens.

CSA STAR: Cloud Security Alliance Security, Trust & Assurance Registry.

SSL/TLS Encryption: Secure Sockets Layer/Transport Layer Security protocols for data transmission.

PCI-DSS Level 1: Payment Card Industry Data Security Standard for processing card payments.

Data Tokenization: Replacing sensitive data with unique identification symbols that retain all essential information about the data without compromising its security.

3. Data Encryption
We employ robust encryption methods to protect personal information both at rest and in transit:

Data at Rest: Information stored on our servers is encrypted using industry-standard encryption algorithms.

Data in Transit: Information transmitted between users and our servers is protected using SSL/TLS encryption.

4. Access Controls
Strict access controls are in place to ensure that only authorized personnel can access personal information:

Role-Based Access: Access to data is granted based on an employee's role and responsibilities within the organization.

Multi-Factor Authentication (MFA): MFA is required for accessing sensitive data and systems to provide an additional layer of security.

Regular Access Reviews: Periodic reviews of access permissions are conducted to ensure compliance with our security policies. We may also personalize your visits to our website by combining collected personal information with data from cookies (described below), enabling us to recognize repeat visits and tailor your website experience.

5. Data Storage and Backup
We utilize secure data storage solutions and maintain regular backups to prevent data loss:

Secure Data Centers: Personal information is stored in secure data centers operated by trusted vendors like Microsoft Azure.

Redundancy and Backups: Regular backups are performed to ensure data redundancy and availability in case of hardware failure or other incidents.

6. Incident Response Plan
EZ Coach has a comprehensive incident response plan to address potential data breaches or security incidents:

Incident Detection and Reporting: Procedures are in place for detecting and reporting security incidents promptly.

Response Team: A dedicated incident response team is responsible for investigating and mitigating security incidents.

Notification Procedures: In the event of a data breach, affected users will be notified in accordance with applicable laws and regulations.

7. Employee Training
We conduct regular training programs for our employees to ensure they adhere to data security best practices:

Security Awareness Training: All employees receive training on data security and privacy practices.

Ongoing Education: Regular updates and additional training sessions are provided to keep employees informed about the latest security threats and mitigation techniques.

8. Third Party Management
We carefully select and monitor third-party service providers to ensure they meet our security standards:

Vendor Assessments: Security assessments are conducted for all third-party vendors before engaging their services.

Contractual Obligations: Contracts with third-party vendors include data protection and confidentiality clauses to ensure compliance with our security policies.

Regular Audits: Ongoing audits and reviews are conducted to ensure third-party vendors maintain the required security standards.

9. Data Minimization
We limit the collection and retention of personal information to what is necessary for the purposes described in our Privacy Policy:

Data Retention Policy: Personal information is retained only as long as necessary to fulfill the purposes for which it was collected or as required by law.

Data Deletion: Procedures are in place to securely delete personal information when it is no longer needed.

10. Continuous Improvement

We are committed to continuously improving our data security practices to adapt to evolving security threats:

Regular Security Audits: Periodic security audits are conducted to identify and address potential vulnerabilities.

Security Updates: Our systems and software are regularly updated to incorporate the latest security patches and improvements.

Contact EZ Coach

If you have any questions or concerns about this Security Policy, please contact us at info@EZCoach.ai.