Privacy Policy

Nov 2025

Fintech Association for Consumer Empowerment

Table for Contents[1]

[1] Board approved the policy through email circulation on 13 Nov 2025. The policy was last updated by the Board at its meeting on 19 Dec 2025.

1. Purpose

This Privacy Policy describes how Fintech Association for Consumer Empowerment (**FACE**) may collect, process, store, and /or use its Users' (defined below) information.

FACE is fully committed to safeguarding and protecting the privacy, confidentiality, and security of the non-public information we collect and receive. We are dedicated to implementing appropriate measures that prioritise the protection of our stakeholders' information, always maintaining their trust and confidence in us.

This Privacy Policy is designed to communicate how we collect, use, disclose, delete and protect users' (including members, customers, vendors, project partners, and stakeholders) information when they engage with FACE by exchanging non-public information. The policy is in accordance with relevant and applicable data protection regulations/laws, and in the event of any conflict or interpretation issues, the regulations/laws will prevail.

You are advised to carefully read the Privacy Policy before sharing information or data (including any Personal Data) with us or our Representatives (defined below), or before accessing our website or interacting with us. We shall not be liable/responsible for any breach of privacy owing to your negligence.

Users have rights under applicable data protection laws, including the right to access, correct, or delete their information as detailed later in this policy.

2. Definitions

(a) "**Applicable Law**" shall mean all applicable statutes, act of legislature or parliament, laws, bye-laws, enactments, regulations, ordinances, policies, treaties, rules, notifications, circulars, government resolutions, directions, directives, permits, guidelines, requirements, licenses, rule of common laws, orders, decrees, judgments, injunctions, writs or orders of any court of record having the force of law, or any restrictions or conditions including any similar form of decision of, or determination, application or execution by, or interpretation or pronouncement having the force of law of, any authority having jurisdiction over the matter in question, whether in effect as on the date of this Privacy Policy or thereafter and shall include any re-enactment, substitution or amendment thereof and shall include Data Protection Laws.

(b) "**Cookies**" means a small file placed on your device when you either visit or use certain features of our website, which allows a website or application to remember your actions or preferences for a certain period of time.

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

(d) **Data Protection Laws**" means and includes the applicable legislation and regulations relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data or privacy of an individual including (without limitation):

(i) The Digital Personal Data Protection Act, 2023 (as and when enforced and amended or superseded from time to time) and the subordinate legislation thereunder;

(ii) The Information Technology Act, 2000 (as amended or superseded from time to time),

including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, CERT-In Rules, CERT-In Directions, and any other subordinate legislation framed thereunder;

(iii) Any other Applicable Laws solely relating to the protection of Data and processing, storage, usage, collection and/or application of Data or privacy of an individual.

(e) "**Governmental Authority**" means any Indian government entity, authority or body exercising executive, legislative, judicial, regulatory or administrative functions of or pertaining to government, including any government body, agency, department, board, commission or instrumentality of India, including the RBI, or any political subdivision thereof, or any court, tribunal or arbitrator, and any securities exchange or body or authority regulating such securities exchange.

(f) "**Log Data**" may include User's computer's Internet Protocol ("**IP**") address, browser version, pages visited, date and time of the visit, duration spent on those pages, and other relevant statistics transmitted from User's website.

(g) "**Personal Data**" means any Data or information about an individual who is identifiable by or in relation to such Data, as defined under the Digital Personal Data Protection Act, 2023.

(h) "**RBI**" shall mean the Reserve Bank of India.

(i) "**Reasonable Security Practices and Procedures**" means security practices and procedures designed to protect information from unauthorised access, damage, use, modification, disclosure or impairment.

(j) "**Representatives**" means the persons engaged by FACE for the purpose of their functions.

(k) "**SRO-FT**" shall mean a self-regulatory organisation in the FinTech sector

(l) "**User**" shall mean and include applicants, members, vendors, project partners, stakeholders, general respondents voluntarily participating in research studies and any other person providing information to FACE or visiting its website.

(m) "**Usage Data**" means and includes various details, including but not limited to the User's IP address, browser type, browser version, the specific pages navigated on the website, the date and time of visit, the duration spent on those pages, as well as unique device identifiers and other diagnostic data. When accessing the website through a mobile device, the gathered usage data may extend to details such as the specific type of mobile device utilised, the device's unique ID, the IP address of the mobile device, the mobile operating system, the type of mobile internet browser utilized, unique device identifiers, and additional diagnostic data.

(n) "Processing" means any wholly or partly automated operation or set of operations performed on Personal Data, such as collection, recording, organisation, storage, use, sharing, disclosure, or deletion.

3. Applicability

The privacy policy rigorously applies to all the non-public information that FACE receives or collects from a range of stakeholders, including but not limited to members, vendors, project partners, and customers (defined as customers of member companies or general respondents voluntarily participating in our research studies.) It mandates full adherence to data handling practices, ensures transparency in data usage, and provides clear guidelines for data protection measures. This policy is intended to complement, rather than replace, any previous consents the users may have provided to FACE regarding their data.

This policy also applies to any third-party service providers or partners engaged by FACE for processing data on its behalf. Such entities are required to adhere to equivalent data protection and confidentiality standards as outlined in this policy.

4. Data acquisition, utilisation and storage

FACE ensures that all data, information, and documentation are acquired, utilised, and stored following the terms specified below:

a. Data acquisition

- Data from companies applying for FACE membership shall be collected in accordance with the FACE application process, which includes PAN/TIN/MoA/GSTN, details of founders/investors, shareholding pattern, employee count, financial position, specifics of lending business (disbursement value/AUM), and contact information of designated persons (name, designation, email, phone) required for the application process. Applicants are informed in advance about the information required in the application form.
- Any requests by FACE for data, information, and documentation from member companies and their authorised representatives (email and phone details) shall be formally made in writing (by email) to the designated representatives of the companies, ensuring that all collected data is in electronic format with explicit consent clarifying the use and process to withdraw the consent and delete previous data, if any, at the request of the data owner.
- On an ongoing basis, several different data and information sets (quantitative and qualitative, such as quarterly data, ad-hoc surveys, research reports, policies, documents, sample loan documents, partner details, anonymised mobile numbers of the customer for demand survey, etc.) shall be collected from members' authorised representatives, founders, CEOs, and employees, capturing their names, designations, official emails, and mobile numbers.
- Contact details, including names, designations, company affiliations, websites, app links, and activities, shall be captured for a wide range of stakeholders such as Fintechs, regulated entities, RBI, government entities, research institutions, think tanks, vendors, and partners associated with or outside formal relationships with FACE through public sources and contacts established through the network.
- The purpose of collecting data, information, and documentation shall be clearly communicated at the time of request. Data collection shall be limited to information necessary for its intended purpose.
- As and when customers' contacts FACE via email or phone with inquiries or complaints, they often provide their names, contact information (email/phone), account details (such as loan account number, lender, customer ID), and occasionally, their KYC data. Such data will be stored confidentially and will be diposed off, after the satisfactory closure of the complaint. Any unsolicited data, if received, shall be promptly and confidentially disposed of to ensure effective safeguarding of data privacy.
- FACE does not collect, process, or store any payment instrument details such as debit/credit card numbers, CVV, UPI IDs, or bank account information. All payment transactions for membership or other contributions are processed securely through authorised payment gateway partners (e.g., Razorpay) in compliance with applicable payment and data protection regulations.

- The lawful basis for processing such data includes the user's consent, legitimate interest in pursuing FACE's objectives as an industry association, and contractual or regulatory necessity where applicable.

b. Data utilisation

- All data, information, and documentation collected shall be processed solely for the purposes for which it was collected or for any other incidental purposes that members would reasonably expect, considering the specified purposes and the context of the collection. This information shall be strictly used for stated purposes.
- The data collected from companies applying for FACE membership is used to evaluate their eligibility and credentials for FACE membership.
- The contact data collected from members is to facilitate regular participation with FACE meetings, interactions, AGMs, EGMs, and for ongoing operational requirements.
- A repository is maintained for the data collected from Fintechs, LSPs, stakeholders, RBI, government entities, research institutions, think tanks, vendors, partners, etc. (whether affiliated with FACE or not). This repository provides updated market information to facilitate engagement with these entities as necessary, utilising publicly available data and voluntarily shared details such as employee coordinates.
- FACE shall process all data, information, and documentation fairly and reasonably, respecting the privacy of the data. If FACE shares any data with third-party processors or service providers, it will inform them beforehand and ensure that third-party vendors follow this policy.
- The FACE team's access to data for information, handling, and processing is on a need-to-know basis.

c. Data Storage

All data, information, and documentation collected from members, including employees and board/committee members, will be stored on cloud-based servers in data centres, in accordance with data privacy and storage requirements under applicable Indian laws. Such information may also be stored on employees' respective systems, subject to ensuring proper safeguards against any unauthorised access or use/data breaches, and business continuity.

Data will be retained only for as long as necessary to fulfil the purpose for which it was collected or as required under applicable law or regulatory obligations. Upon the user's request or once the retention purpose is met, the data will be securely deleted or anonymised in accordance with FACE's data retention policy.

FACE employs reasonable administrative, technical, and physical safeguards—such as access controls, encryption, and secure cloud infrastructure—to protect stored information against unauthorised access or disclosure.

5. User's Representation.

- Every User represents to FACE that she is 18 years of age or above and is in a contracting capacity to share her Data with us.
- In circumstances where the User provides us with Data relating to other individuals on their behalf, the User represents and warrants that she has obtained such individuals' consent for, and hereby consent on behalf of such individuals to, the collection, use, disclosure and processing of such individuals' Data by us. User confirms that the Data she provides to us regarding other

individuals mentioned in this clause is complete, accurate, and consistent.

6. Cookies

Cookies are small data files often used as anonymous, unique identifiers. When the users access the website, these files are sent to the browser and stored on the computer's hard drive. The website employs these "cookies" to gather information and enhance its service. Cookies used on the FACE website may include:

- Essential cookies, which are necessary for core website functions such as navigation and secure access.
- Analytics cookies, which help us understand how visitors use our site in aggregate and enable us to improve its performance.
- Preference cookies, which remember your display settings or other choices to enhance your experience.

FACE does not use cookies for advertising, profiling, or cross-site tracking purposes. Users can accept or decline these cookies and will be notified when a cookie is sent to their computer. Declining cookies may limit access to certain parts of the website. Most browsers automatically accept cookies, but users can modify their browser settings to decline them if preferred. Users can manage their cookie preferences through their browser settings at any time, including deleting existing cookies or restricting new ones. Please note that disabling certain cookies may limit functionality or access to some parts of the website.

7. Links to Other Sites

Our Service may provide links to other websites. Clicking on a third-party link will redirect the user to the respective site. Understanding that these external sites operate independently and are not within our control is essential. Therefore, reviewing the privacy policies of these websites is strongly recommended. We cannot be held responsible for any content of third-party sites or services, privacy policies, or practices. Please be advised that the User's interaction with websites linked through our service is subject to the terms of use and privacy policies of those third-party websites.

8. Usage data

FACE may collect information transmitted by the user’s browser each time the user visits the website via a mobile device, referred to as "Usage Data."

This Usage Data encompasses various details, including but not limited to the user’s computer's Internet Protocol (IP) address, browser type, browser version, the specific pages navigated on the website, the date and time of visit, the duration spent on those pages, as well as unique device identifiers and other diagnostic data.

The Usage Data is collected solely for internal analytics and technical purposes, such as monitoring website performance, understanding aggregate user interactions, and improving the content and usability of FACE’s digital platforms. FACE does not use Usage Data for profiling, advertising, or behavioural tracking. If any third-party analytics service (such as website traffic or security monitoring tools) is used, such service providers are contractually bound to comply with equivalent data protection and confidentiality standards as set out in this Policy.

When accessing the website through a mobile device, the gathered usage data may extend to details such as the specific type of mobile device utilised, the device's unique ID, the IP address of the mobile

device, the mobile operating system, the type of mobile internet browser utilized, unique device identifiers, and additional diagnostic data.

9. Location Data

With consent, FACE may use and store information about the User's location ("Location Data"). This information empowers us to tailor features to meet specific needs and continually refine our services. Users can enable or disable location services on the website at any time through their device settings.

10. Retention of Data

FACE will retain user data for the duration necessary to achieve the purposes for which it was collected and as required by legal or regulatory obligations. Any information that is no longer necessary will be retained for a period of eight (8) years until the retention period of such information is specified by the RBI and any other timeline communicated by the government and regulators.

Where required or appropriate, FACE may retain certain anonymised or aggregated data beyond the specified retention period solely for statistical, research, or regulatory reporting purposes, provided that such data no longer contains any information that can identify an individual or organisation.

11. Disclosure

We pledge not to disclose any Information without the user's prior explicit consent. When collaborating with third parties, we enforce confidentiality standards through Non-Disclosure Agreements (NDAs). Notwithstanding anything contained in this policy, FACE reserves the right to disclose any collected data, information, and documentation to RBI and any government entity and law enforcement agencies inspect, seize, or access such materials when deemed necessary or appropriate by FACE at its sole discretion.

12. Security

We deeply appreciate the User's trust in sharing their Data and employ commercially acceptable methods to safeguard it. FACE shall undertake Reasonable Security Practices and Procedures and implement appropriate technical and organisational measures to secure the confidentiality, integrity, and availability of your Data.

These measures include, among others, encryption, access control mechanisms, role-based authorisations, secure cloud infrastructure, network firewalls, and regular monitoring of systems for potential vulnerabilities. FACE also conducts periodic security reviews and audits to ensure continued adherence to applicable data protection and information security standards.

13. Modifications to Account Information and Preferences

FACE allows users to update the information provided during registration, including communication preferences with us. Users can discontinue the use/transfer/transmission and sharing of their information by writing to us. FACE will accept such information only from/under the signature of an authorised signatory (Founder/CEO or others). FACE will honour the user's request to discontinue the use of information promptly upon receipt of the instructions unless otherwise as required by regulator and law enforcement agencies.

14. Revisions

FACE may revise this Privacy Policy from time to time to ensure alignment with forthcoming developments, industry trends, and any pertinent shifts in legal or regulatory frameworks. FACE will publish updates promptly on its website and inform users of any changes.

15. Inquiry and Grievance Redressal

For any further queries, complaints or grievances related to this Privacy Policy, you could write to us sro@faceofindia.org. All grievances or complaints received at this address shall be acknowledged within seven (7) working days and resolved within thirty (30) working days of receipt, to the extent practicable. If you are not satisfied with the resolution provided, or if the complaint remains unaddressed within the specified timeframe, you may escalate the matter to the relevant Data Protection Authority or other competent authority under applicable law.