VISION RX LAB

Information Security Management System

Privacy Policy

Vision Rx Lab - IT

VRX/DPDP/POL/003

Document Classification: Internal

Document Release History

Version	Prepared Date	Review Date	Release Date	Prepared By	Reviewed By	Approved By
1.0	23-09-2019	25-09-2019	26-09-2019	Nilanjan Ghoshal (Senior Executive- IT & Systems)	Arijit Saha Senior Website Developer Rekha Roy General Manager – IT & Systems	R K Maheshwary (Associate Director)
2.0	12-08-2024	15-08-2024	26-08-2024	Abhinandan Banerjee (Project Manger- IT & Systems)	Arijit Saha Senior Developer Rekha Roy AVP – IT & Systems	Subha Mitra (VP – IT & Systems)

Document Location

Version	Document Type (Printed/ Electronic)	Location of Document
1.0	Electronic	One Drive
1.0	Printed	Department of IT and Systems
2.0	Electronic	One Drive
2.0	Printed	Department of IT and Systems

Document Distribution

Title	Department	Version	Document Type (Printed/ Electronic)	Date
CEO	Management	1.0	Electronic	27th Sep 2019
AD	Management	1.0	Electronic	27th Sep 2019
CEO	Management	2.0	Electronic	14th Aug 2024
AD	Management	2.0	Electronic	14th Aug 2024

Version	Prepared By	Reviewed By	Approved By
1.0	Nilanjan Ghoshal (Senior Executive - IT)	Rekha Roy General Manager – IT & Systems	R K Maheshwary (Associate Director)
2.0	Abhinandan Banerjee (Project Manager - IT)	Rekha Roy AVP – IT & Systems	Subha Mitra (VP – IT & Systems)
SIGNATURE and STAMP			

Contents

Preface 3
Purpose 3
Scope 3
Policy Control and Distribution 4
Acronyms and Definitions 4
Acronyms 4
Definitions 5
PIMS Planning 6
Leadership and Commitment 6
Review Inputs 6
Review Output 6
Policy 7
Vision of VRX Rx Lens Pvt. Ltd 7
Mission of VRX Rx Lens Pvt. Ltd 7
Commitment to Digital Personal Data Protection (DPDP) 7
WHAT ARE WE GOING TO TELL YOU IN THIS NOTICE? 8
PIMS Objective 8
Organizational roles, responsibilities and authorities 9
Legal Team 9
DPO 9
Internal Audit 9
Planning 9
Actions to Address Risks and Opportunities 9
Planning of Changes 10
Support 10
Resource, Competence & Awareness 10
Codes of Conduct and Certifications 11
Data Inventory, Data Flow and Documentation 11
Communication 12
Operation 13
1- Right of access 13
2- Right to rectification 13
3- Right to restriction 13
4- Right to object 13
5- Right to erasure ("right to be forgotten") 13
6- Right not to be subject to automated decision-making 14
7. Right to data portability 14
8. Infringed Rights and Right to Complain 15
9. Consent withdrawals 15
Internal Audit, Performance Evaluation and Continual Improvement 15

Privacy Policy

Preface

This Data Privacy Policy sets out how Vision Rx Lab Pvt. Ltd. uses and protects any information that you provide Vision Rx Lab. The Data Privacy Policy Manual is an integral part of Personnel Information Management System (PIMS) and describes the operation of Organization, covered under the scope.

Vision Rx Lab has a firm policy of protecting the confidentiality and security of information that we collect from our Customers and Vendor along with other those are directly or indirectly involved with the organization. This has been established, documented and implemented in compliance with the Information Security Policy and the applicable Standards including applicable Statutory & Regulatory requirements

Purpose

The Purpose of the policy is:

1- Align to the purpose and context of the organization and support its strategic direction appropriately
2- Establish the Privacy Policy and PIMS Objectives of Vision Rx Lab
3- Establish Personnel Information Management System necessary to meet the Organization's and Customer Business Objectives, statutory and regulatory requirements
4- Establish methods to measure, monitor and continually improve the processes detailed in organization's Systems and Procedures

Scope

- This policy is applicable to all Vision Rx Lab' employees, interns, associates and business partners who may receive personal information, have access to personal information collected or processed, or who provide information to the organization
- This policy is applicable for all End Customers' Personal data received from Customers and Vendors to process ophthalmic products.
- All employees, Associates, of Vision Rx Lab are expected to support the privacy policy and principles when they collect and / or handle personal information, or are involved in the process of maintaining or disposing of personal information. This policy provides the information to successfully meet the organization's commitment towards data privacy
- The Privacy Policy is an embodiment of Vision Rx Lab Personnel Information Management System and is a part of overall Vision Rx Lab' Policies. It describes the processes to comply DPDP requirements and to meet Data Subject's right. There shall be no exclusions unless and until required by any national and regional regulations, which shall be either captured as a part of the domain specific processes or its equivalent.

Policy Control and Distribution

- Data Protection Officer (DPO) is responsible for distribution or issue of the information available as part of this policy document.
- The contents of this policy are mandatory and cannot be altered or omitted without written authority.
- Any uncontrolled copies, shall not be referred to, or quoted, for any purposes by Vision Rx Lab employee or Customers or external agencies, under any circumstances.

Acronyms and Definitions

Few of the acronyms and / or its definitions provided here may not have been used in this document, but has been provided for easy reference to their definitions

Acronyms

Acronym	Description
PIMS	Personnel Information Management System
CIA	Confidentiality, Integrity and Availability
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPDP	Digital Personal Data Protection
ICO	Information Commissioners' Office
PIA	Privacy Impact Assessment
PII	Personally Identifying Information
SPOC/POC	Single Point Of Contact / Point Of Contact
FAQ	Frequently Asked Questions

Definitions

Term	Definition
Anonymization	The data subject is not or no longer identifiable. Apply anonymization when there is a need to entirely mask / anonymize the actual data (for example, data lying in the DEV database can be anonymized because there is no real reason for the developers to see actual data in the DEV server).
Consent	The individual has given clear consent for VRX to process their personal data for a specific purpose.
Contract	The processing is necessary for a contract VRX has with the individual, or because they have asked VRX to take specific steps before entering into a contract.
Data Controller	The entity / organization who determines the purposes and means of processing personal data (i.e., the client).
Data Processing or touch	This means doing anything with personal data, including viewing, accessing, collecting, recording, organizing, storing, amending, using, disclosing, deleting and transferring personal data or otherwise touching personal data in any way. Note, merely having view access to a client database, constitutes processing for DPDP purposes.
Data Processor	The entity / organization who processes personal data on behalf of a data controller, as per their direction and instruction (i.e., VRX, as a service provider).
Data Subject	The living individual who is the topic / subject of the personal data.
Data Transfer	This is the transfer of personal data from one location to another, it includes viewing or accessing personal data held locally from an offshore location.
Encryption	The process of converting information or data into a code, especially to prevent unauthorized access. Apply encryption where there is significant risk of processing (for example, high volume of data processing, transfer of data to another country, retention of data for a considerable amount of time due to compelling reasons).
Exemptions	Member States can introduce exemptions from the DPDP's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary
Legal obligation	The processing is necessary for VRX to comply with the law (not including contractual obligations).
Legitimate interests	The processing is necessary for VRX's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
Personal Data	Any information relating to an identified or identifiable individual, who can be directly or indirectly identified in particular by reference to an identifier. This type of data attract protection. E.g., name, address, email ID, phone number, passport, identification number, location data or online identifier, bank account number, employee ID, IP address, dates of birth, social security numbers, cookies etc.
Pseudonymization	Apply pseudonymization when the actual data can be segregated from other stakeholders by providing a pseudo name to the actual data (for example, providing employee Id instead of employee name), such that, the processing can still continue with the provided pseudo name.

Reference : https://www.meity.gov.in https://gdpr-info.eu/

PIMS Planning

Leadership and Commitment

The Executive and Senior leadership are committed to the development and implementation of the PIMS and promoting continual improvement of its effectiveness by:

1. Defining and propagating the organization's PIMS Policy
2. Ensuring that the PIMS Objectives are aligned to Business Objectives / strategic direction of the organization and are compatible to the Business context and organization's strategic direction thus achieving its intended results
3. Ensuring the integration of the PIMS requirements into the organization's business processes
4. Promoting the use of the process approach and risk-based thinking
5. Conducting Management Reviews
6. Engaging, directing and supporting human resources and other relevant management roles to demonstrate their leadership as part of their responsibilities. Ensuring the availability of adequate resources in terms of infrastructure and manpower. Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility
7. Communicating the importance of effective personal information management and of conforming to the PIMS requirements
8. Promoting continual improvement

Opportunities for improvement are also identified using multiple level management review meetings such as Periodic Reviews with the vertical management and regular Project Management Reviews at the project. The minutes are recorded, maintained and tracked by the DPO & respective teams.

Review Inputs

The quality system review agenda comprises of the following items:

1- The status of actions from previous management reviews
2- Changes in external and internal issues that are relevant to the PIMS
3- Information on the PIMS performance, including trends in:
   a. Nonconformities and corrective actions
   b. Monitoring and measurement results
   c. Audit results
4- Opportunities for continual improvement
5- Feedback from users of the PIMS
6- Risks identified and escalated by organization employee
7- Records of procedural reviews
8- Results of technology upgrades and/or replacements
9- Formal requests for assessment by regulatory bodies
10- Complaints handling
11- Security breaches/security incidents that have occurred

Review Output

The deliberations of the review are collated and circulated to the concerned for initiating necessary actions. The action items are subsequently followed up and monitored by Management Representative. The management review output evaluates the decisions related to continual improvement opportunities and any need for changes to the PIMS, for example, identifying modifications to PIMS policy, procedures and/or technology that might affect compliance.

The action items from the Management Reviews at the Organization and practice / project level are followed up and monitored by the DPO/ POC from respective business units.

Policy

Vision of Vision Rx Lab Pvt. Ltd.

- Maximizing customer value through world class manufacturing practices, products and services
- Global Excellence

Mission of Vision Rx Lab Pvt. Ltd.

- Customer Satisfaction
- Continuous Innovation
- Good Human Resource Practices

Commitment to DIGITAL PERSONAL DATA PROTECTION ACT(DPDP)

VRX is committed to achieve DPDP compliance!

Trust and respect are key values within our organization and we welcome DPDP as an important step towards deepening our commitment to data privacy protection. Data privacy is key in a data-driven world and we see this as an opportunity to further improve the efficiency and transparency of our data handling and practices. We have embedded a DPDP mission statement into our general mission and vision statements, which are used to assess all our activities in the light of protecting data and championing privacy:

Faithful to its core values, Vision Rx Lab continuously strives to be an honest and discrete leader in data privacy protection, treating all personal data in our ecosystem in an ethical, respectful and pragmatic way

Our Privacy Notice (“Notice”) outlines how Personal Information of clients, prospective clients, former clients, visitors, vendors and other third parties we interact with ("External Individuals") is collected, managed and Processed by Vision Rx Lab Pvt. Ltd., Vision Rx Lab Pvt. Ltd is committed to handling the Personal Information of all External Individuals in an appropriate and lawful manner. This Notice sets out the minimum requirements for ensuring that the Personal Information of External Individuals is collected, used, retained and disclosed in a secure and compliant manner.

In some cases, local laws and regulations that apply to the Processing of Personal Information may be more restrictive than this Notice. Where this is the case, the more restrictive requirements will apply. Where required by local laws, Vision Rx Lab will provide you with additional privacy statements or information. In addition, this Notice may be supplemented from time to time with more specific privacy information or notices, for example when you visit https://vrxcompliance.azurewebsites.net

WHAT ARE WE GOING TO TELL YOU IN THIS NOTICE?

- What information do we collect?
- What is the purpose of Personal Data processing?
- What is our legal basis for processing your Personal Data?
- To whom we give your Personal Information
- Disclosure on (International) transfer of your Personal Information
- What steps are taken to safeguard Personal Data?
- What are your rights?
- How long we retain your Personal Information
- How we protect your Personal Information
- Who is the controller of your Personal Data?
- Contact Us
- Capitalized terms are defined at the end of this Notice, in the Definitions section

PIMS Objective

PIMS objectives are measurable / quantifiable and consistent with Vision Rx Lab business objectives. The measured PIMS objectives are analyzed against industry benchmarks, and this lays the foundation for continuous process improvement cycles, leading to better quality and ZERO tolerance to security incidents. Internal and external issues around Business & Quality Objectives are being monitored for enablement of effective planning. Function level objectives alignment with Business Objectives will be ensured by Corporate Functions as well.

Sl. No.	Business Objectives	PIMS Objectives	Process / Measures	Frequency
1	Vision Rx Lab Pvt. Ltd. has two Business Objectives that not only business or profit centric but also it has a social aspect. Primary Objective of Vision Rx Lab is preparing world class ophthalmic product for generals	To produce ophthalmic products, organization required to know the prescription details. Which can be identified as PII. Ensure proper mechanism to ensure security of PII	-ISMS Policy Management -Conduct Awareness Program for all employee about ISMS - Conduct internal audit for GAP analysis - Conduct ISO external audit and other audit procedure	Yearly Program/ Half Yearly/Quarterly
2	The Social Objective of the business, is to create value for stakeholders. That means its customers, vendors, suppliers, employees, communities as well as shareholders	To meet the business objective organization may need to gather information for specific reason. Organization ensure security for Business Information	-ISMS Policy Management -Conduct Awareness Program for all employee about ISMS - Conduct internal audit for GAP analysis - Conduct ISO external audit and other audit procedure	Yearly Program/ Half Yearly/Quarterly

Organizational roles, responsibilities and authorities

The details of the roles & responsibilities of associated with the functioning of the Organization are mentioned below.

Legal Team

To review Umbrella Contract/ Master Service Agreement/ Work Order level changes to comply with DPDP laws & provide approval before sharing the contract (new/modified) with client

DPO

can be part of Information Security Team

- Overseeing data protection strategy, associated procedures and implementation
- To ensure compliance (through regular audits) and to handle privacy and security related queries on regular basis
- Training org employees on DPDP compliance requirements
- Conducting regular data security related risk assessments (including Privacy Impact Assessment) and audits to ensure DPDP Compliance (Liaise with internal audit team)
- Serving as the point of contact between the company and relevant supervisory authority
- Maintaining records of all data processing activities conducted by the org
- Responding to data subjects to inform them about how their personal data is being used (through DPDP Privacy Notice) and what measures the company has put in place to protect their data

Internal Audit

- To maintain updated audit procedure with data privacy related audit and ensure regular audit to comply DPDP laws and regulations
- Reporting the latest status (any breaches, changes in procedure etc.) as part of MR meeting (liaise with DPO) and track the action / improvement items to closure

Planning

Actions to Address Risks and Opportunities

The PIMS is analyzed on internal and external organizational contexts and stakeholders needs and expectations to identify the failure modes that are potential deterrents of the objective of it to exceed the needs and expectations of the relevant stakeholders. Privacy impact assessment and project level self-assessment will be done on periodic basis (On every 6 months, twice in a year) to mitigate the risks associated with PII (Personally Identifiable Information) and data subject's rights. The action plans are monitored and improved on a periodic basis. DPO will be conducting regular data security related risk assessments (including Privacy Impact Assessment) and audits to ensure DPDP Compliance (Liaise with internal audit team)

The data protection risks associated with the privacy risk assessment

1- Relevant privacy laws, standards and frameworks
2- The impact on the rights and freedoms of data subject
3- Any physical, material or non-material damage to data subject
4- the impact on the organization (including, but not limited to reputation, regulatory action, financial loss, etc.)

Handling of Organization & PII related risks, opportunities and risks associated with those opportunities (if any) are detailed through organization's processes. Guideline on PII Risk management considering the following is also available at VRX Rx Lab document inventory.

1- Identify high-risk personal information and related processes that are high risk
2- Establish and maintain privacy risk criteria and identify the risk owners
3- Analyses the privacy risks that
   a. Assess the potential consequences that would result if the risks identified in the privacy risk assessment were to materialize
   b. Assess the realistic likelihood of the occurrence of the risks identified in the privacy risk assessment
   c. Determines the levels of risk
4- evaluate the privacy risks, including
   a. Comparison of the results of risk analysis with the risk criteria
   b. Prioritizing the analyzed risks for risk treatment

Organization shall ensure that the processing of personal information by such systems, products or services

1- Is minimized by default
2- Uses de-identified information where possible
3- Is transparent with regards to the functions and processing of personal information

Planning of Changes

PIMS is analyzed periodically to identify the existing and potential changes and formally implement the change through a controlled Change Management Process. This involves identification of drivers, capability assessment of the as-is status of the selected processes, setting the target for improvement followed by gap analysis, planning, coordinating, implementing, integrating and monitoring changes affecting any production and service within PIMS purview. On-going reviews of overall success of the initiative ensure the reinforcement of continual improvement. For further details on Change management process (VRXRL/ISMS/L3/22/V1.0) for PIMS is available in organization inventory

Support

Resource, Competence & Awareness

Resources requirements are determined and provided

1- To implement the PIMS and to maintain its effectiveness
2- To meet Data Subject's Right and DPDP requirements

Internal Auditor/ DPO will facilitate training and awareness for DPDP at the organizational, project and individual levels for necessary competency building. The Project Specific Training / Ad-hoc Training Requests are driven based on business needs and conducted by the DPO/ POC/ Internal Auditor from respective business units in terms of program design and delivery. Awareness on the following will be ensured by Internal Auditor / DPO at personal level

1- The PIMS Policy
2- Their contribution to the effectiveness of the PIMS, including the benefits of improved PIMS performance
3- The implications of not conforming with the PIMS requirements

DPDP compliance is the responsibility of each and every VRx associates

Codes of Conduct and Certifications

Use of approved codes of conduct and certification mechanisms to demonstrate that Vision Rx Lab complies to DPDP requirements. Signing up to a code of conduct or certification scheme is not obligatory. But if an approved code of conduct or certification scheme that covers Vision Rx Lab processing activity becomes available, it may wish to consider working towards a way of demonstrating that it complies

Adhering to codes of conduct and certification schemes brings many benefits over and above demonstrating that Vision Rx Lab complies. It can

1- ***Improve transparency and accountability*** - enabling individuals to distinguish that Vision Rx Lab meets the requirements of the law and they can trust it with their personal data
2- provide mitigation against enforcement action
3- Improve standards by establishing best practice

When contracting work to third parties, including processors, VRX may wish to consider whether it has signed up to codes of conduct or certification mechanisms. Codes of conduct should help VRX comply with the law, and may cover topics such as

1- Fair and transparent processing
2- The collection of personal data
3- The pseudonymization of personal data
4- The information provided to individuals and the exercise of individuals' rights
5- The information provided to and the protection of children (including mechanisms for obtaining parental consent)
6- Technical and organizational measures, including data protection by design and by default and security measures
7- Breach notification
8- Dispute resolution procedures

Data Inventory, Data Flow and Documentation

a- establishes and maintains a data inventory and data flow analysis that includes the identification of
   1- Key business processes that utilize personal information
   2- Sources of the personal information
   3- Categories of personal information processed, including the identification of high-risk personal information
   4- Purposes for which the personal information can be used, including subsequent secondary purposes over and above the initial purpose collected
   5- Potential recipients of personal information, including disclosure of personal information to third parties, data processors and transfer to vendors
   6- Within personal information data flows where an organization is acting as a data controller, a data processor or a joint data controller
   7- Key systems and repositories of personal information
   8- Within personal information flows where personal information is transferred over international boundaries or subject to differing laws, regulations, standards or frameworks
   9- Retention and disposal requirements for personal information, and the criteria for these requirements
b- Ensures that repeated data inventories produce consistent, valid and comparable results
c- Data retention will be in accordance with the data retention policy and retention schedule
d- When special categories of personal information are being processed, the organization shall identify, define and document the additional legal basis for the processing of personal information, which shall be selected from one or more of the following
   I- Natural person's explicit consent for specific purposes
   II- Necessary for employment rights or obligations

III- Necessary for protecting the vital interests of the data subject
IV- Necessary for legitimate activities of a foundation, association, or any other non-profit making body for a political, philosophical, religious or trade union aim, with appropriate safeguards
V- Information deliberately made public by the data subject
VI- Necessary for the establishment, exercise or defense of legal claims
VII- Necessary for reasons of substantial public interest
VIII- Necessary for preventive or occupational medicine, assessment of the working capacity of an employee, medical diagnosis, provision of health or social care systems and services
IX- Necessary for reasons of public health or professional secrecy
X- Additional provisions for processing of a kind introduced by national laws with regard to the processing of genetic, biometric or health data

e- The DPDP contains explicit provisions about documenting VRX's processing activities
I- Project teams will maintain records on several things such as processing purposes, data sharing and retention
II- Project teams are required to make the records available to the stakeholders on request
III- Documentation will help us to comply with other aspects of the DPDP and improve Vision Rx Lab's data governance
IV- Controllers and processors both will be having documentation obligations as per contract
V- Information audits or data-mapping exercises will feed into the documentation of VRX's processing activities
VI- Records will be kept in writing
VII- Records will be maintained electronically
VIII- Records will be kept up to date and reflect VRX's current processing activities
IX- Some basic templates will be produced to help document its processing activities

Communication

DPO / Internal Auditor will be the single POC for any internal and external communications. Any change in PIMS policy and related processes same will be communicated internally through appropriate channel. In case any data breach same will be communicated to relevant stakeholders. Data Protection Authority would be notified "without undue delay" and not later than 72 hours after becoming aware of the breach. Additionally, Vision Rx Lab will notify it's customer and data subjects affected by the breach "without undue delay". Vision Rx Lab will notify this within 72 hours of becoming aware of the breach, where feasible

1- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Vision Rx Lab will inform those individuals without undue delay
2- Vision Rx Lab will ensure that its robust breach detection, investigation and internal reporting through procedure L3- 29 Incident Management Procedure – L2- Incident Management Policy for data breach detection to facilitate decision-making about whether or not, it needs to notify the relevant supervisory authority and the affected individuals
3- Vision Rx Lab will also keep a record of any personal data breaches, regardless of whether it is required to

Notify Personal data breaches can include

1. Access by an unauthorized third party
2. Deliberate or accidental action (or inaction) by a controller or processor
3. Sending personal data to an incorrect recipient
4. Computing devices containing personal data being lost or stolen
5. Alteration of personal data without permission
6. Loss of availability of personal data

Operation

1- **Right of access**: Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Individuals will have the right to obtain:
   a. Confirmation that their data is being processed
   b. Access to their personal data
   c. Other supplementary information - this largely corresponds to the information that should be provided in a Privacy Notice

2- **Right to rectification**: If personal data is shared with advertisers, then customer can withdraw the consent to share any time.
   a. The DPDP gives individuals the right to have personal data rectified
   b. Personal data can be rectified if it is inaccurate or incomplete

3- **Right to restriction**: Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, Organization is permitted to store the personal data, but not further process it. Organization can retain just enough information about the individual to ensure that the restriction is respected in future. VRX will be required to restrict the processing of personal data in the following circumstances:
   a. Where an individual contest the accuracy of the personal data, VRX should restrict the processing until it has verified the accuracy of the personal data
   b. Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and VRX is considering whether its legitimate grounds override those of the individual
   c. When processing is unlawful and the individual opposes erasure and requests restriction instead
   d. If VRX no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

4- **Right to object**: Customer / Data Subject can object to stop automatic profiling. Individuals have the right to object to:

   a. processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
   b. direct marketing (including profiling) and
   c. processing for purposes of scientific / historical research and statistics

5- **Right to erasure ("right to be forgotten"):** Customer can ask to delete any specific personal data immediately, which is no more valid. The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

a. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:
b. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
c. When the individual withdraws consent
d. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
e. The personal data was unlawfully processed (i.e., otherwise in breach of the DPDP)
f. The personal data has to be erased in order to comply with a legal obligation
g. The personal data is processed in relation to the offer of information society services to a child

6- Right not to be subject to automated decision-making: The DPDP has provisions on:

a. automated individual decision-making (deciding solely by automated means without any human involvement); and
b. profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process

c. Automated individual decision-making is a decision made by automated means without any human involvement. Examples of this include:
    i. An online decision to award Credit Note/Loan
    ii. A recruitment aptitude test which uses pre-programmed algorithms and criteria
    iii. Automated individual decision-making does not have to involve profiling, although it often will do

Based on the traits of others who appear similar, organizations use profiling to:

I. Find something out about individuals' preferences
II. predict their behavior and/or
III. make decisions about them

The DPDP applies to all automated individual decision-making and profiling. DPDP has additional rules to protect individuals, if VRX is carrying out solely automated decision-making that has legal or similarly significant effects on them. VRX can only carry out this type of decision-making where the decision is:

I. Necessary for the entry into or performance of a contract or
II. Authorized by Union or Member state law applicable to the controller or
III. Based on the individual's explicit consent

VRX must ensure if any of its processing:

I. give individuals information about the processing
II. introduce simple ways for them to request human intervention or challenge a decision
III. carry out regular checks to make sure that VRX's systems are working as intended

7. Right to data portability: Right to move the personal from one Controller to another with no strings attached. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability only applies:

I. to personal data an individual has provided to a controller;
II. where the processing is based on the individual's consent or for the performance of a contract; and
III. when processing is carried out by automated means

8. Infringed Rights and Right to Complain: Both Controllers & Processors are under obligation to comply with DPDP. In case of a 'Data Breach', customers can contact the Data Protection Officer (DPO), for more information and immediate action.
   DPO/ Internal Auditor as the point of contact between the company and relevant supervisory authority will ensure the following
   I. Maintenance of records of all data processing activities conducted by the organization
   II. Responding to data subjects to inform them about how their personal data is being used (through DPDP Privacy Notice) and what measures the company has put in place to protect their data
   III. Ensuring that data subjects' requests to see copies of their personal data or to have their personal data erased are fulfilled or responded to, as necessary
9. Consent withdrawals: Data principal shall have the right to withdraw the consent at any time.
   VRX shall, unless retention is necessary for compliance with any law, erase personal data upon the data principal withdrawing his/her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier.
   Data processor processing on behalf of a data fiduciary must also delete such data on receiving the written instructions of the VRX

Internal Audit, Performance Evaluation and Continual Improvement

Data Security Audits will be scheduled at planned intervals, and when major changes take place on the basis of risk based categorization of the projects and importance of the activity to be audited, and will be carried out by the personnel independent of those having direct responsibility for the activity being audited. These audits shall verify conformance of organization's own requirements to PIMS and DPDP requirements.

The results of the audits will be recorded and brought to the attention of the auditee. Risks identified during the audit will be recorded for further tracking the actions to closure. The management personnel responsible for the area will take timely corrective and / or preventive action on the deficiencies / risks /improvement opportunities identified during the audit.

Follow-up audit activities will verify and record the implementation and effectiveness of the corrective action taken. The results of the internal quality audit form an integral part of the input to management review activities.

Internal quality audit findings are used as a basis for improving the suitability and effectiveness of processes. Analysis of audit findings to know the areas that need focus towards process improvement are carried out and reported to management in the form of quarterly Management Review report.

Data / record will be retained in accordance with the retention schedule.

Record and Response plan related to data breaches will be maintained and will be evaluated further to monitor repeat/unique incidents to ensure ZERO non-compliance/tolerance. Measures will be implemented that meet the principles of data protection by design and data protection by default. Measures would include:

I. Data minimization
II. Pseudonymisation
III. Transparency
IV. Allowing individuals to monitor processing
V. Creating and improving security features on an ongoing basis
VI. Use data protection impact assessments where appropriate

The continual improvement structure is supported by many elements which may include:

I. Privacy policy that includes commitments to meeting requirements and to continual improvement, that are periodically reviewed
II. The organization that has established PIMS objectives supporting the privacy policy and the commitment to meet requirements and thus continuously improve
III. Management review that focuses on the need for changes to the PIMS, policy and objectives. It also requires review outputs to include actions related to the improvement of the quality system, audits and resources

IV. The organization that identifies resources needed to maintain and continually improve the Processes
V. The organization that collects and analyses data to determine the effectiveness of the PIMS and takes decisions where improvements can be made.

Process improvements are affected at several layers and the inputs for doing this also come from different sources. Given below are the different layers where this may be typically done:

I. Organization Level
II. Project Level

Process improvement sources include:

I. Process / technology improvements that were piloted in some projects
II. Analysis of past data about project performance (on data security)
III. Analysis of breach data and the causes
IV. Senior Management Directives
V. External / Internal audit findings
VI. Non-Conformance analysis
VII. Customer/relevant stakeholder's feedback, which may include customer / data subjects' complaints, and advisory notices