Data Protection Guidelines and Technical Measures

Data protection is paramount for Transform Management Consulting. The following guidelines and technical measures are developed in consideration of the principles of the European General Data Protection Regulation (hereinafter GDPR), various industry standard practices.

The measures described hereinafter are subject to permanent change of technology and will be adjusted, if required by law to ensure compliance with the highest security standards.

I. Confidentiality

- **Physical Access Control** – Data centers and office and other data processing facilities are operated in a way that ensures that unauthorized physical access is restricted. Personalized chip cards, electronic door openers, facility security services or entrance security staff, as well as alarm systems, video surveillance systems are in place in all the worldwide data processing facilities of the technology provider.
- **Electronic Access Control** – It is ensured that only authorized use of data processing and data storage system by two-factor authentication, a password policy following BSI standards, automatic blocking and locking mechanisms as well as encryption of data carriers and storage media are in place.
- **Internet Access Control** (permission for user rights of access to and amendment of data) – The technology provider ensures permission for user rights of access to and amendment of data, such as no unauthorized reading, copying, changing or deletion of personal data with their IT systems. It follows a strict rights authorization concept with need-based rights of access, and surveillance of by logging of system access events.
- **Isolation Control** – By design of the technology, data of different interests, clients and purposes are strictly separated.
- **Pseudonymisation** – The system is designed in consideration of data minimization and data avoidance and takes measures of privacy by design and privacy by default, ensuring the processing of personal data in such method, that the data cannot be associated with a specific data subject without the assistance of additional key information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures, wherever such measures are applicable and sufficient.

II. Integrity

- **Data Transmission Control** – The technogy is designed in a way that it ensures authorized reading, copying, changing or deletion of personal data by electronic transfer or transport implementing high standards of encryption, providing access to our server spaces for external environments only via Virtual Private Network (VPN).
- **Data Entry Control** – All IT systems implemented at the technology provider guarantee verification, whether and by whom personal data is entered into a data processing system, is changed or deleted.

III. Availability and Resilience

- **Availability Control** – The Backup Strategy provides for the prevention of accidental or willful destruction or loss of personal data, including state of the art virus protection, firewall, reporting procedures and contingency planning and a rapid recovery in emergency situations.

IV. IV. Procedure for regular testing, assessment and evaluation

- The technology provider implements a Data Protection Management System following the advice of external legal experts from privacy and IT law.

V. Order or Contract Control

- The technology provider requires a formalized order and contract management, ensuring that no third party data processing takes place without consent and corresponding instructions from our clients, as well as strict controls on the selection of the service provider by pre-evaluating the technical and organizational measures of data protection and its security and supervisory of follow-up checks

VI. Technology Provider's Guarantee

The above is based on and in line with the technology service provider's Technical and Organizational Measures (TOM), GLF Consulting FZ LLC Creative Zone, Fujairah, UAE.

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