Idera Affiliates Data Processing Terms

(for the Customer-Facing DPA)

Details of Processing of BitTitan MigrationWiz.

a. **Address:**
4001 W. Parmer Lane, Suite 125, Austin, TX 78727

b. **Type of Services provided by the Idera Affiliate involving the Processing of Customer Personal Data:**
BitTitan is the premier provider of cloud migration solutions that support leading cloud ecosystems, including Amazon, Google, Microsoft, and ServiceNow.

c. **Data Protection Officer (DPO) Details:**
VeraSafe, LLC
experts@verasafe.com
100 M Street S.E., Suite 600, Washington, D.C . 20003 USA

d. **EU Data Protection Representative:**
VeraSafe Ireland Ltd.
Unit 3D North Point House North Point Business Park New Mallow Road, Cork T23AT2P Ireland
Contact form: https://verasafe.com/public-resources/contact-data-protection-representative

e. **UK Data Protection Representative:**
VeraSafe United Kingdom Ltd.
37 Albert Embankment London SE1 7TL United Kingdom
Contact form: https://verasafe.com/public-resources/contact-data-protection-representative

f. **Subject matter and duration:**
The subject matter and duration of the Processing of Customer Personal Data are set forth in the Main Agreement and all amendments, exhibits, schedules, task orders, addenda, SOWs, purchase orders and other documents associated therewith and incorporated therein.

g. **Nature and Purpose of Processing:**
The nature and purpose of the Processing of Customer Personal Data are set

forth in the Main Agreement and all amendments, exhibits, schedules, task orders, addenda, SOWs, purchase orders and other documents associated therewith and incorporated therein.

h. **Further Processing:**
No further Processing of Customer Personal Data beyond the Processing necessary for the provision of the Services is allowed.

i. **Categories of Data Subjects:**
Data subjects may include Customer's representatives, such as employees, contractors, collaborators, partners. Data subject may also include individuals attempting to communicate or transfer Customer Personal Data to users of the Services.

j. **Categories of Customer Personal Data:**
The Categories of Customer Personal Data that Customer authorizes and requests that BitTitan MigrationWiz Processes include but are not limited to: any customer data stored in the cloud services customer enables migration services for in the MigrationWiz portal.To the extent that customers' data accounts contain personal contact information – such as full name, address, mobile number, email address; details including employer name, job title and function, identification numbers and business contact details; goods or services provided; IP addresses and interest data – any of these present in the source tenant would be migrated to the destination tenant authorized service users identify.

k. **Special Categories of Customer Personal Data to be Processed (if applicable) and the applied restrictions to the Processing of these Special Categories of Customer Personal Data:**
n/a

l. **Categories of third-party recipients to whom the Customer Personal Data may be disclosed or shared by Idera:**
Subprocessors; and
other Idera Affiliates, if applicable.

m. **Frequency of the Transfer of Customer Personal Data:**
The frequency of the transfer of Customer Personal Data is determined by the Customer. Customer Personal Data is transferred each time that the Customer instructs BitTitan to Process Customer Personal Data.

n. **Maximum data retention periods, if applicable:**
The retention period of the Customer Personal Data is generally determined by

the Customer, and is subject to the term of the DPA and the Main Agreement, respectively, in the context of the contractual relationship between BitTitan and the Customer.

o. **The basic Processing activities to which Customer Personal Data will be subject include, without limitation:**
   Collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction for the purpose of providing the Services to Customer in accordance with the terms of the Main Agreement.
p. **The following is deemed an instruction by the Customer to BitTitan to Process Customer Personal Data:**
   i. Processing in accordance with the Main Agreement.
   ii. Processing initiated by Data Subjects in their use of the Services.
   iii. Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Main Agreement.
q. **List of BitTitan MigrationWiz''s Subprocessors:**

   https://www.ideracorp.com/legal/bittitan/subprocessors
r. **Description of technical and organizational security measures implemented by BitTitan MigrationWiz:**
   i. Measures of pseudonymization and encryption of Customer Personal Data:
      i. Encryption of the transferred Customer Personal Data in transit using the Transport Layer Security (TLS) protocol version 1.2 or higher with a minimum of 128-bit encryption;
      ii. Encryption at rest BitTitan MigrationWiz’s software applications using a minimum of AES-256.
   ii. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services:
      i. Restriction of logical access to IT systems that Process transferred Customer Personal Data to those officially authorized persons with an identified need for such access;
      ii. Active monitoring and logging of network and database activity for potential security events, including intrusion;

  iii. Regular scanning and monitoring of any unauthorized software applications and IT systems for vulnerabilities within BitTitan MigrationWiz;

  iv. Access controls at external points of connectivity; and

  v. Expedited patching of known exploitable vulnerabilities in the software applications and IT systems used by BitTitan MigrationWiz.

iii. Measures for ensuring the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident:

  i. Business continuity plans at BitTitan address testing, maintenance and information security requirements which include the defined purpose and scope, and dependencies of the service; a process and persons responsible for its review, update and approval; defined procedures for communication, roles and responsibilities; detailed recovery procedures, manual workarounds, and reference information; and methods for plan invocation.

  ii. Monitors service continuity with upstream providers in the event of provider failure.

  iii. BitTitan infrastructure is hosted on the Azure cloud which meets many international and industry standards for security, monitoring, maintaining, and testing data center utilities and environmental conditions including failovers and redundancy conditions.

iv. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing

  i. As part of BitTitan's Business Continuity plans, IT governance and service management practices are employed to ensure appropriate access control measures for the security of data processing.

  ii. Automated and manual source code analysis and reviews to detect security defects in code prior to production.

        iii. Periodic system audits identify potential security vulnerabilities and internal procedures for prioritization are in place to ensure timely remediation of any issues found.

v. Measures for user identification and authorization:

    i. BitTitan utilizes a variety of information and access management best practices including monitoring, restriction of access, principles of least access, multi factor authentication, access controls, identity management, risk assessments, compensating controls, SSO, delegated authentication, identity federation, strong authentication, password complexity and lockout capabilities.

vi. Measures for the protection of data during transmission:

    i. utilizes data and virtual machines with policy tags and metadata to manage and limit data access and flows.

    ii. utilizes encryption in transit and at rest for our service context in addition to safeguards to ensure that production data can not be replicated in non-production environments.

    iii. Support secure deletion of archived and backed-up data, and provide assurance of sanitized tenant data after a completed migration.

vii. Measures for the protection of data during storage:

    i. utilize encryption in transit and at rest for our service context;

    ii. utilize safeguards to ensure that production data cannot be replicated in non-production environments; and

    iii. support secure deletion of archived and backed-up data, and provide assurance of sanitized tenant data after a completed migration.

viii. Measures for ensuring physical security of locations at which Customer Personal Data are processed:

    i. Restriction of physical to IT systems that Process transferred Customer Personal Data to those officially authorized persons with an identified need for such access.

ix. Measures for ensuring events logging:

    i. Active monitoring and logging of network and database activity for potential security events, including intrusion.

x. Measures for ensuring system configuration, including default configuration:
    i. Policies and procedures have been established with business practices and technical measures to restrict installation of unauthorized software on organization systems, with controls to restrict and monitor such attempts.

xi. Measures for internal IT and IT security governance and management:
    i. Documented security baselines for our infrastructure components, and periodically update out systems to reflect any necessary changes.
    ii. Utilize anti-malware, anti-virus, and threat detection tools, conduct network, system and application vulnerability scans periodically, and patch issues promptly.
    iii. Security events trigger alerts which are promptly reviewed by authorized personnel. Access to logs is restricted to authorized personnel and reviewed both automatically and manually. Change detection and vulnerability assessment tools take into account the virtualized context of the service. Firewalls, virtual and physical separation/segmentation are used to protect the production environment.

xii. Measures for certification/assurance of processes and products:
    i. BitTitan currently holds ISO 27701 and 27001 certificates.

xiii. Measures for ensuring data minimization:
    i. Data minimization is guaranteed during the design and implementation processes.

xiv. Measures for ensuring data quality:
    i. Customer is responsible for data quality and accuracy since the data is provided by the Customer. Manual test cases and automation test fixtures prevent regressions of expected/actual results as part of our SDLC.

xv. Measures for ensuring limited data retention:
    i. Where copies cannot be avoided due to the nature of the migration project requirements, data will be placed into transient storage; however, the process and procedure of the data purged is designed by Microsoft. Control over such temporary storage accounts can be provisioned to exist

within and under the ultimate control of a customer Azure storage account.

ii. Project metadata is restricted to the line items (mailbox/account names) that are required to manage migration status on a user/owner basis. All such project metadata is purged after 180 days of inactivity by default pursuant to BitTitan policy. This policy can be activated on-demand by a customer (through active deletion of the project through the service user interface) or shortened from the default to a lower period by the end user to a shorter desired period if the default duration is considered too long.

xvi. Measures for ensuring accountability:

i. Documentation about how personal data is processed.

xvii. Measures for allowing data portability and ensuring erasure:

i. BitTitan does not sustain/retain personal data for its own purposes. The scope of BitTitan services is to conduct a migration; therefore, its systems, by design, is not a permanent data storage for any personal data. As such, inquiries for a right to export or right to be forgotten do not generally apply to the customer data. Those responsibilities are retained by BitTitan customers, and BitTitan services have no restrictions that prevent its customers from fulfilling those obligations to their end users.

ii. A Process for deleting Customer Personal Data by making a support request.

xviii. Other:

i. Internal policies establishing that

ii. Where BitTitan is prohibited by law from notifying Data Exporter of an order from a public authority for transferred Customer Personal Data, BitTitan shall take into account the laws of other jurisdictions and use best efforts to request that any confidentiality requirements be waived to enable it to notify the competent Supervisory Authorities;

iii. BitTitan must require an official, signed document issued pursuant to the applicable laws of the requesting third party before it will consider a request for access to transferred Customer Personal Data;

iv. BitTitan shall scrutinize every request for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid; and

v. If BitTitan is legally required to comply with an order, it will respond as narrowly as possible to the specific request.