SSH Privacy Management Policy

Document & Data Control

1. Document Information

Name:	SSH Privacy Management Policy
Version:	1.2
Author(s):	IS & Compliance Manager
Reviewer:	GM
Approver(s):	Directors
Creation Date:	07/12/2024
Distribution:	All Staff
Issue Date:	07/28/2026

2. Revision History

Author	Date	Version	Description
Fawad Qamar	07/12/2024	1.0	Initial Version
Ali Murtaza	10/17/2025	1.1	Minor Changes as per the ISO 27701 requirements
Ali Murtaza	07/28/2026	1.2	Update the Scope and added privacy policies section for example: Training, Privacy Policy, Access Control etc

Copyright © SUPPORT SOLUTIONS HUB (PVT) LTD.
All rights reserved Unauthorized copy or use of this document is strictly prohibited

1 Introduction

Support Solutions Hub (Pvt.) Ltd. ("SSH") is committed to safeguarding the privacy, confidentiality and security of Personally Identifiable Information ("PII") processed on behalf of its Clients.
Within the defined scope of its Privacy Information Management System, SSH acts solely as a **PII Processor**, while its Clients act as **PII Controllers** and determine the purposes and means of processing.
This Privacy Policy describes how SSH accesses, uses, stores, transmits, retains and protects Client PII in accordance with:

- The Client's documented processing instructions;
- Applicable contractual obligations;
- Relevant legal and regulatory requirements; and
- ISO/IEC 27701:2019.

SSH shall process PII only for authorized purposes and shall not use, disclose or process Client PII for its own independent purposes. Appropriate administrative, physical and technological controls shall be implemented to protect PII against unauthorized access, use, disclosure, alteration, loss or destruction.

2 Scope and Applicability

This Privacy Policy applies to all Personally Identifiable Information (PII) processed by Support Solutions Hub (Pvt.) Ltd. ("SSH") on behalf of its Clients in connection with the provision of Contact Centre and Business Process Outsourcing (BPO) services.
The Policy applies to all SSH employees, locations, contractual personnel, consultants, approved third parties and service providers who are authorized to access or process Client PII.
All such personnel and parties shall process PII only:

- For authorized business purposes;
- In accordance with the Client's documented instructions;
- Within the scope of their assigned roles and access privileges;
- In compliance with applicable contractual, legal and regulatory requirements; and
- In accordance with SSH's privacy and information-security policies, procedures and controls.

This Policy applies to all systems, applications, communication channels, records and facilities used by SSH to process Client PII within the defined scope of its Privacy Information Management System.

Copyright © SUPPORT SOLUTIONS HUB (PVT) LTD.
All rights reserved Unauthorized copy or use of this document is strictly prohibited

3 Roles and Responsibilities

Top Management shall provide resources and oversight for privacy management. The Information Security and Compliance Department shall coordinate privacy compliance, risk assessments, incident management and audits. Department Heads shall ensure implementation of privacy controls, while all employees shall protect PII and immediately report suspected privacy incidents.

4 Purpose of Processing PII

We process PII only for the specific purposes outlined in our contractual agreements with Clients. These purposes may include, but are not limited to, providing services, processing transactions, ensuring data security, and complying with applicable laws and regulations. All processing activities are conducted in line with the documented instructions of the Client.

5 PII Inventory and Processing Records

SSH shall maintain appropriate records identifying the categories of Client PII processed, processing purposes, applicable systems, authorized users, retention requirements, transfer locations, recipients and implemented security controls. These records shall be reviewed and updated whenever processing activities change.

6 Data Transfers Between Jurisdictions

6.1 Cross-Border Data Transfers

We do not transfer PII to jurisdictions outside of the Client's home country or to international organizations, as necessary to fulfill contractual obligations. If such transfers occur, we will notify the Client and provide the basis for the transfer, giving them the opportunity to object or terminate the contract if desired.

6.2 Documentation of Transfer Locations

A documented list of countries and international organizations to which PII may be transferred will be maintained to ensure transparency and regulatory compliance if it happens.

7 Data Disclosures

7.1 Disclosure to Third Parties

We do not disclose PII to third parties specifying what data was processed, to whom, and when, in accordance with our legal and contractual obligations.

Copyright © SUPPORT SOLUTIONS HUB (PVT) LTD.
All rights reserved Unauthorized copy or use of this document is strictly prohibited

7.2 Legally Binding Requests for Disclosure

If we receive a legally binding request for PII disclosure (e.g., subpoena, court order), we will promptly inform the Client. We will only disclose PII when required by law and in compliance with our contract with the Client.

7.3 Non-Legally Binding Requests

We will reject any non-legally binding requests for PII disclosures and consult the Client before disclosing PII, ensuring all actions comply with the terms of the Client agreement.

7.4 Subcontractor Use

We do not engage subcontractors to process PII on Clients behalf. Subcontractors will only process PII according to the Client's documented instructions and the terms set forth in the Client contract if it happens.

8 Processing Instructions and Compliance

8.1 Client Instructions

We ensure that PII is processed solely for the purposes outlined in the documented instructions of the Client. Any deviation from these instructions will require prior written consent from the Client.

8.2 Marketing and Advertising

We will not use PII for marketing or advertising purposes unless we have obtained prior, explicit consent from the appropriate data subject (PII principal). Furthermore, we will not make consent a condition for receiving services.

8.3 Legal and Regulatory Compliance

If we determine that any processing instruction conflicts with applicable laws or regulations, we will inform the Client immediately to enable corrective actions.

8.4 Privacy by Design and Change Management

Privacy requirements shall be considered before introducing new campaigns, systems, software, suppliers, processing activities or significant operational changes. Relevant changes shall be assessed for privacy and security risks before approval and implementation.

Copyright © SUPPORT SOLUTIONS HUB (PVT) LTD.
All rights reserved Unauthorized copy or use of this document is strictly prohibited

8.5 Support for Client Obligations

We will provide the Client with the necessary tools and information to assist them in fulfilling their legal obligations regarding PII, such as responding to data subject requests or ensuring the secure transfer of PII.

9 Data Security and Confidentiality

9.1 Access Control and Confidentiality

Access to Client PII shall be granted only to authorized personnel based on job responsibilities and the principle of least privilege. SSH shall maintain access approvals, unique user accounts, password controls, multi-factor authentication where applicable, periodic access reviews, confidentiality agreements and prompt removal of access when personnel leave or change roles.

9.2 Secure Disposal of Temporary Files

We will securely delete or destroy any temporary files containing PII created during processing, in accordance with documented procedures and within defined timelines. SSH retains PII only for as long as necessary to fulfil the intended processing purposes or as required by Clients or applicable laws. Upon expiry of the retention period, PII is permanently deleted or anonymized using approved and secure methods.

9.3 Secure Data Transmission

Any PII transmitted over a data-transmission network will be subject to appropriate security controls to ensure it reaches its intended destination securely, preventing unauthorized access or loss.

9.4 Privacy Incident and Data Breach Management

Any suspected or confirmed loss, unauthorized access, disclosure, alteration or destruction of Client PII shall be reported immediately through SSH's incident management process. SSH shall contain and investigate the incident, preserve relevant evidence, assess its impact, notify the Client without undue delay in accordance with contractual requirements, implement corrective actions and maintain complete incident records. SSH shall not independently notify PII principals or authorities unless instructed by the Client or legally required.

Copyright © SUPPORT SOLUTIONS HUB (PVT) LTD.
All rights reserved Unauthorized copy or use of this document is strictly prohibited

9.5 Record-Keeping for Compliance

We maintain and update necessary records to demonstrate our compliance with the contractual obligations regarding the processing of PII, in line with the applicable data protection laws and the terms outlined in the Client contract.

10 Subcontractors and Third-Party Processors

10.1 Engagement of Subcontractors

We will only engage subcontractors to process PII on behalf of the Client in accordance with the terms of the Client contract. The Client will be notified before any subcontractor is engaged.

10.2 Training and Awareness

All personnel authorized to process Client PII shall receive privacy and information security training during induction and periodically thereafter. Training records, assessments and acknowledgements shall be maintained as evidence of competence and awareness.

10.3 Subcontractor Changes

Where general written authorization has been provided, we will inform the Client of any changes in subcontractors or processors to give the Client the opportunity to object to the new or replacement subcontractor.

11 Client Rights and Assistance

11.1 Rights of Data Subjects

We assist the Client in fulfilling their obligations to data subjects, including providing access, correction, or deletion of PII, where appropriate. We also support the Client in responding to any data subject requests related to their rights under applicable data protection laws.

11.2 Compliance Support

We provide the Client with the appropriate information to demonstrate compliance with their data protection obligations. This includes facilitating audits and making records available as needed for legal or regulatory reviews.

12 Audits and Compliance Records

12.1 Audit Cooperation

We will cooperate with the Client in any audits or inspections to assess our compliance with this Privacy Policy, contractual obligations, and applicable data protection laws.

Copyright © SUPPORT SOLUTIONS HUB (PVT) LTD.
All rights reserved Unauthorized copy or use of this document is strictly prohibited

12.2 Demonstrating Compliance

We will maintain the necessary records, reports, and evidence to demonstrate compliance with the obligations set forth in the applicable contract regarding the processing of PII.

Privacy Incident and Data Breach Management

13 Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal obligations, or services offered. Any updates will be communicated to the Client and will be posted on our website.

14 Policy Approval and Review

This Privacy Policy shall be reviewed at least annually and whenever significant legal, contractual, technological, operational or processing changes occur. All changes shall be approved by Top Management and communicated to relevant personnel and Clients where required.

Copyright © SUPPORT SOLUTIONS HUB (PVT) LTD.
All rights reserved Unauthorized copy or use of this document is strictly prohibited