



## Data Privacy Policy

Version 1.0

SLK Internal Information. All rights reserved.

**Document Template ID:** D-ISMSPD; Ver. 1.0

©2024 SLK SOFTWARE PVT LTD. ALL RIGHTS RESERVED.

## Contents

<b>1</b>	<b>INTRODUCTION</b> .....	<b>3</b>
<b>2</b>	<b>ISO/IEC 27001 CONTROL REFERENCE</b> .....	<b>3</b>
<b>3</b>	<b>SCOPE</b> .....	<b>3</b>
<b>4</b>	<b>ACRONYMS USED</b> .....	<b>3</b>
<b>5</b>	<b>POLICY</b> .....	<b>3</b>
5.1	DATA PRIVACY AND PROTECTION OF PII .....	3
5.2	DATA PRINCIPAL RIGHTS.....	4
5.3	PRIVACY AND PII PROTECTION STANDARDS .....	5
5.4	PRIVACY NOTICE .....	6
5.5	PRIVACY BREACH .....	6
<b>6</b>	<b>KEY PERFORMANCE INDICATOR</b> .....	<b>7</b>
<b>7</b>	<b>REFERENCES</b> .....	<b>7</b>
<b>8</b>	<b>REVISION HISTORY</b> .....	<b>7</b>

## 1 Introduction

The purpose of this policy is to define adequate security controls to protect the privacy and protection of the PII information collected, processed, stored, and managed by SLK Group according to applicable law and regulations, and contractual requirements.

## 2 ISO/IEC 27001:2022 Control Reference

- A.5.34 – Privacy and Protection of PII

## 3 Scope

This policy is applicable to:

- a. Information and information processing systems (including but is not limited to, documentation, personnel, hardware, software, physical and logical controls, network communication systems and data that are in possession of or using facilities) owned by SLK.
- b. All employees, contractors and service providers working for SLK, and using its information and information systems.

In case of any conflict, applicable laws & regulations shall always supersede this policy.

## 4 Acronyms Used

Acronym	Expanded Form
ISMS	Information Security Management System
CISO	Chief Information Security Officer
ESGC	Enterprise Security Governance and Compliance
IT IS	Information Technology Infrastructure Services
PPM	People Process Management
L&D	Learning and Development
DPO	Data Privacy Officer
GDPR	General Data Protection Regulation
EEA	European Economic Area
PII	Personal Identifiable Information
SLK/SLK Group	SLK Software, Avo Automation

## 5 Policy

### 5.1 Data Privacy and Protection of PII

- a. SLK group is committed to embed the data privacy principles into every business activity that is performed within its control to protect the PII of all interested parties.
- b. SLK group shall develop and implement adequate security measures for the preservation of privacy and protection of PII.
- c. Appropriate roles and responsibilities shall be defined and communicated to preserve privacy and protection of PII to comply with relevant legislation and regulations.

- 
- d. Data Privacy Officer (DPO) shall be identified and appointed who shall be responsible to provide guidance to people, service providers and other interested parties on their individual responsibilities and specific security measures that should be followed.
  - e. Changes or updates shall be monitored regarding the applicable privacy law and regulations to reflect it on SLK privacy policy, notice and practices.
  - f. Following principles shall be considered.
    - Lawfulness, Fairness and Transparency: data shall be processed legally, fairly, and transparently.
    - Purpose Limitation: use of personal data only for the purpose specified at the time of obtaining consent of the Data Principal
    - Data Minimization: collection of only as much personal data as is necessary to serve the specified purpose.
    - Accuracy: ensuring data is correct and updated
    - Storage Period Limitation: storing data only till it is needed for the specified purpose.
    - Integrity and confidentiality: principle of reasonable security safeguards
    - Accountability: through adjudication of data breaches and breaches of the provisions of the applicable privacy act and imposition of penalties for the breaches
  - g. PII shall be stored, processed, or transmitted in a manner that is accurate, adequate, relevant, and limited to what is necessary and according to business needs and PII retention that was defined in data Principal's consent and privacy notice.
  - h. Ongoing confidentiality, integrity, availability and resilience of processing systems and services shall be ensured. PII shall not be used for testing, training, and research purposes.
  - i. Appropriate security controls shall be implemented to protect PII against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organizational measures.
  - j. SLK regularly test, assess, and evaluate the effectiveness of technical and organizational measures for ensuring the security of the processing the PII and other relevant data.
  - k. PII shall be regularly reviewed at defined frequency and deleted based on business needs or PII retention period that was defined in data principal's consent and privacy notice.
  - l. Periodic data privacy assessments of PII and other relevant data shall be performed.

## 5.2 Data Principal Rights

- a. Where the data principal exercises a right under applicable privacy law, SLK shall respond by taking any action required by the relevant privacy law, unless the request is obviously unfounded or excessive. SLK shall take the relevant action within one month of receipt unless a different time-period is set by applicable privacy law.
  - b. This applies to:
    - Right to get his/her authorization for collection, use, maintaining, and sharing of (PII) prior to its collection; OR prior to any new uses or disclosure of previously collected PII.
    - Right to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.
    - Right to withdraw his or her consent at any time.
-

- 
- Right to access or get a copy of PII data held by SLK.
  - Right to rectification of inaccurate or incomplete personal data
  - Right to erasure (Right to be forgotten) of individual personal data.
  - Right to restrict Data Processing or limited processing of their personal data
  - Right to be notified about the processing of their personal data, including the purpose, legal basis, and relevant information about the data processing activities
  - Right to data portability of their personal data in a structured, commonly used, machine-readable format from SLK to transmit it to another, where technically feasible.
  - Right to object to the processing of their personal data in specific circumstances, such as for direct marketing purposes
  - Right to respond to his/her complaints, concerns, or questions.
  - Right to lodge a complaint with a relevant data protection authority or regulatory body if they believe their data protection rights have been violated.
  - Right to access SLK Privacy notice.
  - Right to access all his information in SLK's PII inventory.

### 5.3 Privacy and PII Protection Standards

- a. Principle of "Privacy by Design" and "Privacy by Default" shall be adopted to ensure that privacy requirements are satisfied on current, new, or significantly changed systems that collect or process PII.
- b. SLK shall apply suitable data encryption controls to protect PII when data at rest and in motion.
- c. PII data shall not be used in non-production environment unless data masking or data obfuscation technique is applied.
- d. Any transfer of PII shall be based on data principal consent or request.
- e. Approved privacy requirements (collection, use, processing, and sharing) shall be established, and documented for contractors, processors, and service providers; and include it in contracts.
- f. Processing activities shall be recorded that contain but not limited to:
  - Name and contact details of the controller and processor.
  - Purposes of the processing PII
  - Description of the categories of data principal's and of the categories of personal data
- g. Information about user activities on the Internet together with any information that would result in user being identified shall not be used without his consent.
- h. Information collected by software utilities (cookies, single-pixel gif images) shall not be associated with username or email address, at the time of the user visiting the sites.
- i. Controls shall be implemented to safeguard the privacy of the user's identifiable information from unauthorized access or improper use and shall continue to enhance security procedures as new technology becomes available.

- 
- j. Identifiable information can be used to investigate and help prevent potentially unlawful activity or activity that threatens the network or otherwise violates the user agreement for that service.
  - k. Data Principal shall be provided with at least the following information before collecting PII:
    - Purposes of processing the information
    - Any further information regarding the specific circumstances in which personal information is collected, such as:
      - The recipients of the information
      - Whether submission of information is obligatory or voluntary, as well as the impact of failure to submit such information.
      - The existence of the right to access, update or remove personal information.
      - Whether personal information will be used for marketing purpose.
  - l. When SLK uses other agents, contractors, or companies to perform services on its behalf, protection of sensitive critical data such as business, commercial/financial data etc., shall be ensured in consistent with this policy.
  - m. Users those who use, or access PII shall be provided with required training from ESGC department in coordination with PPM and L&D team to protect the privacy of the information by implementing required data security controls including access controls, password security, encryption, proper methods of disposal.

#### 5.4 Privacy Notice

- a. Privacy Notice displayed to the user clearly communicate, at least the following information:
  - SLK's commitment to privacy and security.
  - Purpose for collection of personal information.
  - Method of information processing.
  - Controls for protection of personal information (PII).
  - Usage of tools such as cookies to collect personal information online.
  - Details of information such as IP address, domain information captured about the user.
  - Period for which the PII will be stored.
  - Sharing of information with third parties.
  - Data principal rights to access of personal information.
  - Details to contact SLK for queries on processing personal information.

#### 5.5 Privacy Breach

- a. Documented and approved Information Security Incident Response Plan and Procedure shall be maintained to address breaches related to privacy and protection of PII.
- b. If breach occurs with a probability to result in a risk to the privacy or protection of PII, incident shall be handled as per Information Security Incident Response Plan and Procedure plan to minimize the impact and shall be communicated the PII breach to the data principal without delay.

- c. Breaches shall be handled in accordance with relevant laws and regulations and contractual requirements.

## 6 Key Performance Indicator

Srl.	KPI Definition	Frequency
1.	Number of breaches occurred related to data privacy and protection of PII	Half Yearly
2.	Number of issues/findings reported in internal audits or customer assessments related to data privacy and protection of PII	Half Yearly

## 7 References

Srl.	Document Name
1.	Digital Personal Data Protection Bill (DPDP) - 2023
2.	General Data Protection Regulation (GDPR)
3.	Gramm–Leach–Bliley Act (as applicable)
4.	California Consumer Privacy Act (as applicable)

## 8 Revision History

Date of Revision	Version	Description/Reference	Author	Reviewed by	Approved by	Approved Date
15-Feb-2024	1.0	Updated to ISO 27001:2022 Version ISMS CR-2024-01	Deepak A Thiraviam (Lead – ESGC)	Mukund Rangaswamy Srinivas (Group General Counsel-Legal) Raghavendra K (Deputy CISO) Anand K Deshpande (Lead – ESGC)	Shaila Udupa (CISO)	23-Mar-2024