McKinsey Data Protection Protocols

We have updated our technical and organizational security measures. Effective May 1st 2023 , the technical and organizational measures that McKinsey will implement to protect Client´s Confidential Information will be as described in the Information Security Program Overview (ISPO) available at https://solutions.mckinsey.com/msd/information_security_overview.pdf. For the avoidance of doubt the measures included in the ISPO do not result in a material reduction in the level of protection afforded to Client´s Confidential Information under these Data Protection Protocols

McKinsey agrees and warrants that it has implemented technical and organizational measures appropriate to protect Confidential Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the information to be protected having regard to the state of the art and the cost of their implementation. These measures include, as appropriate and without limitation:

1. Implementing and complying with a written information security program consistent with established industry standards and including administrative, technical, and physical safeguards appropriate to the nature of the Confidential Information and designed to protect such information from: unauthorized access, destruction, use, modification, or disclosure; unauthorized access to or use that could result in substantial harm or inconvenience to the Client; and any anticipated threats or hazards to the security or integrity of such information;

2. Adopting and implementing reasonable policies and standards related to security;

3. Assigning responsibility for information security management and data protection and to provide to the Client contact details of responsible persons at McKinsey if requested;

4. Devoting adequate personnel resources to information security;

5. Carrying out verification checks on permanent staff that will have access to the Confidential Information;

6. Conducting appropriate background checks and requiring employees, vendors and others with access to the Confidential Information to enter into written confidentiality agreements;

7. Conducting training to make employees and others with access to the Confidential Information aware of information security risks and to enhance compliance with McKinsey's policies and standards related to data protection, as well as requiring such personnel to keep all such Confidential Information secure and confidential during their assignment and thereafter;

8. Sub-processing certain infrastructure and maintenance functions (e.g., hosting, backup, maintenance, administration, file sharing and storage, helpdesk) to third parties. With respect to such sub-processors:

    a. The Client acknowledges that McKinsey shall be permitted to engage sub-processors for the processing of the Confidential Information subject to the controls and requirements set forth herein.

    b. McKinsey will ensure that sub-processors are required to implement security controls no less stringent than those set forth herein, are subject to a legally recognized transfer mechanism, and are bound by written agreements reflecting the same.

    c. A list of McKinsey's current sub-processors, which shall be updated when new sub-processors are engaged, can be accessed at https://solutions.mckinsey.com/msd/subprocessors/, and McKinsey will provide the Client with a mechanism to obtain notification of such updates. McKinsey may also directly notify the Client in the event additional sub-processors may be required to process Confidential Information in connection with the Services.

    d. If the Client does not approve of any new sub-processor, such approval not to be unreasonably withheld, then Client shall notify McKinsey of such determination and the parties agree to work together in good faith to resolve such concerns. To the extent that they cannot be resolved, McKinsey shall either cease its use of the sub-processor to process the Confidential Information or notify the Client that it may terminate that portion of the Services that require the use of the sub-processor in accordance with the terms set forth in the agreement pursuant to which such Services are provided.

9. Preventing unauthorized access to Confidential Information through the use, as appropriate, of physical and logical entry controls, secure areas for data processing, procedures for monitoring the use of data processing facilities, built-in system audit trails, use of secure passwords, network intrusion detection technology, encryption and authentication technology, secure log-on procedures, and virus protection, monitoring compliance with its policies and standards related to data protection on an ongoing basis. In particular, McKinsey has implemented and complies with, as appropriate and without limitation:

    a. Physical access control measures designed to prevent unauthorized access to data processing systems such as entry controls including the legitimization of authorized persons (e.g., access ID cards, card readers, alarm systems, burglar alarms, video surveillance and exterior security);

    b. Denial-of-use control measures designed to prevent unauthorized use of data protection systems by technical (keyword/password protection) and organizational measures concerning user identification and authentication (e.g., automatically enforced password complexity, automatic disabling and change requirements, firewalls);

    c. Requirements-driven authorization scheme and access rights, and monitoring and logging of system access to permit access to data processing systems to only persons with appropriate access rights;

    d. Data transmission control measures to restrict Confidential Information from being read, copied, modified or removed without authorization during electronic transmission, transport or storage on

data media, and transfer and receipt records. In particular, McKinsey's information security program shall be designed to facilitate the encryption "in transit" of Confidential Information over public networks to protect the security of the transmission.

e. Penetration tests conducted on McKinsey's IT systems and applications;

f. When subcontracting Services involving the processing of Confidential Information, McKinsey shall execute formal agreements with each subcontractor that requires the subcontractor to implement security controls no less stringent than those set forth here and in the attached agreement;

g. Measures to protect Confidential Information from accidental destruction or loss including, as appropriate and without limitation, data backup, retention and secure destruction policies, secure offsite storage of data sufficient for disaster recovery, uninterrupted power supply, and disaster recovery and emergency programs;

h. Measures to ensure that information collected for different purposes can be processed separately including, as appropriate and without limitation, adequate logical separation of Confidential Information (e.g., "internal client capability"/purpose limitation, separation of functions as production and test);

i. Notification to the Client within 30 days of any data subject request should a data subject directly contact McKinsey requesting any correction or deletion of her or his personal data;

j. Return or secure destruction of the Confidential Information as set forth in the Agreement.

10. Taking such other steps as may be appropriate under the circumstances.