Transform®

Data Ownership, Privacy and Cyber Security Statement
Humanizing Growth Platform

Humanizing Growth Platform by Transform Management Consulting LLC (with its registered seat in Prince Muhammad Ibn Abd Al Aziz, As Sulimaniyah 3951 Riyadh 12223) aims at providing personalized, impactful coaching that empowers leaders and employees to drive cultural change by connecting our clients with top-tier coaches who will support them with actionable insights that lead to meaningful transformation.

Our Intention

We are committed to maintaining the highest standards of integrity and professionalism in our relationship with you. As part of this commitment, we are dedicated to protecting the privacy, security, and ownership of the data you entrust to us. This "Data Ownership, Privacy, and Cyber Security Statement" outlines our approach to managing your data with the utmost care and in compliance with applicable laws and regulations. This document is designed to inform you of your rights and our responsibilities, ensuring transparency and building trust in our processes and systems.

1. Data Ownership

We recognize that our customers own their personal and transactional data. This includes any information provided by the users, data created through the use of our services, and data input manually by the users into any of our systems or applications. Customers retain ownership rights to their data as prescribed by applicable laws.

2. Data Usage

The data provided by our clients and users is primarily used to facilitate the provision of our services. Transform shall only also use this generically. The data will be anonymized to improve your service offerings, perform analysis to enhance user experience, and fulfill our legal and regulatory obligations. We do not share, sell, or lease customer data to third parties for their marketing purposes without explicit consent from our customers. Third parties include the technology provider, operati9ng and maintaining our coaching platform.

3. Privacy

We are committed to protecting the privacy of our customers. Our data collection is limited to what is necessary to provide and improve our services. We outline in clear terms how we collect, use, and store our customers' information. Customers have the right to request

access to their personal information and can ask for corrections or deletion as per the data protection laws applicable in their jurisdiction.

4. Data Security

To prevent unauthorized access, data breaches, and ensure data integrity, we employ robust cybersecurity measures including, but not limited to, encryption, firewalls, and secure server facilities. Our security policies are regularly reviewed and updated to adapt to new threats.

5. Cybersecurity measures used:

a) **Data Encryption:** We encrypt data both at rest and in transit to ensure that even if data is intercepted or accessed without authorization, it remains unreadable and secure.
b) **Access Controls**: We implement strict access controls and authentication procedures, such as multi-factor authentication (MFA), ensures that only authorized personnel can access sensitive data.
c) **Regular Security Audits and Penetration Testing**: We conduct regular security audits and penetration tests helps identify and mitigate vulnerabilities within the company's network and systems before they can be exploited by attackers.
d) **Secure Software Development Lifecycle (SDLC):** We integrate security into the software development lifecycle helps in identifying security vulnerabilities early in the development process and ensure that security is a priority throughout the development of applications.
e) **Network Security Measures:** We includes the use of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and protect the network from unauthorized access and threats.
f) **Data Backup and Recovery:** We regularly backing up data and having an effective disaster recovery plan ensures that the company can restore data in case of a cyber attack or other data loss event.
g) **Security Awareness Training:** We provide ongoing training for employees about the latest cybersecurity threats and best practices helps in preventing security breaches caused by human error.
h) **Endpoint Protection:** We use antivirus software, anti-malware programs, and other security tools on all devices that access the company network to protect against threats.
i) **Cloud Security:** We use security configurations, compliance audits, and cloud-specific security tools.
j) **Incident Response Plan:** We have a detailed incident response plan which allows us to quickly address and mitigate the effects of a security breach.

5. User Control and Rights

Customers can access their personal data, edit inaccuracies, or request deletion. We respect customer rights under data protection laws, such as the right to object to certain processing activities. If you wish to exercise any of these rights, please contact our data protection officer at info@transform.con.sa

6. Compliance and Cooperation with Authorities

In meeting our obligations prescribed by the Saudi Authorities, we comply with applicable data protection laws and regulations. We may disclose personal data to law enforcement or other authorities if mandated by law or as required to protect our rights or the rights of others.

7. Updates to the Statement

This statement is subject to changes to comply with legal requirements or to reflect new processing activities. Any changes to our data ownership, privacy, and cybersecurity practices will be communicated through our website or directly to our customers, as deemed appropriate.

8. Technology Provider's Guarantee

The above is based on and in line with the technology service provider's terms and conditions, data security and cyber security policies and guidelines, GLF Consulting FZ LLC Creative Zone, Fujairah, UAE.

Date of issue:	July 1, 2024
Effective Date:	July 1, 2024
Version number:	Version 1