solutions by stc

Data Privacy Policy

Table of Contents

Confidentiality Agreement

The information contained in this document is the property of solutions and may not be copied or communicated to a third party or used for any purpose other than that for which it is supplied without the express written consent of solutions by stc.

Document Approval

TITLE
Chief Governance Officer
GM, GRC & Cybersecurity (CS&P)
Director, Enterprise Governance & Compliance
Director, Cybersecurity and Privacy Management (CS&P)
Manager, Data Protection and Privacy Office

LIST OF ACRONYMS USED IN THIS DOCUMENT	
DPO	Data Privacy Officer
DPPO	Data Protection and Privacy Office
NDA	Non-Disclosure Agreement
DP	Data Privacy
CS	Cybersecurity
PIA	Privacy Impact Assessment
SOLUTIONS	solutions by STC
BUs	Business Units
FUs	Functional Units
CST	Communications Space and Technology Commission
CS&P	Cyber Security and Privacy Management

1. Introduction

The Data Privacy Policy is part of the Data Privacy Program within solutions that sets the management intentions for upholding privacy rights of the customers, suppliers, contractors, employees, candidates, and visitors through the entire lifecycle of personal data i.e., data collection, storage/retention, use/processing and deletion or disposal. solutions recognizes that a consistent, repeatable, and sustainable approach to data privacy is therefore necessary to ensure secure and lawful handling of personal data within solutions' environment.

The Privacy Policy may be provided upon request under a Non-disclosure Agreement to customers or other third parties who have a need to understand our commitment to privacy.

2. Purpose

This policy outlines principles and statements on how solutions collects, processes, and uses personal data in compliance with applicable requirements around data privacy. Supplemental policies, practices and Governance documents shall be developed, as needed, to meet the regulatory data protection requirements which may provide for more strict or specific privacy and protection standards than those that are set forth in this policy.

3. Scope

This policy is applicable to all relevant entities having accountability and/or responsibility for processing personal data within solutions by stc (collectively "solutions" or “Company”) including BUs/FUs, employees, vendors, consultants, business partners and contractor personnel regardless of their geographic location.

4. Responsibility

4.1 The CS&P is responsible for reviewing/ updating and monitoring compliance with this Data Privacy Policy

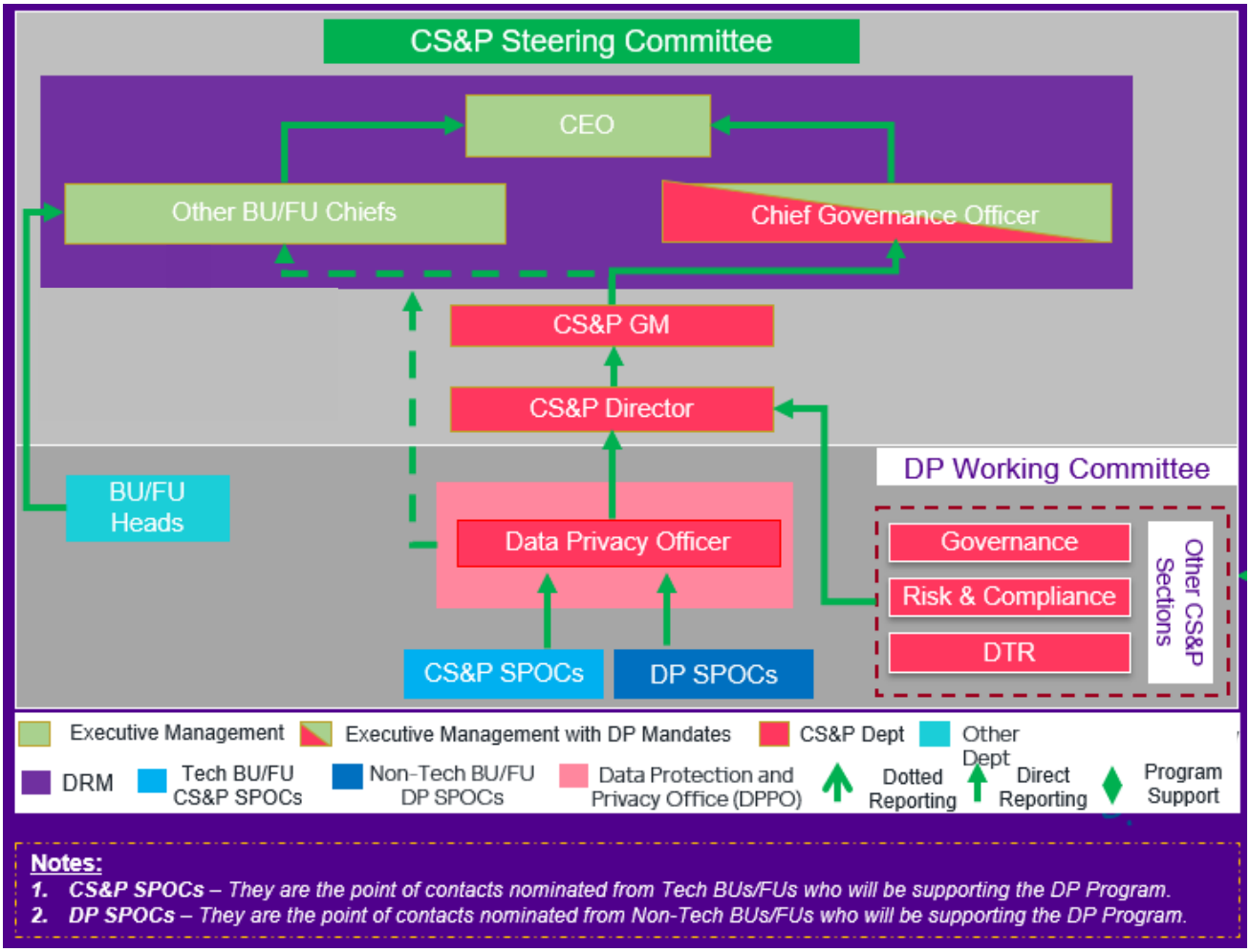
4.2 Each Business Units/ Function Units (BU/FU(s)) are responsible to implement, and maintain the DP requirements as applicable to their operations in accordance to this policy and the DP mandates/operating model.

4.3 All Users are responsible to comply with this policy.

5. Organizational Structure and Roles & Responsibilities

solutions shall define and document Data Privacy Governance Structure and related roles and responsibilities for effective management and implementation of the Data Privacy Program.

Figure 1. Data Privacy Governance Structure



5.1 solutions' CS&P steering committee includes executive management; comprised of CEO, Chief Governance Officer other BU/FU Chiefs or their respective delegates.

5.2 The Chief Governance Officer shall be solutions' executive management member with DP mandates and accountabilities to govern overall DP programs activities and initiatives across solutions.

5.3 The Data Privacy Officer (section Manager of DPPO) shall lead the DP Program and act as DP subject matter expert (SME) across solutions.

5.4 Data Privacy Officer shall present the DP matters to the CS&P steering committee via DRM executive meeting chaired by CEO or his delegate; as and when DPPO needs briefings, support and/or directions; at least once in every quarter.

5.5 The minutes of meetings shall be performed by Corporate Performance Management team and shared with Data Privacy Officer, as needed, where the DRM meetings utilized as CS&P Steering committee meetings.

5.6 The CS&P Director or Data Privacy Office shall present the DP matters to the CS&P steering committee.

Note: Please refer Section '11 – Definitions' for brief description on DRM (Direct Report Management) and CS&P Working Committee

5.7 The table below include the key DP Governance roles and responsibilities at solutions':

Role	Responsibilities
CS&P steering committee	• Overall guidance of Governance and Oversight of Data Privacy Program within solutions. • Ensuring establishment of Data Privacy Vision, Mission, and Data Privacy Objectives for solutions. • Provide direction and support for development of Data Privacy Strategy and Data Privacy Framework. • Provide adequate resources and support for DP Program. • Communicating the importance of effective Data Privacy Program Management and • conforming to the policy's requirements which are achieved through awareness • Refresher programs and induction programs. • Providing direction and support to staff to contribute to the effectiveness of the Data Privacy Program.
Data Privacy Officer (DPO)	• Responsible for developing, initiating, and enforcing data privacy program organizational wide. • Establish and maintain data privacy policies, standards, procedures, and processes to be set as a governance model • Monitor compliance of solutions with applicable laws/ regulations in relation to data privacy; • Develop, establish, and maintain data privacy culture and hygiene practices across solutions and its subsidiaries and customers, where applicable. • Develop and maintain proper alignment with stc's data privacy policies, mandates, and program • Develop, draft and maintain data privacy objectives, framework and policies in alignment with the methodologies and mechanisms established by Enterprise Governance. • Establish Data Privacy Risk Management within solutions; • Oversee the Privacy Incident Management within solutions including handling potential data breaches; • Alert the stakeholders to any risks that might arise about personal data; • Act as a contact point for requests from Data Subjects regarding the processing of their personal data and exercise of their rights; • Liaise Cooperate with regulators in matters concerning data protection.

	• Act as Data Privacy subject matter expert (SME) across solutions and its subsidiaries. • Provide regular and timely update on the status of Data Privacy program initiatives, key privacy risks, compliance issues, and metrics to such as stc, CS&P Steering Committee, AC, sector meeting etc.
Data Protection and Privacy Office (DPPO)	• Support the Data Privacy Officer in developing data privacy processes, procedures, standards, and policies. • Guide DP SPOCs and monitor development and maintenance of Personal Data Inventories and Data Flow Maps. • Carry out periodic compliance assessments to monitor compliance of the solutions' with applicable laws/ regulations in relation to data privacy and protection. • Carry out periodic risk assessment across solutions to identify potential privacy risks and maintain risk registers. • Support the Data Privacy Officer in monitoring the remediation of risks and non-compliances (NCs). • Conduct privacy impact assessments where applicable. • Support the Data Privacy Officer and provide SME support to DP SPOCs in fulfilment of DSAR requests. • Carry out privacy incident response handling activities. • Support the Data Privacy Office in addressing queries from stc and regulators concerning Data Protection. • Provide Data Privacy subject matter expert (SME) support across Solutions and its subsidiaries. • Support the Data Privacy Officer to provide regular and timely update on the status of Data Protection and Privacy program initiatives, key privacy risks, compliance issues, and metrics to such as stc, Management& DRM, AC, sector meeting.
BU/FU Heads	• Ensuring that the resources needed for the data privacy program are available • Communicating the importance of effective data privacy program management and conforming to the policy's requirements • Providing direction and support to staff to contribute to the Effectiveness of the data privacy program • Oversee the overall effectiveness of solutions' data privacy program • Periodically monitor the compliance of the data privacy program to applicable privacy laws/ regulations

	• Ensure adequate guidance and support for treatment of data privacy risks and non-compliances to solutions including risk acceptance.
CS SPoC	• Serve as a Point of Contact within the Technology function for DP matters • Work with respective Technology/Asset owners to implement adequate privacy controls to support the DP Program • Support implementation of technical controls required for privacy risks/NC mitigation • Integrate Privacy requirements into system/software development lifecycle and Technology Change Management Programs • Support DPPO to conduct Go-Live assessments including PIA for Technology products and services • Support respective departments in fulfilment of DSAR requests • Involve DPPO that require SME support and guidance from DPPO • Perform implementation of required data protection and privacy enhancing technologies
DP SPoC	• Serve as a primary Point of Contact within each department (Non-Technology Functions) for DP matters • Develop, review, update, and maintain personal data inventories and data flow maps • Work with the DPPO to identify and document the lawful basis against each data processing activity • Support DPPO in conducting data privacy risk management exercises • Identify risk owners, support risk acceptance, ensure implementation of risk treatment plans and monitor risk status • Support DPPO to identify potential high-risk processing activities that require PIA and support PIA exercise • Work with team members to ensure timely fulfilment of data subject requests assigned by DPPO • Support compliance assessments and performance monitoring exercises conducted by DPPO • Track and ensure timely completion of data privacy training and awareness sessions within respective department • Manage and address queries received from team members on matters related to data privacy • Support other CS&P sections and DPPO during investigation of data privacy incidents and data breaches

6. Data Privacy Principles

solutions has adopted the following principles to govern the lifecycle of personal data and to uphold the privacy rights of Data Subjects:

6.1 Lawfulness, Fairness, and Transparency

Personal Data shall be processed lawfully, fairly, and in a transparent manner.

6.2 Data Minimization

Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes.

6.3 Purpose Limitation

Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes.

6.4 Accuracy

Personal Data shall be accurate, complete, and current as appropriate for the purposes for which they are collected and/or processed.

6.5 Storage Limitation

Personal data should be kept only as long as is necessary for the purposes for which the data is processed or within the limit of applicable regulations for regulated products.

6.6 Integrity and Confidentiality

Personal data should be processed in a manner that ensures appropriate Integrity and confidentiality of the personal data.

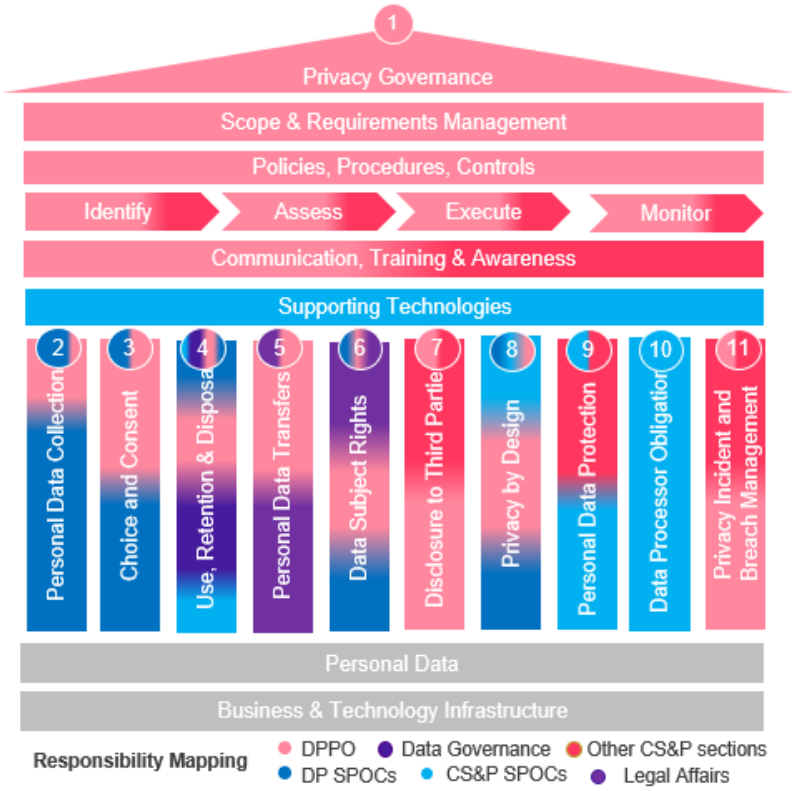
6.7 Compliance with Regulatory Requirements

Personal data should be processed in accordance with the approved policies, standards, procedures, and applicable data privacy laws and regulations.

7. Data Privacy Policy Statements

7.1 Overview

solutions’ DP Framework is aligned to leading standards and applicable regulations. The below figure provides an illustration of solutions’ DP Framework.



The below section provides details of the personal data domains and protocols which form the pillars of solutions’ DP Program and initiatives:

7.2 Data Privacy Governance, Risk & Compliance

7.2.1 Data Privacy Officer (DPO) shall be appointed and shall be responsible for privacy governance, risk, and compliance of privacy related activities and shall be independent of conflicting duties.

7.2.2 Solutions shall appoint a Personal Data Protection Officer (PDPO) considering the nature of processing activities carried out within solutions and where such appointment is mandatory under applicable local/ global privacy laws and regulations.

7.2.3 DPO shall be equipped with the resources, support and training required to perform his/ her role.

7.2.4 DPO shall make his information (name and contact details) accessible and communicated to all relevant stakeholders.

7.2.5 DPO shall develop and maintain the data privacy strategy that defines the vision, mission, goals, objectives tailored to the organization's context and helps meet the needs and expectations of internal and external stakeholders.

7.2.6 DPO shall develop an actionable roadmap to operationalize the strategy, ensure compliance, enable business objectives, meet stakeholder needs and enhance programmaturity.

7.2.7 DPO shall develop and establish the data privacy governance and operating model to further detail the data privacy roles and responsibilities; formally allocated and accepted across solutions.

7.2.8 DPO shall establish a data privacy risk management framework that is integrated into the enterprise risk management program, to proactively identify and manage data privacy risks within solutions.

7.2.9 DPO shall establish a data privacy compliance program to periodically review and monitor solutions compliance to this policy and applicable legal and regulatory requirements for collecting, processing, or maintaining personal data.

7.2.10 DPPO shall support the DPO in carrying out periodic risk and compliance assessments aligned with the established framework and shall be responsible for monitoring the remediation activities.

7.2.11 DPO shall establish a data privacy training and awareness program to ensure all Users shall receive proportionate awareness to their expected role in the data privacy program.

7.2.12 DPPO shall carry out periodic training and awareness programs for solutions employees and contractors.

7.2.13 DPO shall periodically develop, review, and maintain procedures and guidelines aligned to this policy to govern, manage, and operate the data privacy program.

7.3 Personal Data Collection

7.3.1 BU/FU Heads of solutions shall ensure that any personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are collected.

7.3.2 If personal data is collected directly from the Data Subject, solutions shall:

7.3.2.1 Provide a concise, transparent, intelligible, easily accessible, and adequate notice to the Data Subject (employee/ customer/ vendor/ candidates) in physical or electronic format. The notice shall be written in clear and plain language.

7.3.2.2 Notify the Data Subject if there is a change in the purpose of data collection.

7.3.2.3 These disclosures shall be given as soon as possible, and preferably at the first point of contact with the Data Subject.

7.3.2.4 Provide the Data Subject the right to access personal data which include viewing and copying without any charge.

7.3.2.5 Provide the Data Subject the right to modify and update the personal data.

7.3.3 If personal data is collected from someone other than the Data Subject in case of Joint Data Controllers, solutions shall notify the Data Subject of the following, unless the Data Subject has received the required information by other means.

7.3.3.1 The fact of the collection, processing, or transfer of the data by the Joint Data Controller.

7.3.3.2 The nature and purposes of the processing.

7.3.3.3 The recipients or categories of recipients of the data; and

7.3.3.4 The origin of the data.

7.3.4 DP SPOCs shall work with respective departments to maintain records to document the processing activities under its responsibilities.

7.3.5 These records shall be maintained using personal data inventories and data flow diagrams (DFDs).

7.3.6 DP SPOCs shall develop, update, and maintain personal data inventories and DFDs. The personal data inventories and DFDs shall be reviewed, updated, and approved periodically or in the event of any changes to the processing activities.

7.3.7 DP SPOCs shall periodically review personal data collection channels to minimize the collection and processing of personal data from Data Subjects.

7.4 Choice and Consent

7.4.1 Respective departments responsible for collection and processing of personal data shall obtain and record consent from Data Subjects according to the established consent management practices.

7.4.2 Respective departments shall communicate any choices available when personal data is collected or used by a third party or disclosed by solutions to such parties.

7.4.3 As part of Consent Management, solutions shall ensure the following:

7.4.3.1 Consent shall adhere to the principle of freely given, specific, informed, and unambiguous indication of data subject, which means the data subject has a genuine ongoing choice and control over how solutions shall use their data.

7.4.3.2 Request the consent of the data subject using the type of consent (opt-out or opt-in) that is required or appropriate.

7.4.3.3 Ensure that the choices provided to data subject are complete and clear (e.g., how to "opt-out").

7.4.3.4 Inform data subjects of the consequences for failing to consent or to provide their data.

7.4.3.5 Obtain new consent if personal data will be used for a purpose other than originally disclosed to the data subject.

7.5 Use, Retention & Disposal

7.5.1 BU/FU Heads shall ensure processing of personal data is conducted with due regard to the privacy, dignity, and equality of Data Subjects.

7.5.2 Respective departments shall not process personal data in the absence one of the following valid business and legal basis:

7.5.2.1 Data Subject has provided valid consent for the processing of their personal data.

7.5.2.2 Processing is necessary to fulfil solutions contractual obligations towards the Data Subject or an organization

7.5.2.3 Processing is necessary to fulfil solutions legal obligations towards a government or regulatory authority.

7.5.2.4 Processing is necessary to protect vital interests of the data subjects or of another person, in the public interest, or in the exercise of official authority vested in the controller

7.5.2.5 Processing is necessary to protect the legitimate interests of solutions. In such cases, care shall be taken to not pose high risk to data subjects, and to protect the interests and rights of data subjects.

7.5.3 Respective departments shall not process sensitive personal data in the absence of the following valid business and legal basis:

7.5.3.1 Such processing is specifically authorized or required by law.

7.5.3.2 The Data Subject has provided explicit consent to such processing.

7.5.3.3 Where the Data Subject is physically or legally incapable of giving consent, but the processing is necessary by law, for example but not limited to: protecting the vital interest of the Data Subject, Support law suits/ litigations, and Employment. This exemption may apply, for example, where emergency medical care is needed.

7.5.3.4 Processing is necessary for reasons of public interest in public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care.

7.5.3.5 Processing is necessary for the establishment, exercise, or defense of legal claims.

7.5.3.6 Processing relates to personal data which are manifestly made public by the Data Subject

7.5.4 As a Data Controller, respective departments shall only use the personal data for the purposes the data subject has been made aware of in the privacy notice provided to them.

7.5.5 DP SPOCs shall conduct periodic reviews to verify and ensure that divisions and departments that collect/ process personal data appropriately are in compliance with privacy notices, contracts, and this policy.

7.5.6 Employees or Users of Personal Data at all levels shall apply the following while processing personal data:

7.5.6.1 Collection and use of personal data shall be avoided or limited when reasonably possible.

7.5.6.2 The purpose(s) of the collecting or processing of personal data shall be expressly identified by the division or department preparing any new or expanded data collection and processing activity or function.

7.5.7 DP SPOCs and CS&P SPOCs shall ensure to implement reasonable processes to monitor the quality of the personal data it stores/processes as per the solution's Enterprise Data Governance policy.

7.5.8 BU/FU Heads shall define the retention schedule of all personal data stored and processed by their respective departments. Data retention must be identified as per the solution's Enterprise Data Governance policy.

7.5.9 Personal Data shall not be retained longer than required for the purpose it was collected for aligned to legitimate business requirements, and applicable laws and regulatory requirements. However, personal data can be kept for a longer period in case of availability of statutory justification or if personal data connected directly to an open case judicial body.

7.5.10 Personal Data shall be erased if their storage violates any of the data privacy principles or if knowledge of the data is no longer required by solutions or for the benefit of the Data Subject.

7.5.11 Personal Data shall be blocked and restricted, rather than erased, insofar as the law/regulation prohibits erasure, erasure would impair legitimate interests of the Data Subject, erasure is not possible without disproportionate effort due to the specific type of storage, or if the Data Subject disputes that the data is incorrect, and it cannot be ascertained whether they are correct or incorrect.

7.5.12 Disposal of personal data shall be handled with utmost care and shall be governed by the solution's Enterprise Data Governance policy.

7.6 Privacy by Design (PbD)

7.6.1 DPPO under supervision of the Data Privacy Officer shall establish a process to proactively embed privacy requirements into the system architecture and product/ service/ software development lifecycle.

7.6.2 Considerations shall be made for technical land organizational measures to enhance privacy (e.g. data obfuscation/anonymization, data minimization etc.). In addition, appropriate technical and organizational measures shall be considered to ensure that personal data collected or processed is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

7.6.3 Privacy Impact Assessments (PIAs) shall be carried out on processing activities that are likely to result in a high risk to data subject's privacy, rights, and interests.

7.6.4 Procedures shall be developed to elaborate the criteria, triggers, checklists, and methodology for conducting PIAs

7.6.5 PIAs shall be performed for any new launch or major changes made to major products/ services/ technology, which require the processing of personal data.

7.7 Personal Data Transfers

7.7.1 Transfer of personal data outside the Kingdom of Saudi Arabia shall be restricted in accordance with applicable laws and regulatory requirements.

7.7.2 For exceptional situations where, personal data requires to be transferred outside KSA, appropriate mechanisms shall be followed as required by applicable laws and regulations.

7.8 Disclosure to Third Parties

7.8.1 Data Privacy Officer shall establish a Vendor Management process to manage data privacy risks associated with use of third-party vendors which include:

7.8.1.1 Conducting appropriate data privacy due-diligence prior to on-boarding new third-party vendors.

7.8.1.2 Including data privacy responsibilities and obligations as part of contracts signed with third-party vendors including clear instructions around how personal data shall be handled.

7.8.1.3 Based on relevant laws and regulations periodic privacy compliance reviews of third-party vendors.

7.8.2 Respective departments shall clearly notify Data Subjects regarding the category of third parties along with purposes for personal data disclosure.

7.8.3 Personal data shall be shared to third party vendors only for reasons consistent with the purposes for which the data was originally collected or other purposes authorized by law.

7.9 Security of Personal Data

7.9.1 CS&P is responsible to develop and maintain CS policies/ standards/ frameworks aligned to applicable regulatory requirements and leading practices.

7.9.2 CS&P shall assess the data protection and handling measures in accordance to Information Classification and Handling Cybersecurity Standard implemented to safeguard personal data on a regular basis and update the same, where required.

7.9.3 DPPO should support Risk & Compliance to identify key data security requirements aligned to applicable data privacy laws/ regulations to ensure adequate protection of personal data processed within solutions.

7.9.4 CS&P SPOCs and DP SPOCs shall work with respective departments to implement adequate technical and organizational safeguards, in line with this policy, CS policies/standards/frameworks and operating models published by CS&P.

7.9.5 Employees and contractors shall adhere to solutions' internal CS policies, practices and any additional guidance issued around personal data protection by CS&P.

7.9.6 Confidentiality agreements & NDAs covering data protection and privacy responsibilities shall be signed by all employees & contractors on or before their joining date.

7.9.7 Employees, contractors, and third-party vendors involved in any stage of processing personal data shall explicitly be made subject to a requirement of secrecy which shall continue after the end of the employment/business relationship.

7.9.8 Employees, contractors, and third-party vendors shall have access to the personal data necessary for the fulfilment of their employment/ contractual duties.

7.9.9 CS&P shall assess the security measures implemented to safeguard the overall organization on a regular basis and update the same, where required. This assessment is applicable to safeguard measures that directly/indirectly affect personal data.

7.10 Data Subject Rights

7.10.1 Data subjects shall have the right to:

- 7.10.1.1 Request access to copies of their personal data.
- 7.10.1.2 Request information on the processing activities carried out with their personal data.
- 7.10.1.3 Request that their personal data is rectified if it is inaccurate or incomplete.
- 7.10.1.4 Request erasure of their personal data in certain circumstances, except if the data is maintained for regulatory reason.
- 7.10.1.5 Request that the processing of their personal data is restricted in certain circumstances.
- 7.10.1.6 Object to processing of their personal data in certain circumstances.
- 7.10.1.7 Object to, and not to be subject to a decision based solely on, automated processing (including profiling), which produces legal effects or significantly effects on the data subject.
- 7.10.1.8 Withdraw consent.

7.10.2 DPPO under the supervision of the DPO shall review and ensure all requests raised by data subjects are addressed on a timely manner and in compliance with the applicable laws & regulations.

7.10.3 DPO shall advocate the feasibility of fulfilling such requests and provide a reasonable justification in writing (physically or electronically) in case of denial of such requests.

7.10.4 DPPO shall maintain records of such requests irrespective of their fulfilling status.

7.10.5 As a Joint Controller, BU/FU Heads of solutions shall inform its business partners regarding such requests if it pertain to personal data and processing activities that are cover under such arrangements.

7.10.6 Data Subject Request procedures shall be maintained around handling data subject request.

7.11 Data Processor Obligations

7.11.1 Data Privacy Officer shall identify the data processing activities for which solutions is a processor.

7.11.2 Data Privacy Officer shall identify the responsibilities as a data processor and shall develop requirements and guidelines on data processor obligations.

7.11.3 DPO shall ensure that the organization is adhering to its obligations towards the Data Controller by lawfully processing the personal data.

7.11.4 DPPO shall support the Technology BUs in reviewing Data Processing Agreements (DPA) shared by customers and addressing privacy queries raised by customers.

7.11.5 Legal Affairs shall review data privacy obligations before finalizing the contract.

7.11.6 DPPO shall work with CS&P SPOCs to review potential privacy incidents/ breaches that may impact customer data.

7.11.7 Legal Affairs shall support DPPO and Technology BUs to report potential privacy incidents/breaches to customers.

7.11.8 CS&P SPoCs shall develop and implement procedure and processes to support Data Controllers (customers) and fulfil Data Processor obligations

7.12 Data Privacy and Breach Management

7.12.1 Data Privacy Officer shall formulate and implement a data privacy incident and breach management process to ensure that exceptions in data privacy compliance are promptly identified and reported to the DPPO. An incident response team will be formulated upon each incident depending on the incident type.

7.12.2 All the employees shall be aware of the mechanism of raising data privacy incidents.

7.12.3 The DPPO shall work closely with the DTR section to investigate potential data privacy breach incidents resulted from Cybersecurity incidents and track it to closure.

7.12.4 The DPPO shall maintain an inventory of privacy incidents and shall record the lessons learnt.

7.12.5 As a Joint Controller, BU/FU Heads of solutions shall promptly notify its business partners of any data privacy incidents.

7.12.6 Documented procedures shall be maintained to identify, track, review and notify data breaches to relevant regulatory authorities and data subjects.

7.12.7 In case of a Cybersecurity incident which resulted in a privacy incident Cybersecurity Incident Management Framework and Data Privacy Breach Management Procedure should be triggered.

8. Custodian

The custodian for this policy is the Data Protection and Privacy Office (DPPO). DPPO will extend support to Data Privacy Officer with matters related to privacy of personal data. The Data Privacy Officer shall be responsible for the maintenance and accuracy of this policy. Any questions regarding this document shall be directed to DPPO.

9. Conflict Resolution

The CS&P Steering Committee be responsible for resolving conflict or disagreements related to the implementation of this policy including any conflict-of-interest issues that may arise.

Data Privacy Policy is mandatory and shall be followed in all circumstances unless a specific waivers or exceptions have been obtained. Request for waivers form must be filled to include justification and benefits attributed to the waiver and shall be submitted to CS&P Steering Committee for review and approval. A periodic summary report of all the waivers shall be prepared and maintained by the Data Privacy Officer. All waivers shall not exceed one year or a new waiver process shall be initiated.

10. Review and Update

The Data Privacy Officer shall update/review this policy annually, if deemed necessary, and/or if a major change occurred. This policy shall be updated in respect of changes within the privacy field, regulatory changed, change in the market the company operates, and internal changes within the company. Any change in this Policy is subject to approval by the highest approval level.

11. Definitions

Terminology	Explanation
Consent	Freely given, specific, informed, and explicit consent by statement or action signifying agreement to the processing of their personal data.
Data Controller	The entity that determines the purposes, conditions, and means of the processing of personal data.
Data Subject	A natural living person whose personal data is processed by a controller or processor.
Data Subject Rights	Rights through which data subjects can make a specific request to Controller regarding processing of their Personal Data.
Data Processor	The entity that processes data on behalf of the Data Controller.
Data Privacy Officer (DPO)	Data Privacy Officer/ Section Manager is an independent data privacy expert who is responsible for monitoring and enforcement of organization’s data privacy program.
Departments	A sub-unit within a Business Unit in solutions is referred as a Department (For e.g., Digital Products is a department under the BU- Digital solutions).
Joint Controller	Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.
Processing	Any operation performed on personal data, whether or not by automated means, including access, collection, use, recording, disposition, etc.
Personal Data (PII)	Any information regardless of its source or form, which would lead to identifying the individual, or that would render the individual identifiable directly or indirectly, including, names, ID numbers, addresses, contact numbers, licenses and registration numbers, and personal properties, bank account numbers and credit cards numbers, individual’s photos or videos, as well as any other data of personal nature.
Sensitive Personal Data	Sensitive Personal Data is defined as information that if lost, compromised, or disclosed could potentially harm, cause inconvenience, embarrassment, or unfairness to an individual and has high potential of risk to the rights and freedoms of an individual for example revealing racial or ethnic origin, political opinions, religious or philosophical beliefs. Further it is categorized as: Hereditary Genetic Data: Hereditary genetic data, biometric data processed solely to identify a human being.

	Medical Data: Medical data is health-related data. Medical Services: Medical Services are data types where it may show medicines being used along with other health services which are being provided to the subject.
Third Party	Third party, in relation to personal data, means any external organization or external person authorized to process data on behalf of or jointly with the data controller.
Business/Functional Units	Any Business/Functional Units within solutions that own a personal data processing activity.
CS&P SPoC	Is the representative of the system / application. The CS&P SPoC will be the one who drives the day-day data related activities from a Data Management perspective.
CS&P Working Committee	The CS&P Working Committee refers to any regular meetings DPPO have with stakeholders to monitor or ensure implementation and/or effectiveness of DP requirements at operational levels.
Cybersecurity (CS)	Preservation of confidentiality, integrity and availability of information.
Direct Report Management (DRM)	The DRM refers to periodic executive meetings to discuss company related matters. The DRM meetings include solutions' executive management; the CEO, Chief Officers and/or their representatives/delegates. These DRM meetings are also utilized as CS&P Steering Committee meetings as and when DPPO have DP matters to brief, or require support and/or directions from the executive management (CS&P Steering Committee). Corporate performance management is the responsible team at solutions to monitor DRM meetings, record and communicate the minutes of meetings with relevant stakeholders. In addition, Chief Governance Officer is a permanent member in all DRM meetings. Given his mandate towards DP, DPPO ensures continuous presence to discuss and provide feedback on all DP matters.
Employee	The personnel who is employed on a full-time basis and is in the payroll of solutions.
Executive Management	This refers to CEO, Chief Officers of solutions.
CS&P Director	The highest formal full-time dedicated role responsible to execute DP programs and initiatives at solutions
Data Collection	The Data Controller obtains personal data in accordance with the provisions of the system, whether from its owner directly, or from his representative, or from someone who has legal guardianship over him, or from another party.
Data Disposal	Any action which leads to the removal of personal data and makes it impossible to view or restore it again.
Data Disclosure	Enabling any person - except the data controller - to obtain, use or access personal data by any means and for any purpose.
Data Transfer	Transferring personal data from one place to another for processing.

shall	The verbal form ‘shall’ used in the content of this document indicates a requirement.
should	The verbal form ‘should’ used in the content of this document indicates a requirement or recommendation depending on its context, proportional risk(s) and the business value through achieving its compliance.

12. Reference Documents

Internal reference

- Data Privacy Strategy.
- Data Privacy Operating Model.
- Data Privacy Risk Management Framework.
- solution’s Enterprise Data Governance policy.
- CS Corporate Information Security Policy.

External reference

- Personal Data Protection Law, National Data Management Office (NDMO).
- Communications and Information Technology Commission (CITC) Customer Data Privacy Standard.
- STC Data Privacy Policy.