suneratech
Simplifying Cloud | Accelerating Innovation

L1 004 GDPR Suneratech- Privacy Manual

Version- 1.4

Prepared By:	Sai Jyosthna Gandey
Approved By:	Data Protection Officer
Date:	10 June 2020

Document Revision History

PUBLICATION DATE	AUTHOR	REVISION NO	CHANGE DESCRIPTION
10 June 2020	Murali Krishna Dindi	1.0	Initial Version
01 Sep 2021	Murali Krishna Dindi	1.1	Reviewed & Approved by DPO
10 Feb 2022	Sai Jyosthna Gandey	1.2	No changes are made Reviewed & Approved by DPO
05 July 2022	Sai Jyosthna Gandey	1.3	No changes are made, Reviewed & Approved by DPO
24 May 2023	Sai Jyosthna Gandey	1.4	No changes are made, Reviewed & Approved by DPO

Confidentiality Statement	The data contained herein shall not be disclosed, duplicated, or used in whole or in part for any purpose other than to evaluate the proposal, provided that if a contract is awarded to this offer as a result of, or in connection with, the submission of these data, the propose shall have the right to duplicate, use or disclose the data to the extent provided in the agreement. The restriction does not limit the right to use information contained in the data if it is obtained from another source without restriction.
Security Statement	The information contained herein is proprietary to Sunera Technologies and may not be used, reproduced or disclosed to others except as specifically permitted in writing by Sunera Technologies. The recipient of this document, by its retention and use, agrees to protect the same and the information contained therein from loss or theft.
Suneratech Contacts	dpo@suneratech.com (Data Protection Officer)

Document Control

Title: Privacy Manual	
Document No	L1 004
Revision Status	1.4
Effective Date	10 June 2020
Last Review Date	24 May 2023
Approved by	Data Protection Officer
Author Name	Sai Jyosthna Gandey
Signature	Data Protection Officer
Date	24 May 2023

Contents

1. INTRODUCION

Suneratech, Inc. endeavors to meet leading standards and regulations for data protection and privacy. Suneratech respects and values data privacy rights of data subjects, and makes sure that all personal data collected from the data subjects are processed in accordance to the general principles of lawfulness, fairness and transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Integrity and confidentiality (security), Accountability. The policies and guidelines in this Data Privacy Manual (the "Manual") are based on the requirements of GDPR. This Manual shall inform the data subjects of the Suneratech's data protection and security measures and serve as the guide for data subjects in exercising their rights under GDPR.

2. PURPOSE

2.1 COMPLIANCE WITH LAWS AND REGULATIONS

This Manual defines requirements to help ensure compliance with laws and regulations applicable to Suneratech's collection, storage, use, transmission, disclosure to third parties, retention, disposal and destruction of personal data. This will also help ensure that applicable regulations and contracts regarding the maintenance of privacy, protection and cross border transfer of personal data are adhered to.

2.2 BETTER PERSONAL DATA MANAGEMENT

This Manual will help ensure that the Suneratech manages personal data in an accessible and transparent way. This Manual will help limit the use of personal data to identified business purposes for which it is collected.

2.3 PROTECTION AGAINST SECURITY THREATS

This Manual will help ensure that all of the personal data in Suneratech's custody is adequately protected against threats to maintain its security.

2.4 EMPLOYEE AWARENESS

This Manual will help create an awareness of privacy requirements to be an integral part of the day-to-day operation of every employee and ensure that all employees understand the importance of privacy practices and their responsibilities for maintaining privacy. This will also help ensure that the Suneratech's employees are fully aware of the contractual, statutory or regulatory implications of any privacy breaches. This will help ensure that all employees are aware of the processes that need to be followed for collection, lawful usage, disclosure or transfer, retention, archival and disposal of personal information.

2.5 DATA PROTECTION BY THIRD PARTIES

This Manual will help ensure that all third parties collecting, storing and processing personal data on behalf of the Suneratech provide adequate data protection.

3. Scope

This Manual is applicable to all employees of the Suneratech (regardless of the type of employment or contractual arrangement), and to the suppliers, guests, customers, and business partners who may receive personal information from the Suneratech, have access to personal data collected or processed by or on behalf of the Suneratech, or who provide information to the Suneratech.

4. Processing of Personal Information

4.1 Collection

4.1.1 Collection of personal information

The Suneratech shall not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the Suneratech's functions or activities. The Suneratech may collect personal information only by lawful and fair means and not in an unreasonably intrusive way. Where it is reasonable and practical to do so, the Suneratech will collect personal information about an individual only from the individual alone. If, however, this information is collected from a third party, the Suneratech must act reasonably to ensure the individual is or has been made aware of the matters listed under Privacy Notice.

4.1.2 Collection of Sensitive Personal Information

The Suneratech must only collect sensitive personal information:

a. Where the information is reasonably necessary for one or more of the Suneratech's functions or activities and with the individual's explicit consent.
b. If the collection is required by law, and the collection of sensitive personal information of an individual is necessary, the Suneratech must take reasonable steps to ensure that the individual is aware of Privacy Notice.

4.1.3 Consent

In circumstances where consent is needed, the Suneratech shall obtain the explicit consent of the data subject as evidenced by any of the following modes: written, electronic or recorded means, subject to the rules on authentication provided under existing laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. When necessary, provide the data subject a mechanism through which they can subsequently rescind the permission(s) earlier provided and opt-out.

4.2 Usage

Personal data shall be processed fairly and lawfully, and adequate and not excessive in relation to the purposes for which they are collected and processed. Personal information must be accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

As a general rule, the Suneratech's management and employees must not use personal data about a data subject other than for its primary purpose of collection, unless:

a. The data subject has consented to the use or disclosure; or
b. The data subject would reasonably expect the Suneratech to use or disclose non-sensitive information for a secondary purpose and the secondary purpose is related to the primary purpose; or
c. The Suneratech has reason to suspect that unlawful activity has been, or may be engaged in, and uses or discloses the personal information as required by applicable laws and regulations or as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
d. The use or disclosure is required or authorized by or under law; or
e. The Suneratech reasonably believes that the use or disclosure is reasonably necessary for a specified purpose by or on behalf of an enforcement body; or
f. The Suneratech reasonably believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health or public safety or the life or health of a data subject; or
g. Management and employees must only use or disclose personal information in a manner consistent with any Privacy Notice.

4.2.1 Direct Marketing

a. When contacting data subjects for direct marketing in whatever form, the following conditions must be present:
    - The Suneratech provides simple means by which the data subject may easily request not to receive direct marketing communications from the Suneratech.
    - In each direct marketing communication with the data subject, the Suneratech draws to the attention of the data subject, or prominently displays a notice, that he or she may express a wish to "unsubscribe" or "opt-out" or not to receive any further direct marketing communications;
    - The data subject has not made a request to the Suneratech not to receive direct marketing communications.
    - The Suneratech will not charge the data subject for giving effect to a request not to receive direct marketing communications.
b. Personal Information for Direct Marketing. Use of personal information for direct marketing purposes is permitted where:
    - The information has been collected from the data subject and the data subject would reasonably expect the Suneratech to use it for that purpose; or
    - The information has been collected from a party other than the data subject and the Suneratech has either obtained the consent of the data subject.

4.3 Access and Correction

As a general rule, the DPO shall, at the request of the data subject, provide the data subject with access to his/her personal data within a reasonable time after such request is made and will consider a request from the data subject for correction of that information.

4.4 Disclosure and Distribution/Data Sharing to Third Parties

Personal data shall be disclosed to third parties only for identified lawful business purposes and after obtaining appropriate consent from the data subjects, unless a law or regulation allows or requires otherwise.

Where reasonably possible, management shall ensure that third parties collecting, storing or processing personal data on behalf of the Suneratech have:

- Signed agreements to protect personal data consistent with this Manual, Privacy Notices and information security practices or implemented measures as prescribed by law.
- Signed non-disclosure agreements or confidentiality agreements which include privacy clauses in the contracts.
- Established procedures to meet the terms of their agreement with the Suneratech to protect the personal information; and
- Remedial action to be taken in response to the misuse or unauthorized disclosure of personal information by a third party collecting, storing or processing personal information on behalf of the Suneratech.

4.5 Storage and Transmission

The Suneratech shall ensure that appropriate physical, technical and organizational security measures are implemented in personal information storage facilities.

4.6 Retention

We retain personal information that we collect from you where we have an ongoing legitimate business need to do so. If you are a client or vendor (or a representative of a client for a vendor), your personal information will be retained for a period of time to allow us to provide or receive the relevant services (as the case may be) and to comply with applicable legal, tax or accounting requirements. We will not retain your information for longer than is necessary for our business purposes or for legal requirements.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it or, if this is not possible and we have a legal obligation to do so (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

Guidelines and procedures shall be developed for the retention of personal data. These shall address minimum and maximum retention periods, and modes of storage.

4.7 Disposal and Destruction

Guidelines and procedures shall be developed for the secure disposal and destruction of personal data to prevent further processing, unauthorized access, or disclosure to any other party or public, or prejudice the interests of the data subjects. These should address the category of risk ratings assigned for the personal data. These shall also address disposal process on, but shall not be limited to, the following types of storage:

- files that contain personal data, whether such files are stored on paper or magnetic media.
- computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life, especially storage media, provided that the procedure shall include the use of degaussers, erasers, and physical destruction devices, among others; and
- offsite storage or archives.

Upon the expiration of identified lawful business purposes or withdrawal of consent, the Suneratech must take reasonable steps to securely destroy or permanently de-identify or anonymize personal information if it is no longer needed. Data may be anonymized, or pseudonyms used, as deemed appropriate and as may be applicable, to prevent unique identification of an individual.

5. The Rights of a Data Subject

Rights of Data Subject	Description
Withdraw consent	If you have given your consent to processing of personal data relating to you and wish to withdraw it.
Right of access	If you want a confirmation that we process personal data relating to you, information about the processing, access to the personal data, or a copy of it.
Right to rectification	If the personal data relating to you is incorrect or needs updating. This also includes making supplementary statements.
Right to erasure	If you want us to delete personal data relating to you, provided that certain conditions are met.
Right to restriction of processing	If you want us to stop processing personal data relating to you, but not delete it.

Right to data portability	If you want a copy of the personal data relating to you or want to have it transferred to another company.
Right to object to processing	If you have reason to believe that our processing of personal data relating to you does not meet the high ambitions we have set out, you may object to the processing.

6. Security Measures

Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect such personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination. The following gives a general description of those measures.

6.1 Organizational Measures

6.1.1 Compliance Monitoring and Reporting

To ensure compliance with the GDPR, the Suneratech shall undertake the necessary steps as follows:

- Appointment and registration of a DPO for Privacy
- Establishment of a Privacy Management Program, which includes an implementation plan of data privacy and protection controls.
- Conduct a Data Privacy Impact Assessment ("DPIA") for manual and electronic systems that process personal data
- Conduct training and awareness to promote entity-wide compliance with applicable laws and regulations
- Record and/or document activities carried out by the DPO to ensure compliance with GDPR and other relevant policies.
- Non-compliance with this Manual may result in a breach of the Data Privacy Policy, the GDPR and other applicable laws. Instances of noncompliance with privacy policies and procedures shall be documented and reported and, if needed, corrective and disciplinary measures shall be taken on a timely basis.

6.1.2 Conduct DPIA

- The organization shall conduct a DPIA relative to all activities, projects and systems involving the processing of personal data
- In the conduct of DPIA, personal data flow diagrams may be prepared to support the assessment made. These personal data flow diagrams should be regularly updated, as needed, or at least annually.
- In the conduct of DPIA, prepare and consolidate the personal data processing systems (whether automated or manual) in compliance with the legal and regulatory requirements of the GDPR. These personal data processing systems should be regularly updated, as needed, or at least annually.

6.1.3 Data Privacy Trainings

The Suneratech shall conduct trainings on data privacy and security at least once a year to keep its employees and personnel generally aware of personal data privacy and protection and to make them familiar with the Suneratech's policies and practices for compliance with the law.

For training to be effective, it should:

- Be given to new employees and should be conducted periodically after their employment,
- Cover the policies and procedures established by the Suneratech,
- Be delivered in an appropriate and effective manner, and
- Circulate essential information to relevant employees as soon as practical or if an urgent need arises.

Suneratech shall ensure the attendance and participation of employees in relevant trainings and orientations, as often as necessary.

6.1.4 Duty of confidentiality

All employees and authorized representatives of contractors in the name of the Suneratech shall be required to sign a Non-Disclosure Agreement which fully details their duty of confidentiality as regards to the personal data to which they are exposed to and as regards the personal data are shared to them, in the case of third-parties, in the performance of their specific job functions. All employees and authorized representatives of contractors of the Suneratech who have access to personal data shall:

- Operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.
- Not make use of personal data, except for the purpose required by their specific job functions.
- Not share personal data to any person or entity, except as allowed by data sharing agreements or applicable laws.
- Take such steps as are reasonable to preserve the confidentiality of personal data.
- Not reproduce personal data, except to the extent required by their specific job functions.

The employees' and authorized representatives of contractors' duty of confidentiality remains as a continuing obligation to the Suneratech for an indefinite period and extends beyond any termination of their employment period or contract. The Suneratech reserves the right to take disciplinary action, up to and including termination for violations of the Non-Disclosure Agreement.

6.1.5 Review of Data Privacy Manual

This Manual shall be reviewed at least annually, or earlier if deemed required, to check compliance with privacy policies and procedures, commitments and applicable laws,

regulations, service-level agreements, and other contracts, and must be documented. For this purpose, the DPO shall lead the review and/or revision of policies detailed in this Manual. In addition, the Legal Department may review any conflict between the Policy/Guidelines and any local law and make recommendations to Senior Management and the Board of Directors, as necessary, who shall review and approve this Manual at least on an annual basis.

6.2 Physical Security Measures

The Suneratech recognizes the need to implement security measures to monitor and limit access to the facility containing the personal data, including the activities therein. As such, the physical security measures implemented shall provide for the actual design of the facility, the physical arrangement of equipment and furniture, the permissible modes of transfer, and the schedule and means of retention and disposal of data, among others. This physical security measures will also help ensure that mechanical destruction, tampering and alteration of personal data under the custody of the organization are protected from man-made disasters, power disturbances, external access, and other similar threats.

6.3 Technical Security Measures

The Suneratech recognizes the need to implement technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access.

6.3.1 Technical Security Policies and Procedures

a. Access controls

The Suneratech shall establish logical access control policy and procedures to limit access to systems processing personal information only to authorize personnel based upon assigned roles and responsibilities.

b. Monitoring for security incidents and personal data breaches

The Suneratech shall use systems (e.g., intrusion detection system) to monitor security breaches and alert the Suneratech of any attempt to interrupt or disturb the system. When deemed appropriate, conduct also personal data breach exercises.

c. Process for regular testing, assessment and evaluation of effectiveness of security measures

The Suneratech shall review security policies, conduct vulnerability assessments and perform penetration testing within the Suneratech on a regular schedule.

d. Backup, restoration and recovery of personal data

The Suneratech shall maintain a backup file for all personal data within its possession for recovery and restoration purposes in cases of data breach or security incidents.

e. Network security

The Suneratech shall deploy security measures on a network level to protect its underlying network infrastructure from unauthorized access, disclosure, erasure, and modification of personal data.

f. Encryption, authentication process, and other technical security measures that control and limit access to personal data

Controls shall be implemented to desktops, mobile devices, servers, and other devices used for accessing, processing, transmitting, and storing personal data to protect against possible data breaches At the minimum, the controls for the following should be established:

- Patch management procedures
- Anti-virus and Malware protection
- Encryption
- Online access to personal data
- Emails
- access management
- Software development and change management procedures

7. Security Incident and Breach Response and Notification

A DPO shall be responsible for ensuring immediate action in the event of security incident or personal data breach. DPO shall conduct an initial assessment of the security incident or personal data breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the security incident or personal data breach.

8. Inquiries and Complaints

The DPO of the Suneratech should receive all inquiries and complaints related to the privacy of the data subject as well as entertain and institute an investigation in relation thereof. Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the Suneratech, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the Suneratech at DPO@suneratech.com and briefly discuss the inquiry, together with their contact details for reference.

9. References

9.1 References With Policies and Procedures

1) L1 001 GDPR Suneratech - Technical and Organizational Measures (TOM)
2) L1 002 GDPR Suneratech - Data Privacy Policy
3) L1 003 GDPR Suneratech - Data Protection By Design and Default Policy
4) L1 005 GDPR Suneratech - Supplier Data Processing Agreement
5) L1 006 GDPR Suneratech - Data Protection Impact Assessment

6) L1 007 GDPR Suneratech - Roles & Responsibilities of Data Protection Officer
7) L2 001 GDPR Suneratech - Data Breach & Incident Handling Procedure
8) L2 002 GDPR Suneratech - Data Subject Access Request Procedure
9) L2 003 GDPR Suneratech - Data Subject Rights Procedure

Sunera Labs

AUTOMATE | MIGRATE | INNOVATE

USA |INDIA |SINGAPORE | UAE | CANADA

suneratech®