Vakrangee
सशक्त परिवर्तन

DATA PRIVACY POLICY

Contents

1. Introduction

The right to privacy is a fundamental right and is necessary to protect personal data as an essential facet of informational privacy. The growth of the digital economy has meant the use of data as a critical means of communication between people. Hence, it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation.

Our Information Security Philosophy is to ensure that the right data is used by a person in the right role and only in the right context, so that internal and external customers and other stakeholders can trust us for their business. Our Data Privacy Policy is a legal document that we use to disclose the way we gather, use and manage the personal information of our customers and clients. Personal information can be anything that identifies an individual. Our Data Privacy Policy not only covers our customers but also covers our business partners, franchisee partners, and suppliers

We follow strict security procedures in the storage and disclosure of any information so that our internal and external clients, employees, Board members, other partner in our organization (voluntary or otherwise), contractor or agent feel confident about the privacy and security of their personal information.

We handle data protection and privacy by categorizing all data based on our sensitivity (confidentiality), criticality (availability), identifiability (privacy) and compliancy; this categorization is then used to determine the safeguards required. We controlthe framework which is primarily based upon ISO 27001:2013 which states:

Information Security	The protection of the confidentiality, integrity and availability of information.
Information Privacy	Establishing rules which govern the collection and handling of personal information.
Information Compliance	Adherence with all applicable IT regulatory requirements or implementing compensating controls or documenting exception requests.

2. Definitions:

Personal Data:

Any information that directly or indirectly identifies an individual.

Data Controller

A person, department or organization that determines the purposes and means of data processing.

Data subject

An individual whose personal data is subject to processing.

Processing

Any operation or set of operations applied to Personal Data, such as data collection, recording, organization, structuring, storage, adaptation, modification, extraction, consultation, use and transmission.

3. Our Provision

We have made the below provision:

- To protect the autonomy of individuals in relation with their personal data,
- To specify where the flow and usage of personal data is appropriate,
- To create a relationship of trust between people and entities processing their personal data
- To specify the rights of individuals whose personal data are processed
- To create a framework for implementing organizational and technical measures in processing personal data
- To lay down norms for sharing of personal data
- To ensure the accountability of entities processing personal data
- To provide remedies for unauthorized and harmful processing
- To establish a Data Protection Authority for overseeing processing activities
- To protech privacy throughout processing from the point of collection to deletion of personal data
- To carry out processing of personal data in a transparent manner

4. Our Basic principles of personal data processing

Our personnel need to respect and apply the following basic principles when processing personal data:

- Legitimate and fair processing
- Purpose specification
- Based on Customer/User consent
- Data Quality
- Necessity and proportionality
- Accuracy
- Collection limitation
- Right to Information Respect the rights of the data subject or user
- Confidentiality, Security and Availability (CIA)
- Prevention, detection, investigation and prosecution of contraventions of law
- In compliance with law or any order of any court or tribunal Necessary for prompt action

- For reasonable purposes
- Based on explicit consent
- Sensitive personal data of children
- By Implementing Partners

4.1 Legitimate and fair processing

Our policy of processing of personal data shall only be carried out on a legitimate basis and in a fair and transparent manner. We process personal data based on the consent and in the best interests to ensure your safety and security.

4.2 Purpose specification

- Personal data shall be processed only for purposes that are clear, specific and lawful.
- Personal data shall be processed only for purposes specified.

4.3 Based on Customer/User consent

By submitting or providing to us your personal information, you consent to the use of that information as set out in this Privacy Policy. We process personal data based on your consent, given no later than at the commencement of the processing. We process personal data only when there is a legal basis for doing so or you have granted us your consent in this regard.

If you apply online for a franchise or work placement you may need to provide in the course of your application information about your education, mobile no, right to work etc. Your application shall constitute your express consent to our use of this information to assess your application and to allow us to carry out any monitoring activities, which may be required as per the applicable law of an employer and organization.

4.4 Data Quality

Our data protection team ensure that personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed.

4.5 Necessity and Proportionality

The processing of personal data should be necessary and proportionate to the purpose(s) for which it is being processed. Therefore, data that is processed should be adequate and relevant to the identified purpose, and not exceed that purpose.

4.6 Accuracy

Personal data should be recorded as accurately as possible and, where necessary, updated to ensure it fulfils the purpose(s) for which it is processed.

4.7 Collection limitation

Collection of personal data shall be limited to such data that is necessary for the purposes of processing.

4.8 Right to Information Respect the rights of the data subject or user

When we collect or process personal information, we notify and take your consent.

4.9 Confidentiality, Security and Availability (CIA)

We maintain Confidentiality, Security and Availability (CIA) of the data we collect or gather. We maintain Confidentiality of data by ensuring that data exchanged is not accessible to unauthorized users. We make sure the Integrity of the data by ensuring that a system and its data has not suffered unauthorized modification; And the Availability guarantees that data, systems and applications are available to users when they need them

4.10 Prevention, detection, investigation and prosecution of contraventions of law

Processing of personal data in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law shall not be permitted unless it is authorized by a law made by Parliament and State Legislature and is necessary for, and proportionate to, such interests being achieved.

4.11 In compliance with law or any order of any court or tribunal

In compliance with law or court order personal data shall be processed if such processing is:

- explicitly mandated under any law made by Parliament or any State Legislature; or
- for compliance with any order or judgment of any Court or Tribunal in India.

4.12 Necessary for prompt action

Prompt action shall be taken for any personal data if such processing is necessary:

- To respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual
- To undertakes any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health
- To undertake any measure to ensure safety of, or help or services to, any individual during any disaster or any breakdown of public order.

4.13 For reasonable purposes

Personal data shall also be processed if such processing is necessary for such reasonable purposes related to the below activities after taking into consideration:

- Prevention and detection of any unlawful activity including fraud
- Whistle blowing
- Mergers and acquisitions
- Network and information security
- Recovery of debt

4.14 Based on explicit consent

Sensitive personal data shall be processed based on explicit consent only.

We process personal data only when there is a legal basis for doing so or you have granted us your consent in this regard.

4.15 Sensitive personal data of children

We shall process personal data of children in a manner that protects and advances the rights and best interests of the child.

4.16 By Implementing Partners

Where the collection and processing of personal data is one of the responsibilities of Implementing Partners, the personal data is being collected and processed on behalf of us. For these reasons, Implementing Partners are expected to respect and implement the same or comparable standards and basic principles of personal data protection as contained in our privacy and legal policies. This applies whether we intend to share personal data to Implementing Partners or Implementing Partners collect personal data in order to carry out agreed activities.

5. Using Our website

This section describes how your personal information is collected, used, and shared when you visit our website.

When you visit our website, we may collect certain information about your device, including information about user web browser, time zone, and some of the cookies that are installed in the user device. Additionally, as you browse our website, we collect information about the individual web pages that you view, what websites or search terms referred you to our website, and information about how you interact with our website. We refer to this information as "Device Information."

We use the Device Information that we collect to improve user experience by enhancing and optimizing our site/application (for example, by generating analytics about how our customers browse and interact with our website/ application, and to assess the success of our marketing and advertising campaigns).

Please note that we do not alter and practice our Site's data collection when we see a Do Not Track signal from user browser.

6. How we collect personal data

We are committed to collect personal data through lawful and transparent means, with your explicit consent where required, which include:

- When you provide us with information in relation to your attendance at any of our hosted events
- When you provide information to us by filling in the forms on our web site or offline
- Creating an online account with us and managing your preferences
- When you contact us, for example, to enquire about our services or apply for a job or face to face
- Through our provision of services to you, or the organization you represent
- Sending us a letter, e-mail or social media message
- Subscribing to receive a service from us (e.g. a newsletter, blog or by following us on social media)
- Requesting promotional information from us (e.g. information about any of our products or services) participating in a survey, competition or prize draw

7. Information we collect while you use our services

When you visit our websites, or our web applications, or do a search get directions or watch a video, we may also collect certain data through the use of "cookies" and other automated means. Cookies are small pieces of data that are stored by your browser on your computer's storage. Such data may comprise the following data:

- Things you search for
- Videos you watch
- Date and time
- Originating IP address
- Domain name
- Type of browser and operating system used (if provided by the browser)
- URL of the referring page (if provided by the browser)
- Object requested
- Completion status of the request
- Geographic location
- Language preferences
- Your location
- Apps, browsers, and devices you use to access Google services
- Contact details (including names, postal addresses, email addresses and telephone numbers)
- Professional information such as job titles, previous roles, and professional experience and qualifications
- Where you provide the information to us, information concerning your interests both business and personal
- Details regarding your attendance at our events, or an event where we met you
- Details of your visits to our website including, but not limited to, traffic data, location data, and web logs
- purchase or delivery of products or services
- reviews and opinions about our brands, products and services
- information we receive about you from franchisee through whom you have availed our services/product

We do not collect data which is, by its nature, particularly sensitive (e.g. genetic data, biometric data, data revealing racial or ethnic origin, political opinions, sex life, sexual orientation, religion or other beliefs, data concerning health, criminal background or trade union membership) unless it is volunteered by you.

8. How we use your personal information

We have a legitimate business interest in operating and improving its business and the services we offer and therefore we use and processes your personal data and we will not do so to the extent that processing would override your interests, rights and freedoms to protect your personal data. In this situation, we shall only process your personal data when you have given us your explicit consent and you have the right to withdraw your consent at any time. Your decision to provide your data for such purposes is optional and shall have no consequence on your ability to stay with us or benefit from the requested services. Your decision to provide personal data (including special category/ sensitive personal data) to us is voluntary, however, if you do not provide such personal data you may not benefit from some of the services.

We process personal information about you for the following purposes:

- To provide you with information and services that you request from us
- To improve the content and methods of delivery of our website and services
- To maintain and develop our relationship with you
- For research, planning, service development, security or risk management
- To carry out services we have agreed to provide to you
- To comply with legal and professional obligations

9. Personal Information for Marketing Purposes

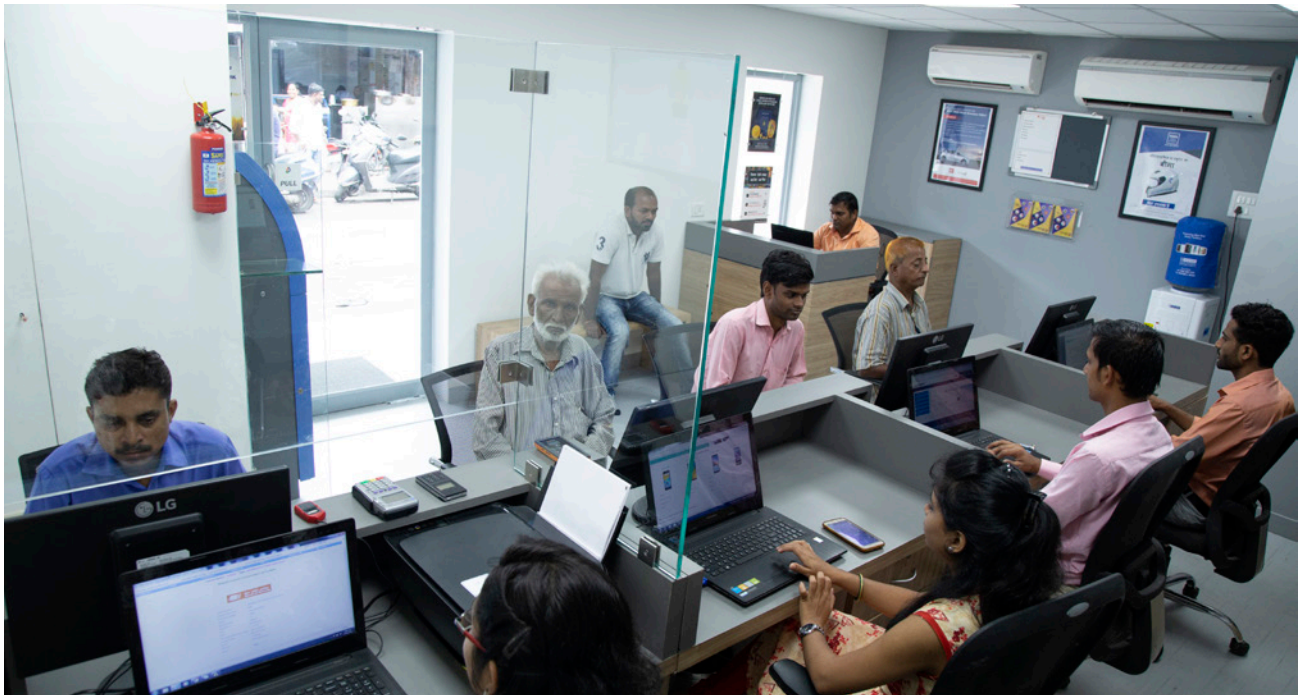
You have the right to ask us not to process your personal information for marketing purposes. When we collect contact information from you (for example, when you provide us with your business card), we may add your details to our contacts database. You can ask us not to use your information in this way at any time by sending us an email at infosec@vakrangee.in.

10. For Minors below the age of 18

Our websites are not for individuals under age 18. Individuals below the age of 18 are not allowed to access the website or provide personal information to us. However, we may collect Personal Information about children below the age of 18 years from the parent or guardian directly, and with that person's explicit consent.

11. Disclosures without Your 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.



12. Customer/User Rights

We shall send you any communications related to product, services, any regulatory or compliance related, or marketing related if you have "opted in" to receiving such communications. You have the right to "opt out" of receiving such communications, whether by email or otherwise, at any time. You can do this by:

- Clicking the unsubscribe link displayed in any of the e-mails you receive
- emailing infosec@vakrangee.in to indicate you no longer wish to receive marketing communications, or
- writing to us at the address below or call us contact details given below:

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

You shall have the following rights in relation to personal data that we hold about you:

12.1 Right to Access

To request confirmation of whether we process personal data relating to you, and if so, to request a copy of that personal data.

12.2 Right to Correction

To request that we rectify or update any personal data that is inaccurate, incomplete or outdated.

12.3 Right to Delete

To request that we delete your personal data in certain circumstances, such as where we collected personal data based on your consent, and you withdraw your consent

12.4 Right to Opt-out

To request that you can opt-out of the emails and communications sent to you by us

12.5 Right to provide consent for Opt-in

To provide consent to opt-in for receiving communications from us

12.6 Right to transfer data

To request to transfer your data to other services providers

12.7 Right to Restriction of Processing

To request that we restrict the use of your personal data in certain circumstances, such as while we consider another request that you have submitted, for example a request that we update your personal data where you have given us consent to process your personal data, to withdraw your consent.

12.8 Right to Withdraw Consent

Where you have given us consent to process your personal data, to withdraw your consent

12.9 Right to Data Portability

To request that we provide a copy of his/her personal data to him/her in a structured, commonly used and machine-readable format in certain circumstances.

To exercise your rights as set out above or to make a complaint or submit an inquiry about our privacy practices, please contact us at infosec@vakrangee.in.

Please Note to help protect his/her privacy and maintain security, we may take steps to verify your identity before we can action your request.

13. How do we Protect Personal Data

We maintain technical, physical and administrative safeguards designed to protect the personal data provided against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use.

All employees receive induction during joining and periodically receive training and awareness emails on data security and/or privacy related risks and procedures.

Also, we provide data privacy and security training and awareness to third party vendor and NDA is signed as well by users/employee/third party vendor.

Employees or management team who might have access to this data in order to provide services shall be contractually obliged

to keep such data in confidence, provide adequate data security measures, and may not use that data for any other purpose.

Also, for your own protection, we encourage you not to include sensitive personal data, credit card or similar personal data in any e-mails you send us or our employee.

14. Customer/User Data Sharing

We share the data with third party who give services on behalf of us and is committed to comply with our policy.

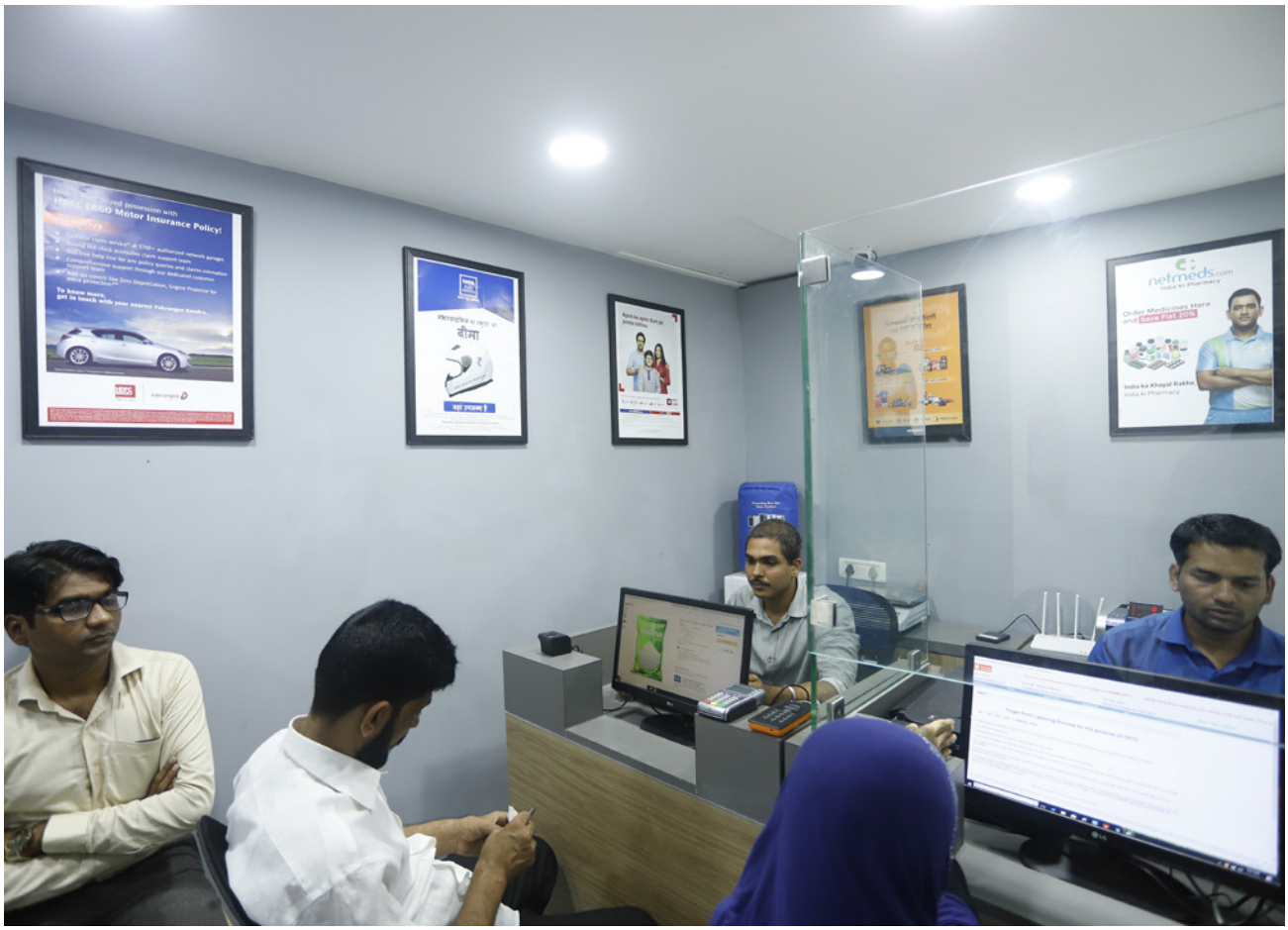
15. Usage of Customer data for Secondary Purposes

We do not use customer data for any purpose other than the primary purpose defined in this Policy. We do not sale customer data to any third party through sale or rentals.

16. We ensure that sharing personal data does not negatively impact:

- The safety and security of our personnel and/ or personnel of Implementing Partners
- The effective functioning of our operation or compromise our mandate, for example due to the loss of the climate of trust and confidence between us and persons of concern or the loss of the perception of us as an independent, humanitarian and non-political Organization.

Before agreeing to share personal data to a third party, we assess the level of data protection afforded by the third party. As part of this assessment, the data controller assess, inter alia, the applicable laws and regulations, internal statutes and policies of the third party, specific contractual obligations or undertakings to respect specific data protection frameworks, their effective implementation as well as the technical and organizational means of data security put in place.



17. Verification

Irrespective of a partnership agreement, we need to verify, prior to sharing personal data to an Implementing Partner or to engaging an Implementing Partner in the collection and processing of personal data, that the processing of personal data by the Implementing Partner satisfies the standards and basic principles of our privacy and legal policies. Such verification may form part of a Data Protection Impact Assessment.

18. Partnership agreements

We mandate Implementing Partners to comply with our privacy and legal policies through an undertaking as part of the signing of partnership agreements. Such agreements also need to specify the specific purpose(s) for the processing of personal data and the legitimate basis for processing.

19. Capacity of the partner

We shall need to assist Implementing Partners in building or enhancing their capacity in order to comply with the data protection standards and principles contained in our Policy. Such assistance may relate to the establishment or adjustment of policies, the delivery of training or putting in place technical and organizational measures.

20. Partnership termination

After termination of a partnership, all personal data collected in the performance of the partnership would be returned to us. Partnership agreements may provide for exceptions, where there are legitimate reasons to do so, namely your consent.

21. Data Share Agreements

Unless there are satisfactory reasons not to do so, prior to sharing personal data to a third party, the data controller shall seek to sign a data share agreement, or, as appropriate, incorporate data protection clauses within broader agreements, particularly where share of personal data are likely to be large, repeated, or structural, i.e. where the same type(s) of data is shared with the same third party for the same purpose over a certain period of time.

Data share agreements should, inter alia:

- address the purpose(s) for data share, specific data elements to be shared as well as data protection and data security measures to be put in place
- require the third party to undertake that its data protection and data security measures follow this Policy
- stipulate consultation, supervision, accountability and review mechanisms for the oversight of the share for the life of the agreement

Our Data Protection Officer and the Legal Officer are to review and clear all data sharing agreements. Copies of final agreements are to be lodged with the Data Protection Officer and Legal Officer.

22. How long we keep personal data for

We are committed to collect and process user data which is limited to the stated purpose only. We maintain appropriate security safeguards to protect your Personal Information and retain it for as long as needed to fulfil the purposes for which it is collected, unless we are required or permitted by law to keep the personal data for longer. We delete your information whenever you request us to do so.

Your Personal data shall be anonymized or deleted if your last interaction with Vakrangee was over 7 years ago. "Interaction with Us includes visiting our office or for franchisee communications if any.

23. Data Retention Policy

	Personal Data Type	Retention Period
Guest Personal Data	Payment Information	3 years
	All other guest personal data	7 years after last engagement with Us
		Engagement includes visiting our office or for franchisee communications if any
CCTV	Video surveillance at Vakrangee for incident, crime and fraud prevention and to protect our guests and employees	90 days

24. Cookies

A "cookie" is an element of data that a website can send to your browser which may then be stored on your system. We use cookies to gather data about the visitors to our websites (as they enable us to improve our websites and deliver a better and more personalized service). We do not associate the data in a website visitor's cookie with any other data about that visitor.

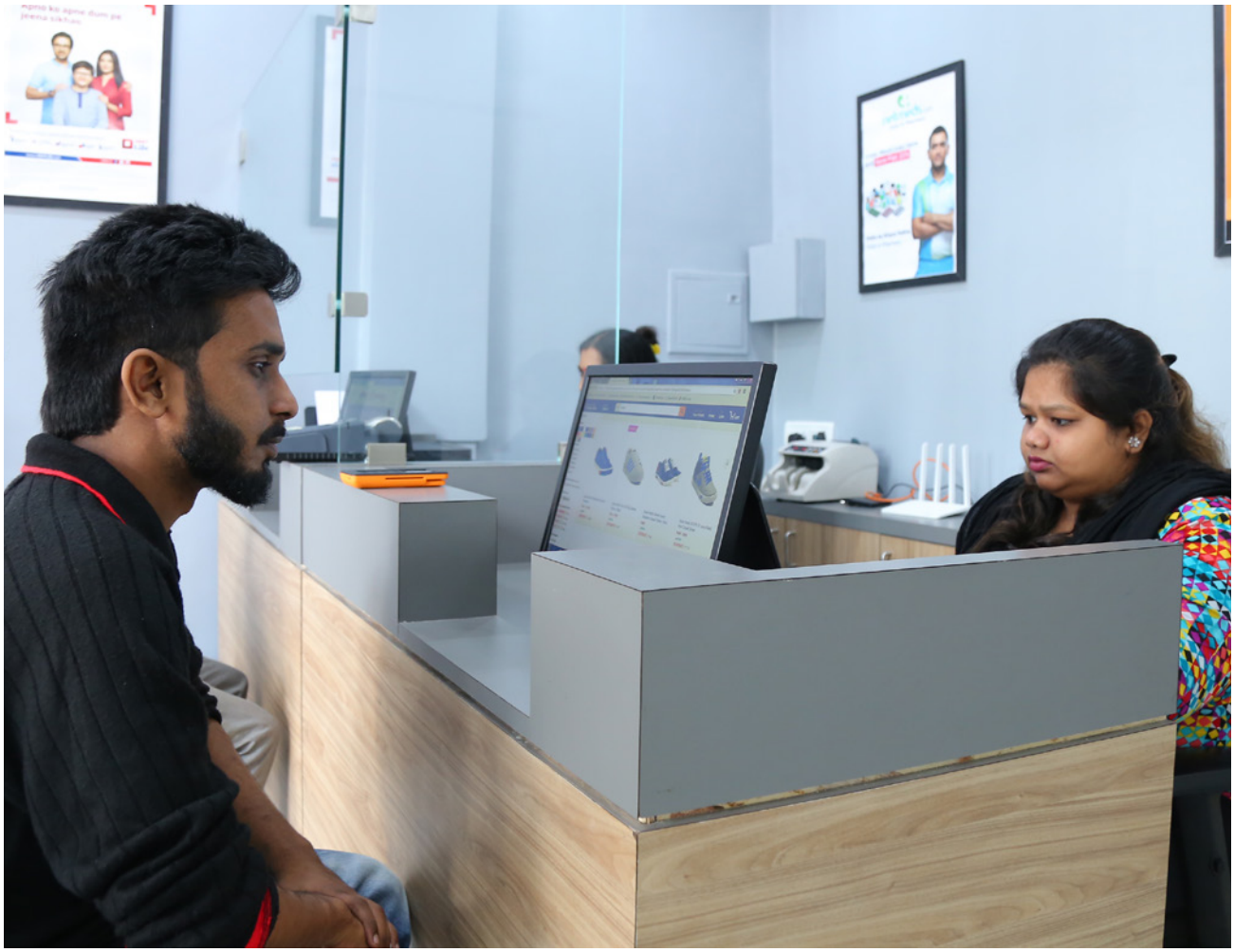
The cookies we use on our websites, where you have accepted are for maintaining session, user preferences, site performance information, site functionality, analytics, conversion tracking.

We do not control the use of third-party technology either use by the browser or any application install in your system. We are not responsible for any actions or policies of such third parties.

When you access our websites/applications, you will receive a clear notice advising you that the websites/applications you are visiting or using intends to use cookies and that:

- By continuing to use the website you consent to their use; or
- you must click an "I accept" box for cookies to be placed.

Unless you have adjusted your browser setting so that it will refuse cookies from our websites, our system will issue cookies. Most browsers will tell you how to stop accepting new cookies, how to be notified when you receive a new cookie, and how to disable existing cookies. You can find out how to do this for your browser by clicking "help" on your browser's menu. Please note, however, that without cookies you may not be able to take full advantage of some of our websites/applications features.



25. Data storage limitation

Our data protection team shall retain personal data only if may be reasonably necessary to satisfy the purpose for which it is processed.

Personal data that is not recorded in individual case files is not to be retained longer than necessary for the purpose(s) for which it was collected.

All individual case files, whether open or closed, are considered permanent records, and must therefore be permanently retained in line with our Access Policy

Our data protection team undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession.

26. In case of Data Breach

A breach of data security leading to the accidental or unlawful/ illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data shared, stored or otherwise processed. Our employees notify the Data Controller / Data Protection Officer/ Information Security Manager as soon as possible upon becoming aware of a personal data breach and to properly record the breach.

- **Disciplinary Action in case of Violation of Data Privacy Policy**
  Adherence to Data Privacy Policy is considered as an important parameter while evaluating performance of employees. We have zero tolerance for any kind of data breach done by any of our employees. In case, any employee is found violating any sections of the Data Privacy Policy, disciplinary and/or legal action is taken.

If a personal data breach is likely to result in personal injury or harm to a data subject, the Data Controller / Data Protection Officer/ Information Security Manager shall use his or her best efforts to communicate the personal data breach to you and take mitigating measures as appropriate without undue delay.

The notification shall describe:

- The nature of the personal data breach, including the categories and number of data subjects and data records concerned
- The known and foreseeable adverse consequences of the personal data breach
- The measures taken or proposed to be taken to mitigate and address the possible adverse impacts of the personal data breach

27. Updates to our Privacy Policy

This Privacy Policy was last updated in January 2020. We update this privacy policy from time to time. If we change our Privacy Policy, we shall post the changes on our website so that you may be aware of the information we collect and its uses. You shall therefore review this page regularly to ensure that you are aware of any changes to our terms. If the user consent for this policy has been taken in the past, it shall be taken again.

If you need any clarifications or help about this Privacy Policy, please contact infosec@vakrangee.in.

28. Periodic Audit by Internal and External IT Auditors

We periodically audited by external and internal auditor for ISO 27001:2013, ISO 9001:2015, ISO 22000-1-2011 certifications. We also conduct or undergo Information Security audit for its entire IT systems by external agencies, regulatory and statutary bodies.

29. Information collected when you use our Mobile Application

When you download our mobile application we may collect, including but not limited to, the below information from you:

- Email ID
- Mobile number
- Location/IP address for geo-locating
- Device details such as Device ID, Make, Model, Mac ID, OS details etc.

30. We implement appropriate information safeguards commensurate with the level of risk.

Such safeguards include but are not limited to:

Control Objective	Description
Access Control	Access to our non-public information is controlled in accordance with the authorized privileges of the user requesting access.
Awareness and Training	We provide ongoing security and privacy awareness training to its employee.
Audit and Accountability	The information systems maintain a record of system activity by system or application processes and by user activity.
Configuration Management	Systems are built and maintained according to a baseline configuration standard which addresses security.
Data Governance	The right data is used by a person in the right role and only in the right context.

Control Objective	Description
Identification and Authentication	The system verifies that people are who they claim to be. Identify and authenticate individuals in a manner that balances the right to privacy and protection of personal information with the need of organizations to collect, use and disclose personal information for legitimate purposes.
Information Security Management System	We establish, implement, operate, monitor, review, maintain and improve information security.
Incidence Response	We have a defined, repeatable process for managing information security related incidents.
Media Protection	We protect media throughout its lifecycle. Only authorized personnel shall have access to Media. Media is always stored in a safe and secure environment. Contents of the re-usable media are always erased when the information is no longer required.
Technology Absorption	We have our own technology policy for our acquisition, absorption and adaptation, on long-term as well as short-term basis. We adept Co-development and co-production.
Personnel Security	We identify the security controls needed to properly address how users, designers, implementors, and managers interact with computers and the access and authorities they need to do their job.
Physical and Environmental Protection	Our facilities are protected against physical and environmental threats. We develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides. We remove individuals from the facility access list when access is no longer required. We escort visitors and monitor visitor activity.
Risk Management	We continually analyse, respond to, communicate, and manage specific risks to our systems.
System and Services Development and Acquisition	Information security and privacy is addressed throughout the development lifecycle.
System and Communications Protection	The technical implementation of the system provides a base level of confidence in the technical implementation so that the system's various security functional capabilities can be trusted.
System and Information Integrity	Systems and information are protected against unauthorized modification.
Compliance	We adhere to the applicable government body regulations, legal, and contractual requirements.

31. Data Controller / Data Protection Officer/ Information Security Manager / Legal Officer

The data controller is responsible for establishing and overseeing the processing of personal data under his or her area of responsibility. He or she therefore also bears the main responsibility for compliance with the Policy. We have appointed a Data Protection officer to obtain more information in data privacy or to submit suggestions or complaints regarding the processing of personal data who can be contacted on email or address given.

Data Controller carryout the following functions:

- Monitoring personal data processing activities to ensure that such processing does not violate the provisions
- Providing advice where required on the way data protection impact assessments must be carried out, and carry out the review of such assessment
- Providing advice where required on the way internal mechanisms may be developed in order to satisfy the principles set out
- Helping and cooperating on matters of compliance
- Act as the point of contact for the purpose of raising grievances
- Maintaining an inventory of all records
- Providing advice, support and training on data protection and this Policy
- Maintaining inventories of data share agreements, specific instances of data sharing by us with third parties, data protection impact assessments, data breach notifications and complaints by data subjects
- Actively encouraging data controllers and other relevant actors to undertake measures aimed at compliance with this Policy
- Monitoring and reporting on compliance with this Policy

32. Grievance Redressal

We have proper procedures and effective mechanisms in place to address grievances efficiently and in a speedy manner.

If you require any information or clarification regarding

- The use of your personal information or
- Any violation of data or any of the provisions of this policy or
- This privacy policy or
- If any grievances with respect to use of your personal information or
- If you would like us to update your personal data we have about you or your any preferences, or to exercise your rights (as detailed above),

You can raise grievance related to privacy issues, the following escalation matrix can be used

- Level 1 - Information Security Officer - infosec@vakrangee.in
- Level 2 - Data Protection Officer / Group CTO - sanjayn@vakrangee.in
- Level 3 - Director - R&D (Board Representative) - drhayat@vakrangee.in

33. Conclusion

We conclude that we at Vakrangee:

- Prevent illegal access to and loss, destruction, falsification or leakage of personal and sensitive data. We manage personal and sensitive data strictly and perform security countermeasures to ensure the data is not illegally accessed, lost, destroyed, falsified or leaked.
- Collect personal and sensitive information when it is reasonably necessary and with their due consent. We ensure that only those who need to use this information have access to it.
- Observe laws and regulations for protecting personal and sensitive data. We follow the data protection, security and privacy laws and regulations for personal and sensitive data of individuals.
- Continuously improve the process of protecting personal and sensitive data. We regularly monitor the laws and regulations for data protection, security and privacy and update our systems and processes ongoing basis. We educate all the stakeholders for the updated systems and processes.
- Amend and delete personal and sensitive data. If we receives a request to amend or delete data related to personal data protection, unless there is a special reason not to do so, the request shall be suitably met after verifying and validating the identity and authority of the requester.

We are committed in ensuring the confidentiality, protection, security and accuracy of personal information available to it and it has been our ongoing strict policy to ensure that personal information is accurate, complete, not misleading, up-to-date and stored in a secure environment protected from unauthorized access, modification or disclosure. We would also ensure that personal data shall not be used for political and commercial purposes. In case of any concerns, the Information Security Manager and Data Protection Officer can be contacted at infosec@vakrangee.in

Vakrangee
सशक्त परिवर्तन

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