Data Request Management Policy

This policy was last modified in April 2020. Please note that this privacy statement will be updated periodically to reflect any changes in the way we handle your personal data or any changes in applicable laws.

CORPORATE OFFICE:
Vakrangee Corporate House
Plot No. 93, Road No. 16, M.I.D.C., Marol, Andheri (East), Mumbai – 400093, Maharashtra

Table of Contents

1. Introduction 4
2. Data Privacy Policy & Security Policy 4
2.1 Policy commitment to respect human rights in data management 4
2.2 Personal data we Collect and Process 5
2.3 Rights of the Data Subject 6
3. Policy Statement 7
4. Timeframe for Responding to Subject Access Requests 8
5. Risk Assessments for Data Privacy 9
5.1 The Information Technology Act (2000) ("IT Act") of India include Section 43A and Section 72A 9
5.2 Penalty for Breach of Confidentiality and Privacy 10
5.3 Supreme Court of India has recognized the right to privacy as a fundamental right 10
5.4 Privacy is recognized by the United Nations as a fundamental human right 11
5.5 United Nations Declaration of Human Rights (UDHR) 1948, Article 12 12
5.6 International Covenant on Civil and Political Rights (ICCPR) 1966, Article 17: 13
5.7 Data Privacy Risk Assessment 16
6. Incident Investigation and Corrective Action 19
6.1 Incidence Reporting 19
6.2 Identification of Reasons of Incident 23
6.2 Root Cause Analysis for Incidents 24
6.3 Corrective action to prevent the incident recurring 24
7. Process for Responding Government Data Requests 25
8. Regular Reporting on Compliance with Any Government Data Requests 27
8.1 Notification of data subjects in case of data sharing under legal requirements 28
8.2 Disclosure of process for evaluating and responding to law enforcement or government data requests 28
8.3 Requests for information in emergencies 29
8.4 Disclosures without data subject Consent 30
9. Regular Human Rights Risk Assessments Linked to Data Privacy 30
9.1 ISO 27001 as a guiding principle of Information Security 33

9.2 Evaluate the key risks and controls 34
9.3 Risk Analysis 36
9.4 Benefits of the Risk Assessment 38
10. Remedy for Victim in Case of Human Right Violation Due to Company's Data Sharing Practices 39
11. Action Taken When We Receive A Subject Access Request 40
12. Types of Requests 42
12.1 Government requests for customer data 42
13. Managerial Responsibility for Government Data Requests Oversight 44
14. Sending A Request to Us 44
15. Fees 45

1. Introduction

This policy is regarding how we protect the personal data we process and control relating to you ("your personal data"; "your data") and the rights you have in relation to the processing of your personal data. This Data Request Management Policy outlines Vakrangee's policies and procedures for responding to any requests related to Customer Data

2. Data Privacy Policy & Security Policy

2.1 Policy commitment to respect human rights in data management

Data is enormously valuable and strong data protection is essential to maintain the right to privacy. We believe that data collection and data processing activities should be conducted in accordance with the human rights principle of 'doing no harm'. The respect and protection of personal identity is central to human dignity and human rights. Today, personal data privacy is an intrinsic human right and we respect fundamental human rights in data management. We believe that personal data could be processed without violating human rights.

Everyone has the right to protect their personal data. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law and guarantees that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

We have our Data Privacy Policy & Security Policy which says about gathering and holding of personal information on computers and on other devices as per proper rules and regulations. This policy covers what type of information we collect, how it

is used and when it may be disclosed. This Data Request Management Policy states that every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored, and for what purposes. If we capture any incorrect personal data or have collected or processed contrary to the provisions of the law of the land, every individual should have the right to request rectification or elimination.

2.2 Personal data we Collect and Process

We always make sure proper protection of the data (sensitive and personal data) we collect of our employees, potential employees, customers, suppliers, business contacts, shareholders, and website users. Processing of these data carried out on a legitimate basis and in a fair and transparent manner. We process personal data based on one or more of the following legitimate bases:

- With the consent of the data subject
- In the vital or best interests of the data subject
- To ensure the safety and security of persons of concern or other individuals

We use customer data only to provide the services we have agreed upon, and for purposes that are compatible with providing those services. We do not share customer data with any third-party advertiser or marketing services.

If the data we collect are not listed in privacy statement, we give individuals (when required by law) appropriate notice of which other data will be collected and how they will be used. Except for certain information that is required, decision to provide any personal data to Vakrangee is voluntary. There are no adverse consequences if individuals do not wish to provide us their personal data. If personal data is of another person (for instance, a potential employee/referral), individuals are responsible for

ensuring that such person is made aware of the information contained in this privacy statement and that the person has given his/her consent for sharing the information with us.

We use your personal data only where required for specific purposes based on your prior consent. To the extent you are asked to click on/check "I accept", "I agree" or similar buttons/ checkboxes/ functionalities in relation to a privacy statement, doing so will be considered as providing your consent to process your personal data. We will not use your personal data for purposes that are incompatible with the purposes of which you have been informed, unless it is required or authorized by law, or it is in your own vital interest (e.g. in case of a medical emergency) to do so.

2.3 Rights of the Data Subject

You are entitled to:

1. **Request access to the personal data we process about you:** this right entitles you to know whether we hold personal data about you and, if we do, to obtain information on and a copy of that personal data.

2. **Request a rectification of your personal data:** this right entitles you to have your personal data be corrected if it is inaccurate or incomplete.

3. **Object to the processing of your personal data:** this right entitles you to request that we no longer process your personal data.

4. **Request the erasure of your personal data:** this right entitles you to request the erasure of your personal data, including where such personal data would no longer be necessary to achieve the purposes.

5. **Request the restriction of the processing of your personal data:** this right entitles you to request that we only process your personal data in limited circumstances, including with your consent.

6. **Request portability of your personal data:** this right entitles you to receive a copy (in a structured, commonly used and machine-readable format) of personal data that you have provided to, or request us to transmit such personal data to another data controller.

To the extent that the processing of your personal data is based on your consent, you have the right to withdraw such consent at any time by contacting our Data Protection Officer.

If, despite our commitment and efforts to protect your personal data, you believe that your data privacy rights have been violated, we encourage and welcome individuals to come to us first to seek resolution of any complaint. You **Always Have the Right** to register a complaint directly with the relevant supervisory authority or to make a claim against us with a competent court where you deem that data privacy law has been infringed.
Contact us to exercise any of your rights.

3. Policy Statement

We protect your personal data in accordance with applicable laws and our data privacy policies. In addition, we maintain the appropriate technical and organizational measures to protect your personal data against unauthorized or unlawful processing and/or against accidental loss, alteration, disclosure, or access, or accidental or unlawful destruction of or damage thereto.

We receive requests from employees, customers, suppliers, business contacts, shareholders and website users who request required information from Vakrangee via e-mail, over the telephone, or via email or in a person.

Please Note:

1. All data requests must be made in writing via email, letter etc., clarifying the type of data requested.

2. All data requests must include the reason the data is needed, type of data needed, period data will be used, and how the data will be secured.

3. We retain the right to prioritize the fulfilment of data requests based on current priorities and the complexity of the request and to refuse any data requests.

4. We will not respond to correspondence sent by non-law enforcement officials to the address below.

5. Please be aware that we do not accept or process requests through other means (e.g., via social media, test messages or verbal messages).

4. Timeframe for Responding to Subject Access Requests

We have one month (30 calendar days) starting from when we received the information necessary to identify you, to identify the information you requested, and provide you with the information (or explain why we were unable to provide the

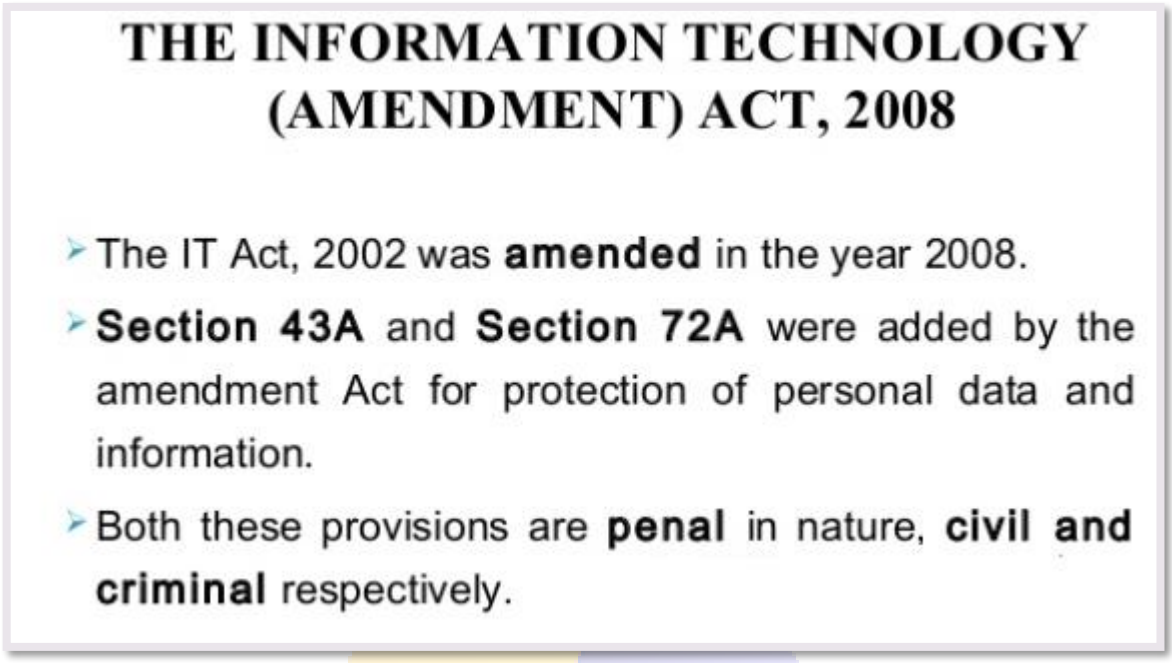
information). Wherever possible, we will aim to complete the request in advance of the deadline.

5. Risk Assessments for Data Privacy

Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built. Privacy is essential to who we are as human beings, and we make decisions about it every single day. It gives us a space to be ourselves without judgement, allows us to think freely without discrimination, and is an important element of giving us control over who knows what about us. Privacy is a qualified, fundamental human right. The right to privacy is articulated in all the major international and regional human rights instruments, including:

5.1 The Information Technology Act (2000) ("IT Act") of India include Section 43A and Section 72A

- The Information Technology Act (2000) ("IT Act") of India include Section 43A and Section 72A, which give a right to compensation for improper disclosure of personal information, which have some similarities with the GDPR and the Data Protection Directive Privacy Right of Privacy.



5.2 Penalty for Breach of Confidentiality and Privacy

Section 72 of the IT Act provides for penalty for breach of confidentiality and privacy. The Section provides that any person who, in pursuance of any of the powers conferred under the IT Act Rules or Regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such material to any other person, shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to INR 100,000, or with both.

5.3 Supreme Court of India has recognized the right to privacy as a fundamental right

- **The Supreme Court of India has recognized the right to privacy as a fundamental right under Article 21 of the Constitution as a part of the right to "life" and "personal liberty".**

5.4Privacy is recognized by the United Nations as a fundamental human right

- **Privacy is recognized by the United Nations as a fundamental human right in their Universal Declaration of Human Rights, Article 12.**

The right to privacy became an international human right before it was a nationally well-established fundamental right.

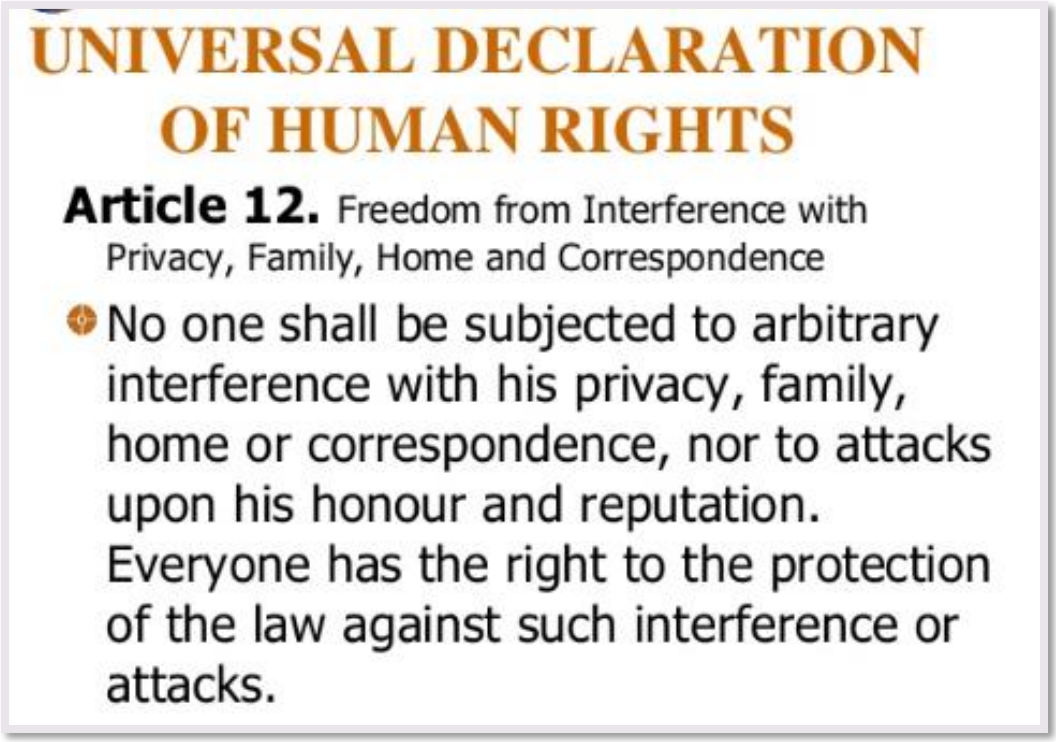
The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly

resolution 217 A) as a common standard of achievements for all peoples and all nations.

The extraordinary vision and resolve of the drafters produced a document that, for the first time, articulated the rights and freedoms to which every human being is equally and inalienably entitled. It sets out, for the first time, fundamental human rights to be universally protected and it has been translated into over 500 languages. The Declaration is the most translated document in the world — a testament to its global nature and reach. It has become a yardstick by which we measure right and wrong. It provides a foundation for a just and decent future for all and has given people everywhere a powerful tool in the fight against oppression, impunity and affronts to human dignity.

5.5 United Nations Declaration of Human Rights (UDHR) 1948, Article 12

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honors and reputation. Everyone has the right to the protection of the law against such interference or attacks", in this way the right to privacy or to respect of one's private life—came into existence.



5.6 International Covenant on Civil and Political Rights (ICCPR) 1966, Article 17:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor or reputation.
2. Everyone has the right to the protection of the law against such interference or attacks."

International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy.

The right to privacy is enshrined by the:

- Universal Declaration on Human Rights; Article 12
- International Covenant on Civil and Political Rights: Article 17
- Convention on the Rights of the Child: Article 16

- International Convention on the Protection of All Migrant Workers and Members of Their Families: Article 14

At the regional level, the right to privacy is protected by:

- European Convention for the Protection of Human Rights and Fundamental Freedoms: Article 8
- American Convention on Human Rights: Article 11

Other human rights instruments contain similar provisions. The right to privacy is included, for instance, in the following:

- Cairo Declaration on Human Rights in Islam: Article 18
- Arab Charter on Human Rights: Articles 16 and 21
- African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression in Africa
- African Charter on the Rights and Welfare of the Child: Article 19
- Human Rights Declaration of the Association of Southeast Asian Nations: Article 21
- Asia-Pacific Economic Cooperation Privacy Framework
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
- Additional Protocol to the Convention for the Protection of Individuals about Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows
- Council of Europe Recommendation No. R(99) 5 for the protection of privacy on the Internet
- European Union Data Protection Directive

The right to privacy is also included in:

✓ Article 14 of the United Nations Convention on Migrant Workers;

✓ Article 16 of the UN Convention on the Rights of the Child;

- ✓ Article 10 of the African Charter on the Rights and Welfare of the Child;
- ✓ Article 4 of the African Union Principles on Freedom of Expression (the right of access to information);
- ✓ Article 11 of the American Convention on Human Rights;
- ✓ Article 5 of the American Declaration of the Rights and Duties of Man,
- ✓ Articles 16 and 21 of the Arab Charter on Human Rights;
- ✓ Article 21 of the ASEAN Human Rights Declaration; and
- ✓ Article 8 of the European Convention on Human Rights.

130 countries have constitutional statements regarding the protection of privacy, in every region of the world.

The power of the Universal Declaration is the power of ideas to change the world. It inspires us to continue working to ensure that all people can gain freedom, equality and dignity. One vital aspect of this task is to empower people to demand what should be guaranteed: their human rights.

Vakrangee is committed to collecting and using data in a lawful, fair and legitimate way and will always respect the privacy of individuals in order to earn and deserve their trust.

An important element of the right to privacy is the right to protection of personal data. While the right to data protection can be inferred from the general right to privacy, some international and regional instruments also stipulate a more specific right to protection of personal data, including:

- the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,
- the Council of Europe Convention 108 for the Protection of Individuals about the Automatic Processing of Personal Data,
- several European Union Directives and its pending Regulation, and the European Union Charter of Fundamental Rights,
- the Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2004, and
- the Economic Community of West African States has a Supplementary Act on data protection from 2010.

Over 100 countries now have some form of privacy and data protection law. However, it is all too common that surveillance is implemented without regard to these protections. That's one of the reasons why Privacy International is around -- to make sure that the powerful institutions such as governments and corporations don't abuse laws and loopholes to invade your privacy.

5.7 Data Privacy Risk Assessment

Data protection has long relied on risk management as a critical tool for complying with data protection laws and ensuring that data are processed appropriately, and the fundamental rights and interests of individuals are protected effectively. Yet these risk management processes, whether undertaken by businesses or regulators, have often been informal, unstructured and failed to take advantage of many of the widely accepted principles and tools of risk management in other areas.

Data protection and privacy laws are meant to protect people, not data. Risk assessment models today play an increasing role in data protection. Risk assessment is fundamental as consideration of risk underlies organizational accountability and all data processing. We always ensure that data are processed appropriately, and the fundamental rights and interests of individuals are protected effectively. We conduct risk assessments for high-risk processing including data security, security breach notifications, privacy by design, legitimate interest, purpose limitation, the probability of possible threats, possible harms, personal data breach and fair processing. This helps us to classify processing activities according to the risks to individuals, prioritize compliance and devise appropriate mitigations. We have determined the level of risk for data processing activities in multiple scenarios and appropriately identified and classified as high risk, medium risk or low risk regarding the rights and freedoms of data subjects. We have appointed a Data Protection Officer as a data controller who records the purposes of all the data processed and implement measures to appropriately manage risks for the rights and freedoms of data subjects.

We have organizational, legal and technical measures envisaged to address and minimize the risks to an acceptable or tolerable level and to demonstrate compliance. We can identify and manage high risks that a system, product or service can generate and can also mitigate such high risks with safeguards, technical and organizational measures and controls before they materialize, for e.g., encryption of personal data.

Identify Impacts

1. We identify impacts — both harms and other negative impacts that effective data protection is intended to avoid or mitigate, and benefits and other positive impacts.

2. We identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

3. We identify damage to data subjects can be:

    a. physical (loss of amenity, disfigurement or economic loss related to physical integrity)
    b. material (loss incurred or lost revenue with respect to an individual's assets)
    c. moral (physical or emotional suffering, disfigurement or loss of amenity, etc.)
    d. privacy harms (Harms to individuals that result from problematic data actions, Loss of self-determination, Discrimination, Loss of trust, Economic loss)

Positive Impact

1. exercise of the right to freedom of expression or information, including in the media and the arts
2. unsolicited non-commercial messages, including for political campaigns or charitable fundraising
3. prevention of fraud, misuse of services or money laundering
4. employee monitoring for safety or management purposes
5. whistle-blowing schemes
6. physical security, IT and network security
7. processing for research purposes (including marketing research).

We share the risk analysis report to all stakeholders quarterly in given format:

Risk analysis report Format

Risk / Threat Event	Vulnerabilities /Characteristics	Mitigating Factors	Existing Security Control(s)	Likelihood (Low/ Medium/ High)	Impact (Low/ Medium/ High)	Risk Level (Low/ Medium/ High)	Recommended Safeguard / controls

* Likelihood / Impact / Risk = Very High, High, Moderate, Low, or Very Low

6. Incident Investigation and Corrective Action

An incident exposing personal data in an organization's possession or under its control to the risks of unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks needs to be investigated. Data breaches often lead to financial losses and a loss of consumer trust for the organization.

In case of occurrence of any incidence, the reporting of the same is done by our **Data Protection Officer to the CISO**. We understand the implications of such incidences and hence, have in all seriousness involved one of the Board Members in this complete process. Director – Research and Development is informed of the incident by the Chief Technology Officer. The role of Director – Research and Development is as follows:

- List down reasons which could have led to occurrence of the Incidence
- Carry out assessment of the incident occurred
- Highlight corrective action that needs to be taken
- Oversee implementation of corrective action

6.1 Incidence Reporting

An incident report can be used in the investigation and analysis of an event. It includes the root cause and corrective actions to eliminate the risks involved and prevent similar future occurrences. Incident reports can also be used as safety documents which indicate potential risks and uncontrolled hazards found in the workplace.

An incident report can be used by:

- an authority to create a report of an incident
- an employee to report an incident he/ she has witnessed
- a member of the organization to raise awareness about an incident that has occurred in the workplace.

VAKRANGEE DATA BREACH INCIDENT FORM

Data Breach Incident From

DPO/COMPLIANCE OFFICER/INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
DDI:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			

INCIDENT IMPACT ANALYSIS

S/N	Imapct On	Severity	Impact
1	Regulatory & Statuatary		
2	Human right impact		
3	Social Impact		
4	Business reputation		
5	Financial impact		
6	Technical impact		

Breach Notification

BREACH NOTIFICATIONS:		
WAS THE SUPERVISORY AUTHORITY NOTIFIED?	**YES/NO**	
IF YES, WAS THIS WITHIN 72 HOURS?	**YES/NO/NA**	
If no to the above, provide reason(s) for delay		
IF APPLICABLE, WAS THE BELOW INFORMATION PROVIDED?	**YES**	**NO**
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?	**YES/NO**	
INVESTIGATION INFORMATION & OUTCOME ACTIONS:		
DETAILS OF INCIDENT INVESTIGATION:		
PROCEDURE/S REVISED DUE TO BREACH:		
STAFF TRAINING PROVIDED: *(if applicable)*		

Investigation Report

DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:	
HAVE THE MITIGATING ACTIONS PRVENTED THE BREACH FROM OCCURRING AGAIN? *(Describe)*	
WERE APPROPRIATE TECHNICAL PROTECTION MEASURES IN PLACE?	**YES/NO**
If yes to the above, describe measures	
Investigator Signature: _____ Date: _____	
Investigator Name: _____ Authorised by: _____	

The CISO (Director - R&D) also presents all the incident and corrective action quarterly in the Board meeting to the Board of Directors in below format:

Incident report to the board of directors

Incident Report for the period of <month - Year> To <month - Year>	
Total No of Incident reported	
No of High Severity incidents	
No of Medium Severity incidents	
No of Low Severity incidents	
Total Closed with action	

Total Closed with No action	
Total Incident in Review	
Recommended Corrective Action	

Currently, till 2019 - 20, no government data requests have been received by our organization.

6.2 Identification of Reasons of Incident

If data is requested from third party or government body or regulatory, we check the purpose of requested data and ask to established identity from requested party. We do not disclose any of the information unless and until we receive formal and valid legal process.

Below are the reasons where incident can take place while sharing or disclosing the data to third party/Vendor/Government body/ Legal Firm/Regulatory body while they are requesting for user/customer information and data:

- ✓ Without knowing the purpose or doing proper assessments of request sharing the data.
- ✓ Wrong interpretation of receiver before providing the data requested for.
- ✓ Disclosing data without any legal process or against company policy.
- ✓ Allowing third parties to access company data without agreement or without signing NDA, etc.
- ✓ Data shared by a person not having proper training for sensitive or privileged data request.
- ✓ No proper communication or training for Data request in place.
- ✓ Not rejecting the request which shows inappropriate and/or over-broad, not clear, or not have valid legal basis.

6.2 Root Cause Analysis of Incidents

We carry out a thorough investigation in case of any incident regarding data breach takes place. Once the investigation is closed and the incident is fully documented in an incident report, there is a root cause analysis is carried out to find out why the incident occurred and how to prevent it from occurring again.

A root cause analysis isolates the main reason the incident occurred. These reasons can be as follows:

- Policies or procedures not developed or not followed
- Inadequate or missing training
- Employee behaviour
- Poor communication

The assessment is then concluded with the following findings on:

- Why the incident occurred
- How future occurrences can be prevented
- Corrective action plan and timeline

6.3 Corrective action to prevent the incident recurring

Once the complete investigation has been done and findings have been obtained, we focus on corrective actions to be taken. These corrective actions are identified keeping in mind that such incidents should not occur again in future.

- Having a centralized and standardized process for receiving, tracking, processing, and responding to legal requests from law enforcement,

government, and third parties from when a request is received until when a response is provided.

- Not allowing "back door" request for direct access of data by the government.
- Thorough review of the effectiveness of the data request process, with recommendations and a timeline to address any weaknesses.
- Modify policy or process, if any changes are required.

7. Process for Responding Government Data Requests

When we receive requests for user data or user information about how a person has used the company's services from Government agencies, courts, and parties in civil litigation, we understand the importance of the same. In accordance with applicable law and our terms of service, our team reviews each request to make sure that it satisfies legal requirements and company's policies. For us to produce any data, the request must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law. If we believe a request is overly broad, we'll seek to narrow it.

We are committed to maintaining trust with both our users and customers by being transparent about how we respond to such requests. For us the customer is primarily responsible for responding to law enforcement requests relating to the customer's data. However, if we receive a government data request regarding a customer account, each request is reviewed using these guidelines:

1. **Respect for the privacy and security of data store with us.**

   When we receive a request, our Data Privacy team reviews it to make sure it satisfies legal requirements. We make sure request should be in writing, signed by an authorized official of the requesting agency and issued under an

appropriate law. If we believe a request is overly broad, we'll seek to narrow it.

2. **Objective and end use of data requested**

   When we receive a request, we carefully examine the objective and end use of data requested by government agencies. Requester must mention objective of end use of requested data explicitly and clearly in the request. We ensure that data requested should be relevant to the said objective and use.

3. **Undertaking for objective and intended use of requested data by the requesting agency**

- The data requests must provide undertaking for objective and intended use of requested data along with Data Request Form with a formal requesting letter on the letter head of the institution/office/ organisation to ensure the identity of the user.
- The data supplied to a requester is only meant for the purpose mentioned in their request letter and in no case the data be parted and handed over to any other user or agency for any other purpose.
- Sender reserves the right to accept or decline any data request on public interest.

4. **Customer notification.**

   Except in emergency situations involving a threat to life, it is our policy to notify the customer before any information is disclosed unless such notification is prohibited by law.

5. **Consideration of customer objections.**

   We notify customer on government access request. If the customer files an objection to disclosure with the court and provides a copy of the objection to

us, receiving such legal process (e.g., a court order) from a police department or court, we will not provide the data in response to the request if the objection is resolved in favor of the customer. But if the request seeks valid, we may disclose some identifying information to the requesting party.

6. **Disclosures without data subject Consent**

We may share personal information with government authorities/ law enforcement agencies in response to warrants, or court orders, in connection with any legal or regulatory process, or to comply with relevant laws. We may also share your personal information in order to establish or exercise our rights, to defend against a legal claim, to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, safety of person or property, for audit purposes, or a violation of our policies.

8. Regular Reporting on Compliance with Any Government Data Requests

Sharing the number and type of requests received by a company is an important part of building trust with users and customers. However, reporting on what happens after those requests are processed internally is equally important. Outcome and compliance data add context and can demonstrate the company's commitment to protecting users by narrowing requests or by carefully reviewing requests.

When Government agency ask us to disclose user information, we carefully review each request to make sure it satisfies the laws, rules, and regulations. If a request asks for too much information, we try to narrow it, and in some cases, we object to producing any information at all. We share the number and types of requests we receive in our Transparency Report.

As a commitment towards information security and data privacy, one representative from the Board of Directors is part of Governance of Information Security and Data Privacy Organization Structure and holds a key position of Director – Research and Development.

This transparency report is prepared by the Data Protection Officer & Information Security Officer and presented to the CISO (Director – R&D). This transparency report is presented to the Board of Directors by CISO (Director – R&D) on a quarterly basis in the Board meeting in given format:

Total Requests Received	Total Requests Accounts	Total Requests Percentage

Same data is also available on our website. Currently, till 2019 - 20, no government data requests have been received by our organization.

8.1 Notification of data subjects in case of data sharing under legal requirements

When we receive a request from a government agency, we send an email to the user account before disclosing information. We notify the customer that his/her data has been requested (so that the customer may attempt to limit or prevent disclosure) unless applicable law prohibits notification. Where appropriate and in order to protect our customer's legitimate interests, through appropriate legal process or other means, we challenge requests that prohibit notification to the customer. If the account is managed by an organization, we give notice to the account administrator.

8.2 Disclosure of process for evaluating and responding to law enforcement or government data requests

- We only provide such data if the government agency has appropriate authority under applicable law to require us to provide such data. For example, without a valid warrant or court order, we do not provide any customer data to the government
- If appropriate, we seek to narrow (including moving to formally modify by judicial mandate) any government agency request or demand for customer data to only the specific information required to respond.
- We make an exception to these commitments in emergency cases where we believe disclosing customer data will prevent imminent death or serious physical harm to an individual. We will notify the customer promptly if such an exception is made and will include that disclosure in our transparency report.
- We will not give notice when legally prohibited under the terms of the request. We provide notice after a legal prohibition is lifted, such as when a statutory or court-ordered gag period has expired.
- We might not give notice if the account has been disabled or hijacked. We might not give notice in the case of emergencies, such as threat to someone's life, in which case we will provide notice if we learn that the emergency has passed.

8.3 Requests for information in emergencies

If we reasonably believe that we can prevent someone from dying or from suffering serious physical harm, we may provide information to a government agency — for example, in the case of bomb threats, school shootings, kidnappings, suicide prevention, and missing persons cases. We still consider these requests considering applicable laws and our policies.

- We are committed to report data regarding requests or demands for customer data that we receive from Police station, government, regulatory bodies, law enforcement and national security agencies.

8.4 Disclosures without data subject Consent

We share personal information with government authorities/ law enforcement agencies in response to warrants, or court orders, in connection with any legal or regulatory process, or to comply with relevant laws. We share your personal information in order to establish or exercise our rights, to defend against a legal claim, to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, safety of person or property, for audit purposes, or a violation of our policies.

9. Regular Human Rights Risk Assessments Linked to Data Privacy

Risk assessments have always been part of our practice as it is very important to ensure that no Human Rights violation takes place linked to Data Privacy. Hence, the involvement of all the stake holders for risk assessment (e.g. executive board, board of directors, top management, HOD's, other management team) is essential.

The Board has appointed a sub-committee in the aspect of conducting Human Rights Risk Assessment linked to Data Privacy. This sub-committee is known as 'Risk Management Committee' and it comprises of the following members –

Sr. No.	Name of Members	Designation	Board Designation
1	Mr. S N Kaushik	Chairman	Non Executive Independent Director
2	Ms. Divya Nandwana	Member	Executive Chairperson
3	Ms. Savita Keni	Member	Non Executive Independent Director
4	Mrs. Sujata Chattopadhyay	Member	Non-Executive Independent Director

The responsibilities of the Risk Management Committee for Human Rights Risk Assessment linked to Data Privacy include the following –

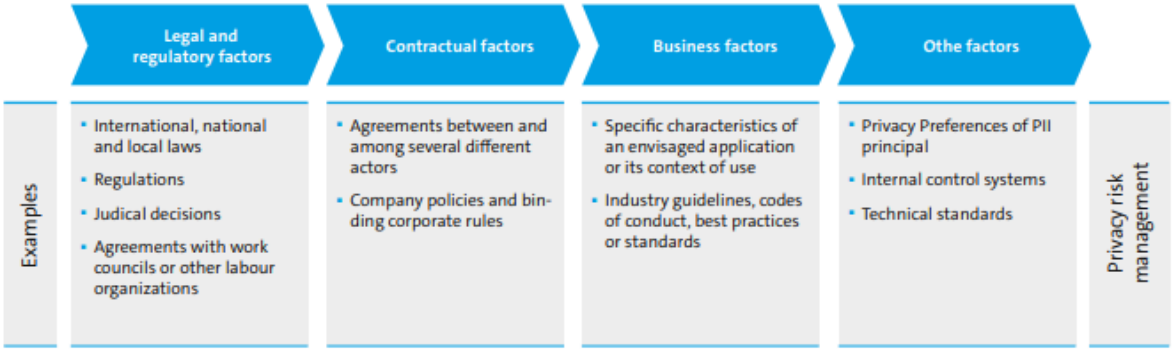
- To evaluate actual and potential Human Rights risk related to Data Privacy
- To verify the Human Rights Risk Assessment framework related to Data Privacy
- To monitor implementation of Human Rights Risk Assessment framework related to Data Privacy
- To report Human Rights Risk Assessment to the Board of Directors related to Data Privacy

The reporting of Human Rights Risk Assessment is carried out by the DPO and Information Security Officer on regular intervals and report to the **Risk Management Committee**. The Risk Management Committee then reports to the Board of Directors in the Board meetings held quarterly.

We conduct the following steps as a part of our regular Human Rights risk assessment process to ensure that our policy is meeting risk mitigation in the following area of Human Rights:

S/N	Category	Information
1	Information Privacy	which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records
2	Bodily privacy	which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches
3	Privacy of communications	which covers the security and privacy of mail, telephones, email, and other forms of communication
4	Territorial privacy	which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space
5	Racism	use of algorithms to arbitrarily discriminate, including against marginalized communities and communities of color

- ✓ We periodically review all the policies in line with the national and international laws related to Data Privacy
- ✓ We assess the actual and potential risks based on changes and updates in national and international laws, especially related to Information Security law, Data Protection law, Data Privacy law and laws related to human rights. Based on this assessment, we realign and updates our policy on regular basis.
- ✓ We define the Internal and External Context for example requirements from international or national law, Judicial decisions, Regulations, Contractual agreements, Business factors (for example codes of conduct, industry standards), Internal control systems



- ✓ We have Information Security internal and external audits - monthly, quarterly, half yearly and yearly in place including to assess Human Rights risk related to Data Privacy. All kind of risk assessment is also an integral part of these audits.
- ✓ The results of the internal audits are regularly reported to the management and the Risk Management Committee of the Board.
- ✓ Based on the risk assessment outcome, we identify business leverages and responsibilities, decision-making and actions needed, which is updated on regular basis and recorded
- ✓ We have monitoring, review, reporting and continuous improvement plan which is updated on a regular basis and recorded
- ✓ We provide training and capacity building on worker-management communication and negotiation
- ✓ We establish / revise grievance and remediation systems

9.1 ISO 27001 as a guiding principle of Information Security

Our risk assessment is based on the likelihood of occurrence and the severity of the risk. Measures, which are implemented in Vakrangee, include assessment of risk related aspects in accordance with an information security management system ("ISMS"). ISMS is a procedure for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. Proof of compliance with the requirement of an appropriate level of protection is provided by means of various documentation which is usually accompanied in an ISMS.

SHAMKRIS®

SHAMKRIS CERTIFICATION

Vakrangee Limited

"Vakrangee Corporate House", Plot No. 93, Road No. 16, M.I.D.C. Marol, Andheri (East), Mumbai – 400 093

SHAMKRIS GLOBAL certifies that the Management System of the above organization has been audited and found to be in accordance with the requirements of the management system standard detailed below

Standard

ISO/IEC 27001:2022

Scope of Certificate

Delivering Banking, ATM, e-Governance, e-Commerce, Insurance and other strategic alliances and partner's services/products, by creating franchisee network and monitoring the performance, impact of our outreach and roll-out initiatives by insuring front-end service delivery points within the reach of each and every citizen with prompt, accurate, secure and reliable integrated services/products to end customers through online devices with strong management and field team till the block level end by being the last-mile link connecting India's rural and urban citizens with the modern ecosystem.

SHAMKRIS®

Certificate No : GIS1153
Date of Initial Registration : 02/04/2009
Date of Last Issue : 29/05/2024
Date of Expiry : 01/04/2027
Surveillance Audit 1st year : 01/03/2025
Surveillance Audit 2nd year : 01/03/2026

GAAS
CAB-05

This certificate is valid ONLY if the annual surveillance completed & updated on website

Signed on the behalf of Shamkris Global Inspection Services Pvt. Ltd.

This certificate remains the property of ***SGISPL*** *This certificate and all copies of reproductions off the certificate shall be returned or destroyed if requested by* **Shamkris Global Inspection Services Pvt. Ltd.**

To verify the validity of this certificate, kindly visit our website: **www.shamkris.com**
B-01, Western Edge II, Off Western Express Highway, Borivali (East), Mumbai – 400066, Republic of India

9.2 Evaluate the key risks and controls

Center point of our all policies and process related to Personal Data Privacy is people. We evaluate the key risks and controls in order to prioritize human rights of an individual. We evaluate the risks in terms of probability (or likelihood of occurrence) as well as severity (i.e. a measure of the financial and reputational consequences associated with each risk) impacting human rights of an individual.

Risk Severity Rating:
1. **Very Low:** Immaterial impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
2. **Low:** Low impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
3. **Medium:** Moderate impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
4. **High:** Significant impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
5. **Very High:** Very significant impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives

Risk Severity Rating:
1. **Very Low:** Immaterial impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
2. **Low:** Low impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
3. **Medium:** Moderate impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
4. **High:** Significant impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives
5. **Very High:** Very significant impact on the company's reputation and/or annual earnings, or on its ability to achieve business objectives

We evaluate controls to establish whether things need to be fixed or new controls should be built in:

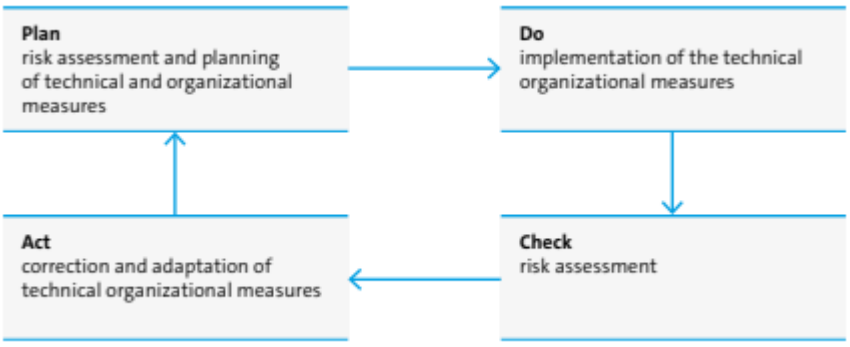
Control Effectiveness Rating:
1.**Highly effective** – Risk exposures are within established tolerance levels; controls are tested and functioning effectively; linkage between risk and return is explicitly established (performance based); comprehensive metrics and dashboard reporting in place
2.**Effective** – Risk exposures are within established tolerance levels; controls are tested and functioning effectively; linkage between risk and return is implicitly established (judgment based); some metrics and dashboard reporting in place but development plans are established
3.**Moderately effective** – Risk exposures are generally within established tolerance levels with few exceptions; controls are functioning at an acceptable level but not fully tested; some metrics and dashboard reporting in place
4.**Needs improvement** – Some or material exceptions to established tolerance levels; controls are established but not fully tested; minimum metrics or dashboard reporting in place
5.**Needs significant improvement** – Significant exceptions to established tolerance levels (or tolerance levels are not established); controls are not in place or functioning effectively; minimum or no metrics or dashboard reporting

- Overview of the assets (personal data / information and everything needed for its processing or which is required for it)
- determine technology for risk assessment
- risk management process
- risk identification, risk analysis and risk evaluation
- action plan
- risk management plan
- internal audit program and audit reports (including corrective measures)
- management report or report to the company management
- further documentation such as minutes from committee meetings, effectiveness tests, internal guidelines and specifications, training certificates etc.

We carry out appropriate processes on a regular basis:

1. The PDCA cycle is used as the motor of the management system.

2. The phases of risk assessment, the preparation and implementation of a risk management plan, internal audits, management assessment and taking corrective actions are stipulated.

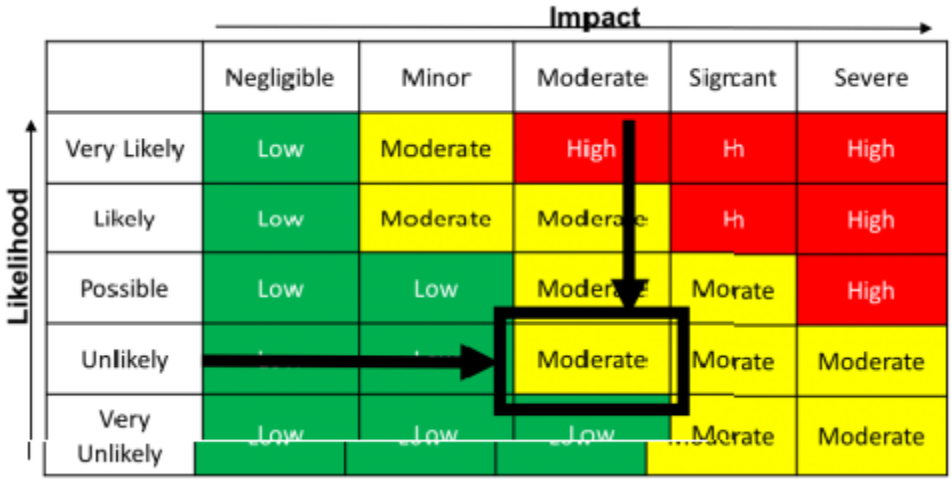


9.3 Risk Analysis

Risk levels are calculated as the product of the LIKELIHOOD and IMPACT (of a potential threat event / threat event category.

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

For example, a threat event where the likelihood is "unlikely" and the impact is "moderate" equals an assessed risk of "Moderate":



Systems that process data protected are considered high-risk systems. This is because the likelihood of compromise is (at a minimum) possible, while the impact (due to regulatory or industry standard violation) is considered a severe loss of confidentiality. The risk level for each threat event category is then calculated. The overall risk level for the system is equal to the HIGHEST risk level for any risk event. For example:

Because one of the risk events was rated as "High Risk", the overall risk level is High.

Threat Event	Likelihood	Impact	Risk Level
1. Loss of Confidentiality	Possible	Severe	HIGH
2. Loss of Integrity	Unlikely	Minor	LOW
3. Loss of Availability	Possible	Significant	MODERATE
		OVERALL RISK:	HIGH

We have a risk management policy that defines:

- who is responsible for carrying out a risk assessment,
- who provides information and evaluates the data protection risks,
- how is the controller for data protection risks determined,
- how often is the business procedure carried out,
- what is the methodology/technique for risk assessment
- which applicable risk treatment options are available,
- what happens with the analysis results of the security of processing?

We encourage our employees to do their part to promote a culture of privacy and we have built a responsible, innovative, and effective information security and data privacy culture. To get this we:

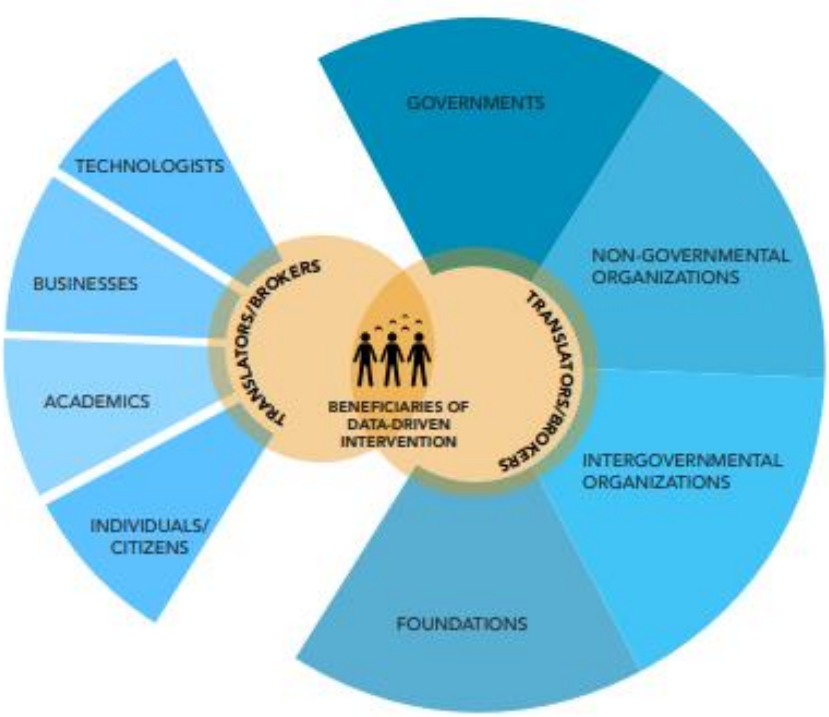
- ✓ Kept pace with technology and the proliferation of data
- ✓ Define clear owners
- ✓ Create Data Privacy Policy
- ✓ Implement Data Privacy controls
- ✓ Initiate Data Privacy training and awareness
- ✓ Create periodic campaigns and workshops
- ✓ Provide privacy awareness to new joined in their inductions program

9.4 Benefits of the Risk Assessment

- Enhanced awareness and transparency of the key risks facing the human rights.
- Facilitated cross-functional learning and knowledge transfer for the stakeholders.
- Improved risk analytics and quantification processes (by targeting these efforts on the most critical risks).
- Enhanced Board and senior management reporting.
- Improved business performance through risk-based decision making.
- Converting qualitative opinions into a quantitative evaluation

In this way we have built customer trust and strive for better business outcomes by mitigating the risk of violation of fundamental rights of privacy of an individual. We give clarity to our customer when we communicate with them.

10. Remedy for victims in case of Human Right Violation due to company's data Sharing Practices



This is an Ideal model for incorporating all stakeholders to coordinate around data-driven interventions. Data request Management policy serves to connect both internal and external stakeholder groups to develop a common understanding of technological approaches and responsible actions. People-centered human security and rights frameworks place beneficiaries at the ultimate focal point of any data-driven intervention.

In case of any infringement of the provision by any party the liability will be attached to the erring party and dealt as par the said law.

In the event where the fault lies with Data Supplier, he/she will be held responsible. Once the data has been supplied to recipient, post which, is wrongly utilized or misused, then the

recipient will be held liable for the damages that take place. In such a case, the receipt individual cannot claim the remedy since he/she is at fault.

Remedy for victim is available by way of approaching to National Commission Human Rights or State Commission Human Rights as the case may be. The final appeal lies with the Supreme Court of India.

In case of violation or negligence of human rights, the victim or any person on his behalf can reach to:

- ✓ Local or State or National Commission Human Rights
- ✓ Human Rights Courts for the purpose of providing speedy trial of offences arising out of violation of human rights,
- ✓ The Supreme Court or the High Court concerned for such directions, orders or writs as that Court may deem necessary

National or State Commissioner also has:

- ✓ Authority to grant interim relief
- ✓ Authority to recommend payment of compensation or damages

CISO presents Human Rights violation data quarterly to Board of Directors in Board meeting. Currently, till 2019 - 20, no government data requests have been received by our organization.

11. Action Taken When We Receive A Subject Access Request

We first verify the identity of the person requesting access if we doubt your identity, we will ask for information to verify it. For example, we may ask you for a piece of information held in your records that you might reasonably be expected to know. We cannot disclose personal information to anyone other than the individual in question.

We then validate the answer provided by the third party with the information saved with us which identifies a third party.

Before sharing information that relates to third parties, we, where possible, anonymize or edit information that might affect individual privacy. We may also summarize information rather than provide a copy of the whole document. As per rule we require to provide information, not documents.

12. Types of Requests

12.1 Government requests for customer data

1. **Data Requests.**

   A data request is a request for information or documents relating to Subscriber accounts in connection with official criminal investigations or other official legal proceedings. Except in limited emergency situations (see below), we require data requests to be made through formal legal process and procedures, and we respond to such requests as required by law.

   Examples of data requests include:

   a. Court Orders
   b. Search Warrants
   c. Summons
   d. FIR requests
   e. Judicial decision
   f. Legal process received from outside India may require a Mutual Legal Assistance Treaty with India
   g. Other forms of legal process such as Civil Investigative Demands

2. **Preservation Requests.**

   A preservation request asks us to preserve Subscriber account records in connection with official criminal investigations or other official legal proceedings. Preservation requests must include the following information:

   a. Identification of the account(s) at issue

b. Identification of the investigating agency and/or specific pending official proceedings (requests must be signed on law enforcement letterhead)

c. Assurances that the requesting agency or individual is taking steps to obtain appropriate legal process for access to the data that Vakrangee is being asked to retain and

d. A valid return email address and phone number.

3. **Emergency Requests.**

   An emergency request is only appropriate in case a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay. We respond to emergency requests when we believe in good faith that such harm may occur if we do not respond without delay.

4. **Notice to our Subscribers.** Our policy is to notify our Subscribers of requests for their data unless we are prohibited from doing so by statute or court order.

5. **Information to Include in a Request.**

   The following information must be included in a request for Subscriber data:

   a. First and last name of the customer and email address associated with the subject and
   b. Details of the information required with the objective

We may not be able to respond to a request without this information. Additionally, we reserve the right to request a copy of the complaint and any supporting documentation that demonstrates how the information requested is related to the pending litigation.

13. Managerial Responsibility for Government Data Requests Oversight

In case of providing information to public or governmental authorities requests, we require an official, signed document issued pursuant to local law and rules.

Managerial responsibility to oversee the government data requests lies with the Data Protection Officer. The Data Protection officer along with his/her team and senior management, reviews government demand for customer data to ensure the requests are valid. The Data Protection Officer rejects those that are not valid, and only provides the data specified in the legal order.

We provide information if the Data Protection Officer determines that for purposes of national security, lawful basis, law enforcement, or other issues of public importance, the required disclosure is necessary or appropriate. We first and foremost determine that disclosure is reasonably necessary to enforce our terms and conditions or protect our operations or users.

14. Sending A Request to Us

Requests should be sent to or mailed or faxed to:

Vakrangee Limited

"Vakrangee Corporate House"

Plot No. 93, Road No. 16,

M.I.D.C., Marol, Andheri (East),

Mumbai – 400093, Maharashtra

Phone: +91 22 6776 5100

E-mail: infosec@vakrangee.in

Important Note:

In the event you send us a notice of any kind via email and do not receive a response from us, please submit a duplicate copy via paper and/or fax (fax # 28502017). Due to the vagaries of the internet and email communication in particular, including without limitation the burdens of spam and the occasional unintended effects of spam filters, sending an alternate form of notice, will help assure that your notice is received by us and acted on in a timely manner.

15. Fees

We may seek reimbursement for costs in responding to requests as provided by law and may charge additional fees for costs in responding to unusual or burdensome requests. It means if your data subject access requests are excessive or manifestly unfounded, we will charge to cover the administrative costs involved in dealing with your request. In extreme circumstances, we reserve the right to refuse your requests with reasonable reason.

Thank You

CORPORATE OFFICE:
Vakrangee Corporate House
Plot No. 93, Road No. 16, M.I.D.C., Marol, Andheri (East), Mumbai – 400093, Maharashtra