Data Privacy and Protection Policy

Reference

Version 1.0

Author: Nikhil Sugnani

Department: Technology Security

Filed as: Policy

Status: Release

C2 – Vodafone Idea Internal

Scope

This document details the Data Privacy and Protection Policy and standards applicable to Vodafone Idea Ltd., (hereinafter referred as **VIL**)

Document Distribution

All Employees of Vodafone Idea Ltd., its subsidiaries and affiliates

Approving Authorities

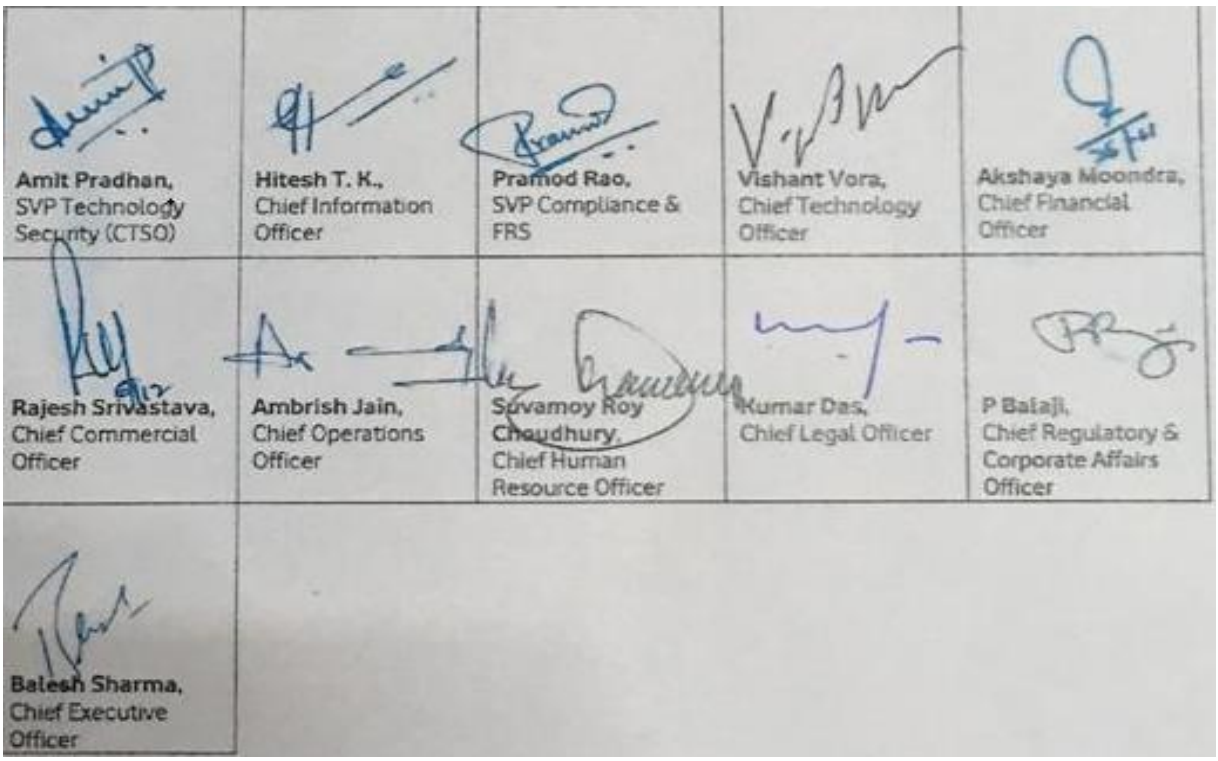

TABLE OF CONTENTS

1. Introduction

1.1: Our Privacy Culture

Background

Vodafone Idea Ltd. (**VIL**) aims to create a culture where everyone in the organization has a clear understanding of how important privacy is to our customers and how to ensure it is respected. Our Privacy Commitments sets out the principles that govern our approach to privacy and how we communicate with customers, employees, vendors and stakeholders on relevant issues – such as designing products to privacy or assisting law enforcement.

The Data Privacy and Protection Policy defines the standards to adhere to when handling personal information of an individual (which is collected, processed, transferred and stored).

The standards set out in this policy are intended to protect the personal information and preserve the privacy of customers, employees, vendors, contractors and other individuals (together termed as "**Individuals**" in this policy) who provide personal information to Vodafone Idea.

What is Privacy?

As per the *International Association of Privacy Professionals (Iapp)*.

"Information privacy is the right to have some control over how your personal information is collected and used."

Objective

The objective of this policy is to ensure that:

- VIL pro-actively addresses customers' expectations concerning their privacy and security in order to create and ensure trust and confidence in VIL and the products and services it provides;
- Compliance with relevant privacy and data protection laws is maintained thereby minimizing legal liability, regulatory risk, brand and reputational exposure; and
- An Individual's personal information is collected and processed in a fair and transparent manner and in compliance with applicable laws and regulations

Scope and Compliance

This Policy applies to (i) all VIL employees' who are on the payroll of Vodafone Idea Limited, including employees on probation and training; (ii) contractors; (iii) suppliers; and their staff, who are engaged by Vodafone Idea Ltd. (iv) contract employees and (v) consultants in the course of their activities, whether the said individuals are paid for their services or working on an honorarium basis or on a voluntary basis.

Compliance levels are monitored on a regular basis and results reviewed by appropriate governance bodies. Any breach will be treated as a serious disciplinary offence and may be subject to disciplinary actions.

All Personal Information and Sensitive Personal Information (SPI) governed by this policy shall be classified as C3: *Vodafone Idea Confidential.*

1.2: Our Privacy Commitments

Respect
We value privacy because of its value to people. It's more than legal compliance – it's about building a culture that respects privacy and justifies the trust placed in us

Openness and honesty
We communicate clearly about actions we take that may impact privacy, we ensure our actions reflect our words, and we are open to feedback about our actions

Choice
We give people the ability to make simple and meaningful choices about their privacy.

Privacy by design
Respect for privacy is a key component in the design, development and delivery of our products and services

Balance
When we are required to balance the right to privacy against other obligations necessary to a free and secure society, we work to minimize privacy impacts.

Laws and standards
We comply with privacy laws, and we will work with governments, regulators, policymakers and opinion formers for better and more meaningful privacy laws and standards

Accountability
We are accountable for living up to these principles throughout our corporate family, including when working with our partners and suppliers

2. Privacy Vision and Principles

2.1 Privacy Vision

VIL is recognized as a trusted guardian of customer and employee privacy and is known for its innovative, fair, responsible and proactive approach to privacy. Our ambition is:

- To be open and transparent about the way we process personal data, to provide fair choices on how such data is processed,
- To manage personal data responsibly and to offer secure services to our customers and employees;
- To gain competitive advantage and manage privacy risks through a world class, demonstrable, consistent and mature privacy program;
- To create opportunities and strategic advantage through Privacy by Design, privacy enabled products and smart privacy related strategies which strike the right balance between privacy and business objectives;
- To exercise privacy thought leadership and influence across society, industry, governments and regulators.

2.2 Privacy Principles

These are the core principles according to which our products and operations must be designed and operated to reach Privacy Vision. VIL privacy principles are:

How we operate

- **Accountability:** We are accountable for living up to these principles throughout our corporate family, including when working with our partners and suppliers. We have in place accountable privacy compliance measures and we monitor and enforce our compliance with these principles.
- **Fairness and lawfulness:** We comply with privacy laws and act with integrity and fairness. We will work with governments, regulators, policy makers and opinion formers for better and more meaningful privacy laws and standards.
- **Openness and honesty:** We communicate clearly about our actions that may impact privacy, we ensure our actions reflect our words and we are open to feedback about our actions.
- **Choice and access:** We give people the ability to make simple and meaningful choices about their privacy and allow individuals, where appropriate, to access, update or delete their personal data.
- **Structured framework:** To establish and embed a structured framework of processes and tools, which deliver a consistent approach to this Policy including Privacy Risk Management (hereinafter referred to as "PRM").
- **Audit, Review & Reporting**: We ensure that there is continued support of Executive and Senior Management for PRM arrangements by demonstrating compliance and improvement through audit and review, and regular reporting.

How we manage and protect data

- **Responsible Data Management and limited disclosures:** We apply appropriate data management practices to govern the processing of personal data. We choose the partners who participate in the processing of personal data carefully and we limit disclosures of personal data to such partners to what is described in our privacy notices or to what has been authorized by our customers.

- **Security safeguards**: We implement appropriate technical and organizational measures to protect personal data against unauthorized access, use, modification or loss.

How we design our products and services

- **Privacy-by-design:** Respect for privacy is a key component in the design, development and delivery of our products and services.

How we make decisions

- **Balance:** When we are required to balance the right to privacy against other obligations necessary to a free and secure society, we work to minimize privacy impacts.

3. Vodafone Idea Privacy Organization and Governance Structure

The Chief Executive Officer of Vodafone Idea is responsible for ensuring this Policy is adopted and implemented. The 'Privacy Council' should consist of stakeholders from key departments managing personal information and will oversee the privacy organization.

The privacy organization should be led by the 'Privacy Officer', who is responsible for privacy governance across Vodafone Idea. She/he should be supported by 'Privacy Manager' who should be accountable for the management of personal information within the organization such that implementation of Vodafone Idea defined framework.

The operations team should comprise of 'Privacy Management Team' and 'Circle Privacy Champions' who are responsible for compliance with the privacy policies on a day-to-day basis. He/ she would liaise with the multiple departments that collect, store, process or dispose of personal information. Privacy Management Team would comprise of Technology Security and representatives from Business and Support Functions. The 'Circle Privacy Champions' should be the coordinators at circle offices as nominated by the Privacy Council.

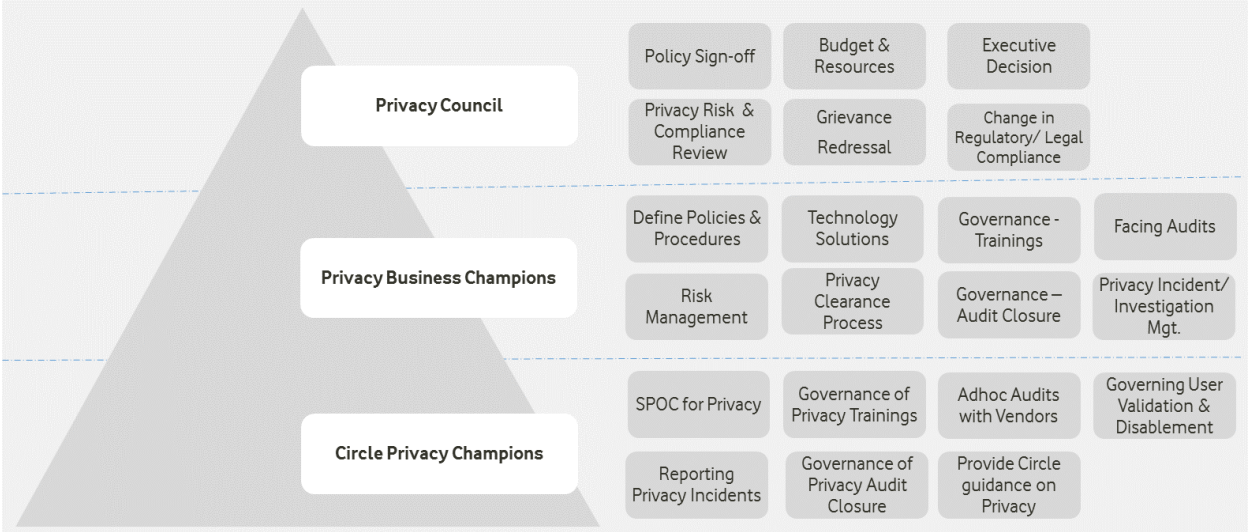

Figure: Vodafone Idea Privacy Organization & Governance Structure

3.1 Privacy Council

The Privacy Council meets bi-annually to provide direction for privacy implementation. The council provide guidance in the areas of regulatory compliance in the existing environment and privacy best practices

Reports to:

Chief Executive Officer (Vodafone Idea)

Role:

The council should provide an oversight and management support to the Information Privacy Organization.

Comprises of:

- CTSO and Privacy Officer
- Chief Human Resource Officer
- Chief Legal Officer
- Head – Compliance & Fraud Risk & Security
- Chief Technology Officer
- Additional invitees to attend the meeting from time to time as required.

Responsibility:

- Supports privacy activities through ongoing consultation, setting strategies and direction for the privacy and data protection policy and initiatives;
- Vets policies and decisions made by its members and approving budgets for privacy and data protection initiatives;
- Review and approve information privacy policy and overall responsibilities assigned to personnel;
- Approve privacy risk and impact analysis and corresponding treatment plans;
- Review and approve all the changes and exceptions to the Personal Information Management System (PIMS);
- Approve major initiatives to augment privacy of personal information;
- Review major information privacy incidents and ensure that the resultant preventive action plan is implemented;
- Review privacy audit reports and monitor the progress of corrective and preventive actions plans and
- Ensure continued compliance of the PIMS with business objectives and external requirements.

3.2 Privacy Officer

Reports to:

Chief Technology Security Officer

Supported by:

- Privacy Council
- Privacy Management

Role:

Privacy officer is the leader of the privacy organization who provides direction and guidance for ensuring organization-wide privacy of information.

Responsibility:

- Lead the Privacy Council meetings and follow up actions;
- Report to the Privacy Council on compliance with the PIMS and overall information privacy environment in the organization;
- Authorizes executive responsibilities for ensuring information privacy within Vodafone Idea;
- Assess the risk of sharing with third parties in consultation with information security and business heads;
- Approving privacy training courses and the associated budget

3.3 Privacy Manager

Reports to:

Privacy Officer

Supported by:

- Privacy Business Champions
- Privacy Circle Champions

Role:

Privacy Manager is accountable for privacy management and ensures compliance to privacy policies and procedures.

Responsibility:

- Develop privacy procedures;
- Management and communication of privacy notices;
- Define and implement controls for protection of personal information of customer, employees, vendors and contractors;
- Perform review of policy and procedures;
- Ensure the implementation of all information privacy related initiatives, components, processes and procedures across the organization;
- Creation of personally identifiable information inventory for the organization.
- Initiate and carry out privacy risk and impact assessment;
- Point of contact for privacy related complaints and queries;
- Handling the privacy incidents raised on privacyofficer@vodafoneidea.com. Review, analyze and escalate the privacy breach incidents reported in the organization;
- Developing positive and constructive relationships with external stakeholders, such as privacy regulators, national and local governments and consumer and privacy advocates;
- Initiate privacy reviews and ensure that action is taken to rectify any shortfalls that are identified;
- Act as a custodian for PIMS documents, systems audits, tools, work papers and reports;
- Consolidates executive responsibility over the implementation and maintenance of VODAFONE IDEA's privacy policies as well as privacy policies specific to his/her LoB;
- Develop and conduct privacy awareness and training program
- Continuously checking that the PIMS reflects changes in legislation, practice and technology.

3.4 Privacy Business Champions

Each business functions should nominate privacy coordinator for their respective functions. Each coordinator should liaise with the privacy team for all privacy related matters.

Liaising with:

- Privacy Manager

Supported by:

- Privacy Manager
- Business function heads

Role:

The Privacy Coordinator is primarily responsible for monitoring and implementation of Privacy Information Management System (PIMS). He/she is accountable for implementing privacy controls across their respective departments.

Responsibility:

- Assisting Privacy Manager in developing privacy policy and procedures, performing risk assessment and privacy impact assessment;
- Assisting Privacy Manager in creating personally identifiable information inventory for the organization;
- Reporting privacy related activities to the Privacy Manager;
- Acting as privacy champions for customers and employees;
- Implementation of new privacy measures across Vodafone Idea;
- Support Privacy Manager in investigating and reporting privacy related breaches;
- Liaising with information security team to implement privacy related controls;
- Support Privacy Manager in rolling out privacy related initiatives;
- Prepare inventory of personally identifiable information for their respective functions as per defined procedures;
- Support and coordinate maintenance of PIMS relating to their respective business processes and applications;
- Coordinate on the implementation of Vodafone Idea's privacy policies and procedures at all locations of the organization, applicable to their respective business functions;
- Assisting employees within their department to comply with the privacy policy and procedures;
- Promoting and maintaining privacy awareness across their circles and
- Apprise the corporate privacy team with respect to the new business process and/or changes to the existing business processes for their respective business functions, and assist in analyzing the impact on the overall privacy environment.

3.5 Circle Privacy Champions

Liaising with:

- Privacy Officer

Supported by:

- Business Head
- Privacy Manager
- Function heads

Role:

The Circle Privacy Champions is primarily responsible for monitoring and implementation of Privacy Information Management System (PIMS). He/she is accountable for implementing privacy controls across their respective departments in circle offices.

Responsibility:

- Assisting Privacy Officer in conducting risk assessment and privacy assessment at circles;
- Reporting privacy related activities to the Privacy Officer;
- Acting as privacy champions for customers and employees;
- Implementation of new privacy measures across Vodafone Idea;
- Support Privacy Officer in investigating and reporting privacy related breaches;
- Liaising with information technology team to implement privacy related controls;
- Support and coordinate maintenance of PIMS relating to their respective business processes and applications;
- Coordinate on the implementation of Vodafone Idea's privacy policies and procedures at all circles of the organization, applicable to their respective business functions;
- Assisting employees within their department to comply with the privacy policy and procedures;
- Promoting and maintaining privacy awareness across their circles and
- Apprise the corporate privacy team with respect to the new business process and/or changes to the existing business processes for their respective business functions, and assist in analyzing the impact on the overall privacy environment.

4. Organisational controls

VIL have in place the necessary organizational controls, requirements and processes to ensure the objectives of this Policy are met. The controls, requirements and processes under this Policy has a defined owner, kept up to date through a regular review cycle, and they shall be made available to all employees through the VIL intranet and training programs.

4.1: Risk Management and Annual Plans

The Privacy related risks at Vodafone Idea is aligned with the risk management framework:

- Creating and updating the risk register – Privacy Officer is responsible for maintaining privacy risk registers, which are then reported to the Board Sponsor.
- Creating and implementing a privacy plan – Privacy Officer is responsible for preparing an annual Privacy Plan which is specifically focused on Privacy risk.

4.2: Privacy Requirements

VIL has pre-defined Privacy requirements in place. These requirements define repeatable ways to solve recurring Privacy issues.

Accountability: Define privacy responsibilities, document the data being processed, conduct privacy risk assessments and control identification (Privacy by Design), and ensure business accountability for implementation of controls and residual risks

Privacy Notice: VIL will provide clear and understandable Notice prior to collection and use of Personal Information.

Permissions and Choices: VIL will obtain and manage necessary permissions for communications content, traffic data, location data, sensitive data, marketing and analytic.

Purpose Limitation and Data minimization: VIL will only collect and process data that is necessary, relevant and compatible with purposes, which were communicated to the data subjects

Data Categorization: VIL will maintain an inventory of personal information collected and processed; all the personal information collected from customers, employees, vendors and contractors are categorized using a twofold approach, viz., Sensitive personal information (SPI) and personally Identifiable Information (PII)

Data Management: VIL will manage data diligently to maintain its accuracy and quality across product life cycle, not retain data for longer than is necessary and ensure rights and obligations related to data carry over to all instances of data.

Disclosure to Third parties: VIL will not disclose personal data to unauthorized governmental agencies and ensure suppliers comply with privacy and security requirements. Data Protection Schedule shall be incorporated in the Supplier contractual agreement.

Safeguarding personal information: VIL will establish safeguards and security programs to protect personal information from unauthorized disclosure, use, modification and destruction.

4.3: Privacy by Design for new products, services and operations (PbDA)

VIL has a defined PbDA process for new products, services and operations development which:

a) Identifies privacy risks and designs privacy safeguarding controls as part of the design and development;
b) identifies what Data is processed, for which purposes and by whom;
c) verifies conformance with Vodafone Privacy requirements before launch; and
d) ensures a corrective plan exists for deviations and agreed upon by the business owner

4.4: Organisational Privacy Impact Assessment Process (OPIA)

VIL has defined an OPIA process across their business which:

a) identifies High Risk Personal Data and / or SPI Processing activities;
b) verifies their conformance with Privacy requirements;
c) ensures performance of regular Privacy Impact Assessments to such activities on a rolling basis; and
d) ensures a corrective plan exists for deviations and that the business owner has approved the significant residual risks

4.5: Supplier management

VIL identifies responsibilities, resources and processes and other suppliers engaged in processing Personal Data and / or SPI. These requirements are integrated into procurement processes and agreements to ensure VIL's suppliers comply with this Policy and applicable regulation and law.

4.6: Training and Awareness

VIL has designed a training and awareness program to ensure that employees and other relevant stakeholders are aware of their Privacy related obligations, which includes recognizing Privacy Month across organization, the mandatory e-learning module on Data Privacy. The Program shall include the following elements:

a) Basic Privacy training of the requirements and processes under this Policy to all new employees and to existing employees on a rolling basis every year;
b) Tailored training for high risk teams and employees, done on a rolling basis every year;
c) Internal publication of this Policy and related requirements, processes and other documents mandated by this Policy;
d) Awareness through Doing What's Right and on-site campaigns together with Internal Communications. Periodic training to ensure complete awareness.

4.7: Privacy Incident Management

VIL has defined Privacy Violations and Consequence Management Model (CMM) for handling privacy incidents, including breaches of confidentiality of Personal Data and / or SPI or other instances of serious non- compliance with this Policy. The incident management procedures shall ensure capability to meet regulatory time limits for notifying authorities or Data Subjects, as the case may be.

The Privacy Officer liaise with the relevant stakeholders to address the privacy complaint, violation or breach. Refer to CMM procedure document for more details.

4.8: Privacy Record keeping

VIL retains Personal Data and / or SPI only for such periodicity as may be necessary, for legitimate business purposes, in accordance with the regulatory requirements and as per requirements under Section 7 of the Information Technology Act, 2000.

5. Operational controls

The following operational controls ensure compliance with this Policy on a product, process and operations level.

5.1: Confidentiality of communications and Sensitive Personal Information/ SPI

VIL has defined the minimum requirements applicable to protecting the content of communications and related communications metadata as well as Personal Data and / or SPI against unauthorized processing (including without limitation listening, tapping, storage or other kinds of interception or analytics).

5.2: Openness and Transparency of Personal Data and / or SPI processing

VIL has defined the minimum requirements to ensure that data subjects (consumers, employees and others whose Personal Data and / or SPI Vodafone Idea Controls controls) are given comprehensive and understandable information about the way their Personal Data and / or SPI is processed at the time of collecting such Personal Data and / or SPI.

5.3: Permissions

VIL has defined the minimum requirements applicable to managing the permissions and preferences related to processing Personal Data and / or SPI and other Data, where required, including without limitation permissions and preferences relating to

a) processing of communications content;
b) processing of communications metadata for marketing or other value added purposes;
c) processing of location Data;
d) accessing information from data subject's devices and personal storages;
e) processing of Personal Data and / or SPI for marketing purposes and profiling;
f) processing of SPI

5.4: Rights of individuals to request access, deletion, portability

VIL has defined minimum requirements applicable to ensuring data subjects can request access to update, delete, or port their personal data (wherever required and appropriate).

5.5: Data management

VIL has defined minimum requirements ensuring that appropriate documentation and inventories of Personal Data and / or SPI processing are maintained, that the accuracy and quality of Personal Data and / or SPI is maintained across the Data life cycle, that Personal Data and / or SPI is not retained for longer than is necessary for the purpose(s) it was collected for and that unnecessary Personal Data and / or SPI is deleted.

5.6: Cross Border Data transfers

VIL ensures the applicable regulation requirements such as but not limited to (Department of Telecom, Telecom Regulation Authority of India.) related to international Data transfers are complied with and that Data is not transferred outside countries where such transfers are prohibited.

5.7: Disclosures of Personal Data and / or SPI to government entities

If VIL receives, a demand from any Law Enforcement Agency to provide assistance related to Data or services hosted or managed by it, such requests must adhere to the law of the land and guidelines issued by the local Government for such assistance.

The Central Government under Section 17 of The Information Technology Act, 2000 is empowered to appoint a Controller of Certifying Authorities for the purposes of this Act. The Controller may take such measures or cease carrying on such activities if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

Any person who fails to comply with any order under the applicable laws shall be guilty of an offence and shall be liable on conviction to imprisonment or to a fine or to both and may also attract penalties and sanctions under Chapter IX of The Information Technology Act, 2000.

VIL shall extend co-operation and assistance as stipulated hereunder:

- Mandatory assistance: A country's laws may require VIL to provide law enforcement assistance. VIL would act only in accordance with the Law Enforcement Assistance requirements.

- Discretionary assistance: If the Law Enforcement Assistance is not mandated by law; and providing assistance would not break a law.

- Legitimate business purpose: To the extent reasonably necessary to protect a legitimate business interest, such as fraud or other crime committed against us, VIL may provide assistance, but only if doing so would not break a law.

5.8: Security for Privacy

VIL ensures that the security baseline requirements and processes include security related privacy requirements:

(a) to protect Personal Data and / or SPI against unauthorized access, disclosure, modification or deletion or loss; and

(b) to ensure the confidentiality, integrity, availability and resilience of the systems and processes where Personal Data and / or SPI are processed during transit and at rest, as further defined in the Information Security Policy.

6. Exceptions and Escalation

VIL employees have a general responsibility to be aware of their privacy related obligations.

An employee with any privacy compliance related concern should, in the first instance, contact the Privacy Officer. Any complaint or query with respect to processing or handling of Personal Data and / or SPI or any violation / breach to this Privacy Policy or any violation/breach involving compromise or suspected compromise to Personal Data and / or SPI shall report to Privacy Officer.

Exceptions to this Policy may be advised by the Privacy Officer.

Potential escalations for issues relating to the implementation or interpretation of this Policy shall follow the principle of escalating to the next level of seniority within the Privacy Program and affected business.

7. Policy Review

The policy is reviewed annually and the Privacy Council approves any updates. The following aspects are considered for revision:

- Changes in the regulatory compliances or legal provisions related to Data Privacy
- Changes or addition of industry standards and technology
- Changes to methods of operating business including changes in the HR policy
- New strategies of business and/ or channels of business/customer outreach expected
- Any other considerations as mandated by EXECO and/ or board of directors.

The revision of this policy and changes therein will be notified, as appropriate, to employees and third parties through appropriate means such as emails, intranet, privacy trainings, and educational posters.

8. Glossary

- **Data Subject** refers to any person whose personal data is being collected, held or processed.

- **Data** in accordance with the Information Technology Act, 2000 means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

- **Information** in accordance with the Information Technology Act, 2000 includes Data, text, images, sound, voice, codes, computer programs, software and Databases or microfilm or computer generated microfiche.

- **Personal information (PII)** means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

- **Sensitive personal data or information (SPI)** - Sensitive personal data or information of a person means such personal information which consists of information relating to:
    - Password
    - Financial information such as Bank account or credit card or debit card or other payment instrument details
    - Physical, physiological and mental health condition;
    - Sexual orientation;
    - Medical records and history;
    - Biometric information;
    - Any detail relating to the above clauses as provided to body corporate for providing service; and
    - Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

9. Annexure I – PII & SPI Inventory

#	Categories	Personal data elements	Classification
1	Personal	Blood Group	SPI
2	Personal	IP Address	PII
3	Personal	Handset Make / Model	PII
4	Personal	Biometric Information of Employees	SPI
5	Professional	CTC Details	SPI
6	Professional	Salary Components	SPI
7	Professional	Employee Investment Details	SPI
8	Financial	Credit Card Number	SPI
9	Financial	CVV Number	SPI
10	Financial	Credit Card Expiry Date	SPI
11	Financial	Bank Account Number	SPI
12	Financial	Bank A/C Holder's Signature	SPI
13	Financial	Bank A/C Holder's Name	SPI
14	Financial	Monthly / Annual (Gross / Net) Income	SPI
15	Subscriber	Consumer Account Number / Customer Id	PII
16	Subscriber	Subscriber's Credit History	PII
17	Subscriber	Details of Previous Payment	PII
18	Subscriber	Subscriber's Usage Details	PII
19	Subscriber	Subscriber's Last Billed Amount	PII
20	Subscriber	PUK Code	PII
21	Subscriber	SIM Number	PII
22	Subscriber	Subscriber's Credit Limit	PII
23	Subscriber	IMEI Number	PII
24	Subscriber	IMSI Number	PII
25	Subscriber	Mobile Number	PII
26	Subscriber	Pensioner's ID Card Number/Student/College ID/ Senior Citizen ID	PII
27	Subscriber	Current Location	PII
28	Subscriber	Services Subscribed	PII
29	Subscriber	Subscriber Talk Plan	PII
30	Subscriber	Current Unbilled Amount	PII
31	Subscriber	Unique Portability Code	PII
32	Personal	Vehicle Registration Certificate Number	PII
33	Personal	Anniversary Date	PII
34	Personal	PAN Number	PII
35	Personal	Customer's Signature	PII
36	Personal	Photographic Image	PII
37	Personal	Mother's Maiden Name	PII
38	Personal	Gender / Orientation	PII

#	Categories	Personal data elements	Classification
39	Personal	Marital Status	PII
40	Personal	Address	PII
41	Personal	Date of Birth	PII
42	Personal	Residence Telephone Number	PII
43	Personal	Passport Number	PII
44	Personal	SIM Contacts / Personal Address Book	PII
45	Personal	Name	PII
46	Personal	Driver's License Number	PII
47	Personal	Voter ID Number	PII
48	Personal	Alternate Address	PII
49	Personal	Alternate Telephone Number	PII
50	Personal	Email ID	PII
51	Personal	Father's Name	PII
52	Personal	Language	PII
53	Personal	Maiden Name	PII
54	Personal	Mother's Name	PII
55	Personal	Nationality	PII
56	Personal	Vehicle Number	PII
57	Personal	Age	PII
58	Personal	Local Reference (for Foreign Customers)	PII
59	Personal	Aadhar / VID number	PII
60	Professional	Employee Salary Details	PII
61	Professional	Employee PF Account Number	PII
62	Professional	Designation	PII
63	Professional	Office Telephone Number	PII
64	Professional	Employee ID	PII
65	Professional	Employee Education Details	PII
66	Professional	Employee Work Experience	PII
67	Professional	Employee Date of Joining	PII
68	Professional	Employee Department	PII
69	Professional	Employee Type	PII
70	Behavioral	SMS Pattern	PII
71	Behavioral	VAS Service Pattern	PII
72	Behavioral	Roaming Pattern	PII
73	Behavioral	Voice Calling Pattern	PII

10. Document History

Identifier	Previous Reference	Current Version	Changes / Remarks
Version 1	August 2018	First Release	