

Privacy Statement

The following Privacy Policy governs the online information collection practices of Auxify (a Brand of Getit Express Private limited) and Getit Express Private Limited (“Auxify”, “we,” “us,” “our”). It outlines the types of information that we gather about you while you are using our website, our digital platforms & services, and the ways in which we use this information.

Auxify/Getit Express Private Limited is an AI services company which builds customized AI solutions for enterprises. We process your data in accordance with the applicable laws and regulations following industry best practices.

PURPOSE AND SCOPE

The Privacy Policy applies primarily to information that we collect online; however, it may apply to some of the data that you provide to us offline and/or through other means, as well (for example, via telephone or through the mail). The Privacy Policy documents and describes the manner in which our organization collects information from all our users/viewers of our services. While providing our services on behalf of our registered users, we collect information related to viewers. The use of information collected on behalf of our users is governed primarily by our contract for the engagement with them and the privacy policies governing their organization. We are not accountable for the privacy policies and practices undertaken by our users or any other third parties.

HOW DO WE WORK

A. Artificial Intelligence & Automated Processing:

We provide a platform which will perform AI based calling where;

- Interactions is AI-generated or AI-assisted;
- Voice responses may be synthesized;
- AI may analyze conversations;
- AI may generate summaries/transcripts;
- Automated workflows may route conversations;
- Human review may occur;
- Users may request human assistance;
- AI outputs may not always be accurate.

HOW WE COLLECT DATA ABOUT YOU

We may collect different data from or about you depending on how you use the sites.

Data collected through automated means:

System Data

Technical data about your computer or device, like device type, operating system, and IP address. This data helps us improve the delivery of our web pages and to measure traffic on the site. The collection of data will also depend on the individual settings of your device and software. It is recommended to refer to the policies of your device manufacturer or software provider to learn about information they might share with us.

User Generated Data:

Usage as a viewer

We collect information and material (user-generated content) provided to us voluntarily by our users or the viewers to publish and process on our website. The user-generated content is inclusive of text, photos & videos associated with the accounts/ emails used to access links as viewers. Some information is collected through the use of cookies, web beacons, and tracking technologies. Please refer to the Cookie Policy for more details on the type of cookies being used.

THE TYPE OF INFORMATION WE COLLECT AND STORE

Depending on the nature of the Services used, integrations enabled, and interactions conducted through our platform, we may collect, receive, generate, process, analyze, store, or otherwise handle various categories of personal information, communication data, technical information, and business-related data.

The categories of information we may collect include, without limitation:

A. Personal Information

We may collect personal information such as:

- First name and last name;
- Mobile phone number;
- Email address;
- Postal address;
- Business name;
- Company information;
- Designation or job title;
- Profile photograph;
- Customer identifiers;

- Government-issued identifiers where legally required;
- Communication preferences;
- Location information;
- Ip address;
- Account credentials and authentication information.

B. Communication & Interaction Data

In connection with our communication automation, AI engagement, voice calling, messaging, and customer interaction services, we may collect and process:

- Call recordings;
- Voice call metadata;
- Call transcripts;
- AI-generated call summaries;
- Customer support interactions;
- Chat conversations;
- WhatsApp messages;
- Instagram direct messages;
- Email communication content;
- Sms content;
- Attachments and media shared through communications;
- Customer queries and responses;
- Ticketing and support records;
- Communication timestamps;
- Delivery and read receipts;
- Communication preferences and opt-in/opt-out records.

C. AI & Conversational Processing Data

Our Services may use artificial intelligence, machine learning, conversational automation, and analytics technologies. In connection with such services, we may collect and process:

- Prompts and instructions submitted to AI systems;
- AI-generated responses and outputs;
- Conversational workflows;
- Interaction analytics;
- Communication intent analysis;
- Sentiment analysis;
- Conversation quality metrics;
- Engagement scoring;
- Lead qualification data;
- Automation triggers and workflow logs;
- Behavioral patterns and interaction history;

- Customer engagement insights;
- Conversational performance analytics.

D. CRM & Business Workflow Data

Where users connect CRM systems, customer engagement platforms, sales tools, or business applications, we may process:

- Lead information;
- Customer records;
- Sales pipeline information;
- Sales notes and interactions;
- Customer preferences;
- Support history;
- Business workflow information;
- Tags, labels, and segmentation data;
- Account activity history;
- Follow-up schedules;
- Internal business notes;
- Campaign interaction data;
- Customer lifecycle information.

E. Technical & Device Information

We may automatically collect certain technical information regarding devices, browsers, APIs, systems, and platform usage, including:

- Browser type and version;
- Operating system;
- Device identifiers;
- Device type;
- Ip address;
- Geolocation information;
- API request logs;
- Server logs;
- Browser and device fingerprinting information;
- Cookies and tracking identifiers;
- Authentication logs;
- Login activity;
- Session information;
- Integration metadata;
- Network and connectivity information;
- Platform performance analytics;
- Crash reports and diagnostic data.

F. Integration & Third-Party Platform Data

Where users integrate third-party services with our platform, we may receive and process data from such integrations including:

- WhatsApp Business platform data;
- Meta and Instagram account information;
- CRM synchronization data;
- Cloud telephony metadata;
- SIP integration information;
- Email platform interaction data;
- Analytics platform data;
- Ticketing system information;
- Workflow automation data;
- Webhook and API integration information.

G. Payment & Transaction Information

Where applicable, we may collect limited payment-related information including:

- Billing address;
- Invoicing information;
- Transaction references;
- Subscription details;
- Payment status;
- Tax-related information.

Payment card information may be processed directly by authorized third-party payment processors and may not be stored by us except as necessary for lawful business and accounting purposes.

H. Sensitive & Special Categories of Information

Certain Services may involve the processing of potentially sensitive information depending upon customer usage patterns, communication content, integrations, or workflows enabled by users.

Such information may include:

- Voice recordings;
- Biometric voice characteristics;
- Financial communication content;
- Customer support discussions;
- Health-related communications where voluntarily shared by users;
- Authentication or verification data.

We process such information only:

- As necessary for providing Services;
- Under user instructions;
- In accordance with applicable law;
- Subject to appropriate security safeguards.

I. Information Generated Through Automated Systems

We may generate derived information, insights, analytics, scores, predictions, recommendations, summaries, or classifications based on interactions with the Services. Such generated information may be used for:

- Workflow automation;
- Conversational optimization;
- Analytics and reporting;
- AI model performance;
- Fraud detection;
- Quality monitoring;
- Customer support;
- System security;
- Operational improvement.

J. Information Provided by Enterprise Customers

Where our Services are used by businesses or enterprise customers, such customers may upload or share information relating to their employees, customers, leads, vendors, prospects, or users.

In such cases:

- The enterprise customer remains responsible for obtaining necessary consents and authorizations;
- We process such information on behalf of and under instructions from the enterprise customer, subject to applicable agreements and laws.

HOW WE USE YOUR PERSONAL INFORMATION

The above personal information may be used for the following purposes:

- To provide you with information about our offerings and/or our periodic newsletters;
- To respond to your requests;
- For creation or development of business intelligence or data analytics in relation to the offerings provided by us (for this purpose we may share the personal information with certain software or tools available online);

- To manage our relationship with you;
- For internal record keeping;
- To provide you with authorization to login and use your user account;
- To verify your identity;
- To maintain correct and up-to-date information about you;
- To identify you as a contracting party;
- To improve our website;
- To enable automated handling of the subscriptions;
- To otherwise be able to provide the services to you;
- To respond to lawful requests by public authorities, including to meet national security or law enforcement requirements; and
- To comply with our other legal or statutory obligations.

LEGAL BASIS FOR PROCESSING

We process personal information, communication data, AI interaction data, customer records, and related information only where we have a lawful basis to do so under applicable laws and regulations.

The legal basis for processing may vary depending on:

- The nature of the Services used;
- The type of information processed;
- The relationship between the parties;
- Customer configurations and instructions;
- Applicable legal and regulatory requirements.

Depending on the circumstances, we may rely upon one or more of the following legal bases for processing.

Consent

We may process information where users, customers, communication recipients, or authorized individuals have provided consent for specific processing activities.

Such consent may include, where applicable:

- Consent to receive communications;
- Consent for AI-assisted or AI-generated interactions;
- Consent for call recording or monitoring;
- Consent for marketing or promotional communications;
- Consent for communication through WhatsApp, Instagram, Email, SMS, Voice calling systems, or related platforms;
- Consent for cookies or tracking technologies;
- Consent for optional integrations or platform features.

Where processing is based on consent:

- Users may withdraw consent subject to applicable law and operational limitations;
- Users may withdraw consent by:
 - Updating account settings where available;
 - Contacting the Grievance Officer;
 - Using unsubscribe or opt-out mechanisms;
 - Submitting requests through designated support channels.
- Withdrawal of consent may affect the availability or functionality of certain services.

Enterprise customers utilizing the Services remain responsible for obtaining legally required consents from their end users, customers, employees, leads, prospects, or communication recipients where applicable.

DPDP Consent Notice

Where consent is relied upon for processing personal data under applicable Indian law:

- Consent shall be free, specific, informed, unconditional, and unambiguous;
- Consent requests shall be presented in clear and plain language;
- Individuals may withdraw consent at any time through available mechanisms;
- Withdrawal of consent shall not affect the lawfulness of processing undertaken prior to such withdrawal;
- Withdrawal of consent may affect the availability or functionality of certain Services.

We shall make reasonable efforts to provide notice regarding:

- The categories of personal data processed;
- The purposes of processing;
- The manner in which individuals may exercise their rights;
- Grievance redressal mechanisms available under applicable law.

Performance of Contract

We may process information where such processing is necessary for:

- Providing the Services;
- Performing contractual obligations;
- Enabling account functionality;
- Onboarding enterprise customers;
- Facilitating integrations;

- Processing transactions;
- Managing subscriptions;
- Customer support;
- Platform administration;
- Communication routing and workflow execution;
- Enforcing contractual rights and obligations.

Without such processing, certain Services or functionalities may not be available.

Legitimate Interests under Applicable Indian Laws

In certain circumstances permitted under applicable Indian data protection laws, including the Digital Personal Data Protection Act, 2023 (“DPDP Act”), we may process personal data for certain legitimate uses without separately obtaining consent where such processing is expressly permitted by law. We may process information where reasonably necessary for our legitimate business, operational, security, administrative, or commercial interests, provided such interests are not overridden by applicable legal rights or protections.

Such legitimate interests may include:

- Improving platform performance and reliability;
- Enhancing AI and automation functionality;
- Analytics and operational reporting;
- Fraud prevention and abuse detection;
- Network and information security;
- Platform monitoring and troubleshooting;
- Customer support and service management;
- Research and development;
- Service optimization;
- Enforcing our terms and policies;
- Protecting users, customers, and platform integrity;
- Maintaining business continuity and operational resilience.
- Compliance with legal obligations;
- Responding to medical emergencies;
- Fraud detection and prevention;
- Cybersecurity and information security activities;
- Prevention of unlawful activities;
- Protection of rights and claims;
- Employment-related purposes permitted under law;
- Processing publicly available personal data in accordance with applicable law;
- Business continuity, network security, and operational protection activities;
- Other lawful purposes expressly permitted under applicable law.

Where appropriate, we may take measures intended to minimize the impact of such processing on user privacy and rights.

Legal & Regulatory Obligations

We may process information where necessary to comply with:

- Applicable laws and regulations;
- Legal processes and governmental requests;
- Telecom and communication regulations;
- Tax, accounting, and reporting obligations;
- Cybersecurity and security obligations;
- Lawful investigations;
- Fraud prevention requirements;
- Court orders or lawful directives;
- Regulatory compliance obligations.

Such processing may include disclosure of information to competent authorities where required under applicable law.

Security, Fraud Prevention & Platform Protection

We may process information where necessary to:

- Detect, investigate, prevent, or mitigate fraud, spam, abuse, unauthorized access, cybersecurity threats, or unlawful activity;
- Secure our systems, infrastructure, APIs, communications, integrations, and users;
- Protect the rights, safety, property, reputation, or legal interests of users, customers, third parties, or our organization;
- Monitor suspicious or harmful activities involving the services.

This may include automated monitoring, analytics, anomaly detection, abuse prevention systems, communication monitoring, and security logging activities.

AI, Automation & Communication Services

Where users or enterprise customers utilize AI-powered communication, workflow automation, conversational systems, customer engagement tools, or analytics functionality, we may process information as necessary to:

- Generate AI-assisted outputs;
- Facilitate automated workflows;
- Route communications;
- Perform conversational analytics;
- Provide summaries, recommendations, or insights;
- Improve operational performance;

- Enable communication automation functionality.

Such processing may involve automated or semi-automated systems, subject to applicable safeguards, customer configurations, and legal obligations.

Processing on Behalf of Enterprise Customers

Where enterprise customers use our Services to process information relating to their own customers, employees, users, leads, or prospects, we may process such information on behalf of and under instructions from the relevant enterprise customer.

In such cases:

- The enterprise customer may determine the applicable legal basis for processing;
- The enterprise customer remains responsible for ensuring lawful processing activities and obtaining required notices or consents.

International Transfers & Third-Party Providers

Certain processing activities may involve:

- Third-party infrastructure providers;
- Cloud hosting vendors;
- Communication platforms;
- AI service providers;
- Subprocessors;
- Cross-border data transfers.

Such processing may occur as necessary for:

- Providing the Services;
- Maintaining infrastructure;
- Communication routing;
- Analytics and automation;
- Operational support;
- Security and reliability.

User Choices & Rights

Subject to applicable law, users may have rights relating to:

- Withdrawal of consent;
- Access to personal information;
- Correction or deletion requests;
- Objection to certain processing activities;

- Restriction of processing;
- Communication preferences;
- Opt-out rights for marketing communications.

Certain rights may be subject to legal limitations, contractual obligations, technical feasibility, or legitimate business and security requirements.

Evolving Legal Requirements

As laws, regulations, technologies, and industry practices evolve, we may update our legal bases for processing and related disclosures from time to time.

Material changes may be reflected through updates to this Privacy Policy or related documentation where appropriate.

WHO HAS ACCESS TO YOUR DATA WITHIN OUR ORGANIZATION?

Within our organization, access to your data is limited to those who require access to provide you with the products and services you purchase from us, to contact you, and to respond to your inquiries, including refund requests. Those staff members may be on teams, such as marketing, events, development, executive, and customer support. Employees only have access to relevant data to their team on a 'need to know' basis.

WHO DO WE SHARE YOUR DATA WITH OUTSIDE OUR ORGANIZATION, AND WHY?

Processors

We may use service providers & third parties for operating and improving the sites, assisting with certain functions, such as payment processing, email transmission, conducting surveys or contests, data hosting, managing our ads, third-party solutions for marketing and analytics, and some aspects of our technical and customer support. We take measures to ensure that these service providers access, process, and store information about you only for the purposes we authorize.

Authorities

We may access, preserve, and disclose information about you to third parties, including the content of messages if we believe disclosure is in accordance with or required by applicable law, regulation, legal process, or audits. We may also disclose information about you if we believe that your actions are inconsistent with our Terms of Service or related guidelines and policies, or if necessary to protect the rights, property, or safety of, or prevent fraud or abuse of, the Company or others.

Transfer of business

If we (or our assets) are acquired, or if we go out of business, enter bankruptcy or go through some other change of control, personal information could be one of the assets transferred to or acquired by a third party.

Third-Party Communication Platforms & Integrations

Our Services may integrate with third-party communication, messaging, social media, customer relationship management (“CRM”), analytics, cloud infrastructure, and automation platforms in order to provide Omni channel communication and AI-powered workflow services.

These integrations may include, without limitation:

- WhatsApp Business Platform;
- Meta Platforms and related services;
- Instagram messaging and engagement services;
- Email communication providers;
- CRM platforms;
- Cloud telephony and SIP service providers;
- AI model and conversational processing providers;
- Customer support and ticketing platforms;
- Marketing automation systems;
- Analytics and monitoring tools.

Communication Platform Integrations

When users, customers, or authorized business clients connect third-party communication platforms with our Services, certain information, metadata, and communication content may be transmitted, processed, synchronized, stored, or analyzed through such integrations for the purpose of enabling platform functionality, automation, analytics, customer engagement, conversational workflows, and support services.

Depending on the integrations enabled by the customer, the following categories of information may be processed:

- Phone numbers;
- Email addresses;
- Usernames and social media identifiers;
- Profile information;
- Chat messages;
- WhatsApp messages;

- Instagram direct messages;
- Email communication content;
- Communication history;
- Customer support interactions;
- AI-generated responses;
- Attachments and media files;
- Communication metadata;
- Lead and customer management data;
- CRM synchronization data;
- Campaign interaction data;
- Delivery and engagement analytics.

WhatsApp & Meta Platform Processing

Where our Services integrate with WhatsApp Business APIs, Meta Platforms, Instagram APIs, or related Meta technologies, users acknowledge and agree that:

- Communications may be transmitted through Meta-controlled infrastructure;
- Meta Platforms may independently collect, process, retain, or analyze certain data in accordance with their own policies and terms;
- Use of WhatsApp, Instagram, and Meta-integrated services may also be governed by Meta's applicable terms, privacy policies, platform policies, and developer requirements;
- Message delivery, template messaging, platform approvals, and communication restrictions may be subject to Meta platform rules and regulatory requirements;
- Certain communications and metadata may be processed outside the jurisdiction of the user's location depending upon Meta infrastructure and associated sub processors.

We do not control the independent privacy, security, or operational practices of Meta Platforms or other third-party communication providers.

Users are encouraged to review:

- Meta privacy policy;
- WhatsApp business terms;
- Instagram terms of use;
- Applicable third-party platform policies.

Automated Messaging & AI-Assisted Communications

Our Services may enable:

- Automated replies;

- AI-generated communications;
- Chabot interactions;
- AI-assisted customer engagement;
- Workflow-triggered notifications;
- Automated email sequences;
- Appointment reminders;
- Lead qualification messaging;
- Conversational analytics;
- Customer support automation.

By interacting with such services, users acknowledge that some communications may be generated or assisted by artificial intelligence technologies.

Where required by applicable law, customers using our Services are responsible for obtaining all necessary consents from end users prior to sending communications through WhatsApp, email, voice calling systems, Instagram, SMS, or related communication channels.

CRM & Business System Integrations

Users may voluntarily integrate third-party CRM systems and enterprise tools with our Services. Such integrations may involve synchronization or exchange of customer records, communication history, sales pipeline data, support tickets, notes, analytics, and workflow information.

We process such information solely for:

- Enabling requested integrations;
- Providing services;
- Workflow automation;
- Analytics and reporting;
- Customer support;
- Platform security and operational purposes.

The customer remains responsible for ensuring that:

- They possess lawful rights to upload or synchronize such data;
- Required notices and consents have been obtained from relevant individuals;
- Their use of integrated systems complies with applicable laws and platform policies.

Third-Party Platform Responsibility Disclaimer

Third-party platforms integrated with our Services operate independently and may maintain separate privacy practices, security standards, retention policies, and compliance obligations.

We are not responsible for:

- Acts or omissions of third-party platforms;
- Service interruptions caused by external providers;
- Policy changes implemented by third-party platforms;
- Independent data processing conducted by such providers;
- Account restrictions or suspensions imposed by external platforms.

International Processing & Cross-Border Transfers

Certain third-party communication providers, cloud vendors, AI infrastructure providers, and integration partners may process or store information on servers located outside India or outside the user's jurisdiction.

By using our Services and enabling such integrations, users acknowledge and consent to such cross-border processing where permitted under applicable law.

We implement commercially reasonable safeguards intended to protect information transferred through such integrations.

Consent & Communication Preferences

Customers using our communication automation services are responsible for:

- Obtaining legally valid communication consent;
- Maintaining opt-in records where required;
- Honoring unsubscribe and opt-out requests;
- Complying with anti-spam and telecom regulations;
- Complying with applicable messaging platform policies.

Users may opt out of promotional communications in accordance with applicable laws and communication preferences made available through the Services.

COMMUNICATION CONSENT, AI CALLING & TELECOM COMPLIANCE

Our Services may enable businesses, enterprises, and authorized users to communicate with individuals through AI-powered voice calling systems, automated communication workflows, WhatsApp messaging, email communication, SMS, social media messaging platforms, customer engagement tools, and related communication technologies.

By interacting with our Services, websites, applications, communication channels, or AI-enabled systems, users acknowledge and understand that communications may be initiated, processed, monitored, recorded, analyzed, or automated through artificial intelligence technologies and third-party communication infrastructure.

Consent to Receive Communications

Users and recipients acknowledge and agree that communications may be sent or initiated through:

- AI-powered voice calling systems;
- Automated calling technologies;
- AI-assisted customer support systems;
- WhatsApp Business messaging;
- Instagram messaging;
- SMS and text messaging systems;
- Automated email systems;
- CRM-triggered workflows;
- Appointment reminder systems;
- Customer engagement and marketing automation platforms.

Customers and users utilizing our Services are solely responsible for obtaining all legally required consents, authorizations, notices, and permissions from end users, customers, prospects, leads, or communication recipients prior to initiating communications through the Services.

Such consent may include, where applicable:

- Consent to receive AI-generated or AI-assisted communications;
- Consent to receive marketing or promotional communications;
- Consent to receive automated calls or messages;
- Consent for call recording and monitoring;
- Consent for communication analytics and AI processing;
- Consent for communication through WhatsApp, Instagram, email, SMS, or related platforms.

AI-Generated & Automated Communications

Our Services may use artificial intelligence, machine learning, conversational automation, synthesized speech technologies, workflow automation systems, and communication analytics tools to facilitate customer interactions.

Users acknowledge that:

- Certain communications may be generated or assisted by artificial intelligence systems;
- Voice interactions may involve synthesized or AI-generated speech;
- Automated systems may respond to, classify, prioritize, route, summarize, or analyze interactions;
- Human review or intervention may occur in certain cases;
- AI-generated outputs may not always be fully accurate, complete, or error-free.

Where required by applicable law, customers using the Services should provide appropriate disclosure that communications may be AI-generated or AI-assisted.

Call Recording & Monitoring Consent

Certain communications conducted through the Services may be recorded, transcribed, monitored, summarized, analyzed, or retained for purposes including:

- Quality assurance;
- Training and operational improvement;
- Customer support;
- Dispute resolution;
- Compliance monitoring;
- Fraud prevention;
- Analytics and reporting;
- AI model performance and optimization;
- Security and lawful business purposes.

By continuing with communications through the Services, users acknowledge and consent to such recording, monitoring, transcription, and processing to the extent permitted by applicable law.

Customers utilizing the Services are responsible for:

- Providing legally required call recording disclosures;
- Obtaining necessary consents from communication recipients;
- Complying with applicable telecom, privacy, employment, and consumer protection laws.

Marketing Communications & Promotional Messaging

Our Services may be used for sending:

- Promotional communications;

- Customer engagement messages;
- Marketing campaigns;
- Lead nurturing communications;
- Sales outreach;
- Event notifications;
- Reminders and updates.

Users may opt out of promotional communications:

- By using available unsubscribe mechanisms;
- By replying with opt-out keywords where supported;
- By contacting the relevant sender or business;
- Through communication preference settings where available.

Transactional, security-related, operational, or service-critical communications may continue to be sent where legally permitted even after opting out of marketing communications.

Do Not Disturb (DND) & Anti-Spam Compliance

Customers using the Services are responsible for complying with all applicable:

- Telecom regulations;
- Anti-spam laws;
- DND/do-not-disturb requirements;
- Marketing communication rules;
- Platform communication policies;
- Consumer protection laws.

Users shall not use the Services for:

- Unlawful robocalling;
- Spam communications;
- Deceptive or misleading campaigns;
- Unauthorized marketing;
- Impersonation;
- Fraudulent communication practices;
- Contacting recipients without required consent.

We reserve the right to suspend, restrict, investigate, or terminate accounts or communication activities that:

- Violate applicable laws;
- Generate spam or abuse complaints;
- Breach telecom or platform policies;

- Create security, fraud, reputational, or legal risks.

Communication Preference Management

Users may manage communication preferences through:

- Account settings where available;
- Unsubscribe links;
- Opt-out instructions;
- Communication preference tools;
- Direct communication with the relevant business or sender.

We may maintain suppression or opt-out records to ensure compliance with communication preferences and applicable laws.

Third-Party Communication Infrastructure

Communications facilitated through the Services may rely upon third-party infrastructure providers including:

- Telecom operators;
- Cloud telephony providers;
- SIP providers;
- Meta platforms;
- WhatsApp business APIs;
- Email service providers;
- Messaging gateways;
- CRM systems;
- Communication automation platforms.

Such third-party providers may independently process certain communication-related data subject to their own policies, operational standards, and legal obligations.

Compliance with Applicable Laws

Users, enterprise customers, and businesses using the Services agree to comply with all applicable:

- Telecom laws;
- Privacy laws;
- Communication regulations;
- Consumer protection requirements;
- Anti-spam regulations;
- AI governance requirements;
- Platform policies;

- Industry-specific compliance obligations.

Nothing in this Privacy Policy shall be interpreted as legal authorization to use the Services in violation of applicable law or regulatory requirements.

ACCEPTABLE USE, LAWFUL COMMUNICATIONS & PROHIBITED ACTIVITIES

Our Services are intended solely for lawful, authorized, ethical, and legitimate business, customer engagement, communication, operational, and automation purposes.

Users, enterprise customers, businesses, administrators, and authorized personnel utilizing the Services are responsible for ensuring that all communications, workflows, campaigns, AI-generated interactions, integrations, and activities conducted through the platform comply with applicable laws, regulations, industry standards, telecom requirements, platform policies, and contractual obligations.

Lawful Use Requirement

Users may use the Services only for lawful and authorized purposes.

Users shall not use the Services:

- In violation of applicable laws or regulations;
- In a manner that infringes the rights of others;
- For deceptive, fraudulent, abusive, unethical, or misleading purposes;
- In ways that may cause harm to individuals, businesses, communication networks, platforms, or third parties.

Enterprise customers remain solely responsible for:

- The legality of communications initiated through the Services;
- Obtaining required notices and consents;
- Ensuring lawful use of AI-generated or automated communications;
- Complying with telecom, privacy, consumer protection, anti-spam, and industry-specific requirements.

Prohibited Communications & Activities

Users shall not use the Services for any unlawful, unauthorized, deceptive, harmful, abusive, or prohibited activity including, without limitation:

a. Fraudulent & Deceptive Activities

- Phishing or credential harvesting;
- Scam calls or fraudulent communications;
- Impersonation of individuals, businesses, regulators, government entities, financial institutions, or emergency services;
- Deceptive ai-generated interactions;
- Social engineering attacks;
- Misleading or false representations;
- Unlawful solicitation schemes;
- Fraudulent lead generation;
- Deceptive marketing campaigns;
- Identity theft or identity misrepresentation.

b. Unauthorized Communications

- Contacting individuals without legally required consent;
- Unlawful robocalling;
- Spam communications;
- Bulk unsolicited messaging;
- Bypassing opt-out or unsubscribe preferences;
- Violating do-not-disturb (“dnd”) requirements;
- Unauthorized promotional campaigns;
- Unlawful telemarketing activities;
- Use of purchased, scraped, or unlawfully obtained contact databases.

c. Political, Manipulative & Sensitive Use Cases

- Political robocalling campaigns where prohibited;
- Unlawful political campaigning;
- Voter manipulation activities;
- Misinformation or disinformation campaigns;
- Deceptive synthetic voice usage;
- Undisclosed ai impersonation intended to mislead recipients;
- Manipulation of vulnerable individuals;
- Harassment, intimidation, or abusive communications.

d. Financial & Debt Collection Misuse

- Unlawful debt collection activities;
- Abusive collection practices;
- Unauthorized financial solicitations;
- Deceptive lending or investment promotions;
- Unlawful recovery communications;
- Misleading financial representations.

e. Security & Platform Abuse

- Attempting to gain unauthorized access to systems or accounts;
- Bypassing platform security controls;
- API abuse or unauthorized automation;
- Distribution of malware or malicious code;
- Interference with platform operations;
- Excessive automated requests intended to disrupt services;
- Attempts to reverse engineer, exploit, probe, or compromise platform infrastructure.

f. Harmful or Illegal Content

- Unlawful, defamatory, obscene, abusive, discriminatory, extortion or threatening content;
- Communications promoting violence, exploitation, or unlawful conduct;
- Illegal products or services;
- Communications violating intellectual property or privacy rights;
- Unlawful surveillance or monitoring activities.

AI Communication Transparency

Where required by applicable law or platform policies, users and enterprise customers are responsible for ensuring that recipients are appropriately informed when:

- Communications are AI-generated;
- Voice interactions involve synthesized or artificial speech;
- Automated systems are being used;
- Communications are recorded or monitored.

Users shall not use the Services to deceptively impersonate humans, conceal automated activity where disclosure is legally required, or mislead recipients regarding the nature of communications.

Telecom, Platform & Messaging Compliance

Users utilizing communication-related functionality agree to comply with all applicable:

- Telecom regulations;
- Anti-spam requirements;
- Messaging platform rules;
- WhatsApp business policies;
- Meta platform requirements;
- Consumer protection laws;

- Marketing communication regulations;
- Call recording requirements;
- Ai governance obligations;
- Communication consent requirements.

Users are solely responsible for:

- Message content;
- Campaign targeting;
- Communication frequency;
- Recipient consent management;
- Opt-out handling;
- Regulatory compliance obligations.

Monitoring, Enforcement & Investigations

We reserve the right, but do not assume the obligation, to:

- Monitor usage of the Services;
- Investigate suspected violations;
- Review abuse complaints;
- Restrict or suspend platform access;
- Remove or disable workflows, integrations, or communications;
- Cooperate with regulators, telecom operators, law enforcement agencies, platform providers, or governmental authorities;
- Preserve logs, records, or evidence relating to suspected misuse;
- Take corrective, preventive, or enforcement measures.

Actions may be taken where we reasonably believe that usage of the Services:

- Violates applicable laws or policies;
- Creates legal, security, operational, or reputational risks;
- Harms users, customers, communication recipients, or third parties;
- Threatens the integrity, security, or reliability of the services.

Third-Party Platform Restrictions

Users acknowledge that:

- Third-party communication providers may independently enforce their own platform policies;
- Telecom operators or messaging providers may block, filter, suspend, or restrict communications;
- Meta, WhatsApp, email providers, sip providers, cloud telephony vendors, or other platforms may impose limitations, approvals, or restrictions;

- Violation of third-party policies may result in suspension or restriction of integrations or services.

We are not responsible for restrictions, suspensions, filtering decisions, or enforcement actions taken by third-party providers outside our control.

Customer Responsibility & Indemnification

Enterprise customers and users remain solely responsible for:

- Communications initiated through the Services;
- AI workflows configured by them;
- Compliance with applicable laws and regulations;
- Activities conducted using connected integrations, apis, or third-party platforms.

Users agree not to use the Services in any manner that could:

- Expose us to legal or regulatory liability;
- Damage platform reputation;
- Disrupt communication infrastructure;
- Create cybersecurity risks;
- Result in telecom or platform enforcement actions.

Suspension & Termination Rights

We reserve the right to suspend, restrict, terminate, investigate, or limit access to the Services where we reasonably determine that:

- Unlawful activity may be occurring;
- Communications violate applicable laws or policies;
- Deceptive or abusive conduct is detected;
- Telecom or platform abuse complaints arise;
- Platform integrity or security may be affected.

Such actions may be taken with or without prior notice where reasonably necessary for security, legal, operational, or compliance purposes.

INTERNATIONAL TRANSFER OF DATA

Our Services may involve the transfer, storage, processing, analysis, transmission, or access of information across multiple jurisdictions and countries through the use of global cloud infrastructure, communication networks, artificial intelligence systems, third-party integrations, subprocessors, and service providers.

By accessing or using our Services, users acknowledge and understand that their information may be processed in jurisdictions outside their state, province, or country of residence, including jurisdictions that may have data protection laws different from those applicable in their own jurisdiction.

Cross-Border Processing Activities

Information collected through our Services may be transferred to, processed by, or accessed from international locations for purposes including:

- Cloud hosting and infrastructure management;
- AI model processing and conversational analytics;
- Communication routing and delivery;
- Customer support operations;
- Security monitoring and fraud prevention;
- Platform performance optimization;
- Data backup and disaster recovery;
- Workflow automation;
- CRM synchronization;
- Email and messaging services;
- Analytics and operational reporting.

Third-Party International Service Providers

Our platform may utilize international service providers, sub processors, and technology partners including providers relating to:

- Cloud infrastructure;
- Artificial intelligence and machine learning services;
- Communication and messaging systems;
- WhatsApp business APIs;
- Meta and Instagram integrations;
- Cloud telephony and SIP services;
- CRM integrations;
- Email delivery systems;
- Analytics and monitoring tools;
- Payment processing;
- Cybersecurity and authentication services.

Such providers may operate servers, personnel, support teams, or infrastructure in multiple countries.

Cloud Hosting & Infrastructure

Depending upon platform configuration, integrations enabled, customer preferences, and operational requirements, data may be stored or processed in cloud environments and infrastructure located in multiple jurisdictions.

These jurisdictions may include, without limitation:

- India;
- United States;
- European Union member states;
- Singapore;
- Other regions where our service providers, infrastructure vendors, or sub processors maintain operations.

We may utilize globally distributed infrastructure to support:

- Platform reliability;
- Scalability;
- Communication delivery;
- AI processing;
- Redundancy;
- Backup and disaster recovery systems.

AI & Communication Infrastructure

Certain AI-powered functionalities and communication workflows may involve international processing through third-party infrastructure providers, including those offering:

- AI language models;
- Conversational processing systems;
- Speech synthesis technologies;
- Analytics platforms;
- Communication routing infrastructure;
- Cloud telephony services;
- Messaging delivery systems.

As a result, communication data, prompts, transcripts, recordings, metadata, and related information may be processed through systems located outside the user's jurisdiction.

Safeguards & Security Measures

We implement commercially reasonable technical, contractual, administrative, and organizational safeguards intended to protect information transferred across borders, including where appropriate:

- Encryption in transit and at rest;
- Access controls and authentication mechanisms;
- Role-based access restrictions;
- Confidentiality obligations;
- Vendor due diligence procedures;
- Contractual data protection obligations;
- Information security policies;
- Monitoring and logging systems;
- Secure API and infrastructure practices.

Where appropriate and commercially feasible, we seek to work with service providers that maintain recognized security and compliance standards.

Contractual & Legal Protections

Where required under applicable law, we may implement contractual protections and data processing arrangements intended to safeguard international transfers of personal information.

Such protections may include:

- Data processing agreements;
- Confidentiality obligations;
- Contractual safeguards with subprocessors;
- Platform compliance commitments;
- Information security requirements;
- Lawful processing obligations.

User Acknowledgement & Consent

By using our Services, enabling integrations, or submitting information through the platform, users acknowledge and consent to the transfer, storage, processing, and access of information across international jurisdictions where permitted by applicable law.

Users further acknowledge that:

- Certain third-party providers may independently process information under their own policies;

- Data protection laws in other jurisdictions may differ from those in the user's jurisdiction;
- Communication networks and cloud infrastructure may involve international routing or processing.

Enterprise Customer Responsibility

Enterprise customers utilizing the Services are responsible for:

- Evaluating whether international transfers are permissible under laws applicable to them;
- Obtaining any necessary notices, disclosures, or consents from their end users;
- Ensuring lawful use of cross-border communication and processing systems.

Compliance with Applicable Laws

We endeavor to process and transfer information in accordance with applicable data protection, privacy, telecom, cybersecurity, and communication laws to the extent applicable to our operations and Services.

However, users acknowledge that no method of international transmission or electronic storage can be guaranteed to be completely secure.

WHY AND FOR HOW LONG DO WE STORE THE INFORMATION WE COLLECT FROM YOU?

We retain certain information collected from you while you are a member on the site, and in certain cases where you have deleted your account, for the following reasons:

- So that you can use our sites;
- To ensure that we do not communicate with you if you have asked us not to;
- To provide you with a refund, if entitled;
- To better understand the traffic to our sites so that we can provide all members with the best possible experience;
- To detect and prevent abuse of our sites, illegal activities and breaches of our Terms of Service; and
- To comply with applicable legal, tax or accounting requirements.

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, as required by applicable law, or as permitted. When data is no longer needed, we will securely delete, anonymize, or aggregate it to prevent re-identification. We retain different categories of data for different periods of

time depending on the type of data, the category of user to whom the data relates, and the purposes for which we collected the data.

We shall delete personal data when:

- The purpose for which such data was collected is no longer being served;
- Retention is no longer required under applicable law;
- Consent has been withdrawn and no other lawful basis exists for retention;
- Retention periods prescribed under applicable agreements or laws expire.

Certain information may be retained for legal, regulatory, fraud prevention, dispute resolution, security, or compliance purposes where permitted or required under applicable law.

SECURITY

We implement and maintain commercially reasonable administrative, technical, organizational, and physical security measures designed to protect personal information, communication data, customer records, AI interaction data, and business information against unauthorized access, disclosure, misuse, alteration, destruction, loss, or accidental compromise.

Our security program is designed taking into consideration:

- The nature of the Services;
- The sensitivity of information processed;
- Operational requirements;
- Industry practices;
- Applicable legal and regulatory obligations;
- Evolving cybersecurity risks.

Security Safeguards & Technical Measures

Depending upon the Services used and system configuration, we may implement security controls including:

Encryption Controls

- Encryption of data during transmission using secure communication protocols;
- Encryption of sensitive data at rest where commercially appropriate;
- Secure API communication mechanisms;
- Encrypted communication channels between integrated systems and infrastructure.

Access Controls

- Restricted access to systems and information on a need-to-know basis;

- Role-based access control mechanisms;
- Authentication and authorization procedures;
- Privileged access management;
- Periodic review of user access rights.

Authentication & Account Security

- Password protection mechanisms;
- Multi-factor authentication (“MFA”) for administrative or privileged access where applicable;
- Session management controls;
- Login monitoring and authentication logging;
- Account verification and identity validation procedures.

Monitoring & Threat Detection

- System monitoring and operational logging;
- Audit logging of critical system activities;
- Anomaly detection and security monitoring processes;
- Fraud prevention and abuse detection mechanisms;
- Incident identification and response procedures;
- Security event tracking and analysis.

Infrastructure & Network Security

- Firewall and network security controls;
- Infrastructure segmentation where appropriate;
- Secure cloud infrastructure practices;
- Vulnerability management procedures;
- Periodic security testing and risk assessments;
- Malware and threat protection systems.

Data Protection & Storage Controls

- Controlled storage environments;
- Secure backup and recovery procedures;
- Redundancy and disaster recovery mechanisms;
- Retention and deletion controls;
- Data minimization practices where feasible.

Organizational Security Measures

- Confidentiality obligations for personnel and contractors;
- Internal information security policies and procedures;
- Employee awareness and security training programs;
- Restricted internal access to customer and communication data;
- Vendor and sub processor due diligence processes.

AI, Communication & Integration Security

Because our Services may involve:

- AI-generated communications;
- Cloud telephony systems;
- WhatsApp and Meta integrations;
- CRM synchronization;
- Email automation;
- API-based integrations;
- Conversational analytics;
- Call recordings and transcripts;

We implement commercially reasonable safeguards intended to reduce risks relating to:

- Unauthorized access;
- Misuse of communication systems;
- Data leakage;
- Spam or abusive activity;
- Platform abuse;
- Unauthorized API access;
- Fraudulent or deceptive usage.

Third-Party Infrastructure & Service Providers

Certain components of our Services may rely upon third-party service providers, cloud infrastructure vendors, communication platforms, AI providers, telecommunications providers, CRM systems, analytics vendors, and sub processors.

While we take commercially reasonable steps to evaluate and manage such providers, we do not guarantee the independent security practices, uptime, or operational controls of third-party systems outside our direct control.

Incident Response & Security Management

We maintain processes intended to identify, investigate, respond to, and mitigate security incidents and operational risks.

Where appropriate and required by applicable law, we may:

- Investigate suspected unauthorized access or misuse;
- Restrict or suspend access to affected systems;
- Notify affected parties;
- Cooperate with lawful investigations and regulatory requirements;
- Implement remediation and corrective actions.

User Responsibilities

Users and enterprise customers are responsible for:

- Maintaining the confidentiality of account credentials;
- Implementing reasonable internal security controls;
- Restricting unauthorized access to connected systems;
- Safeguarding API keys, authentication credentials, and integration tokens;
- Ensuring secure usage of integrated communication channels and third-party systems.

Users should promptly notify us of:

- Suspected unauthorized access;
- Credential compromise;
- Suspicious platform activity;
- Security vulnerabilities affecting the services.

No Absolute Security Guarantee

We implement a variety of administrative, managerial, and technical security measures to help protect your personal information. Auxify has various internal control standards which relate specifically to the handling of personal information. These include certain controls to help safeguard the information we collect online. Our employees are trained to understand and comply with these controls, and we communicate our Privacy Policy practices and guidelines to our employees. However, while we strive to protect your personal information, you must also take steps to protect your information. We urge you to take every precaution to protect your personal information while you are on the Internet.

We do not sell, rent, share, or disclose mobile phone numbers or text messaging consent information to third parties for marketing or promotional purposes.

While we strive to use commercially reasonable safeguards and industry-aligned security practices, no method of electronic transmission, cloud storage, communication infrastructure, artificial intelligence processing, or internet-based service can be guaranteed to be completely secure, uninterrupted, or immune from cybersecurity threats.

Accordingly, users acknowledge and accept that use of the Services involves inherent technology and communication security risks.

SECURITY INCIDENT, BREACH NOTIFICATION & INCIDENT RESPONSE

We maintain commercially reasonable administrative, technical, organizational, and operational processes intended to identify, assess, investigate, respond to, mitigate, and manage suspected or confirmed security incidents affecting our

Services, systems, infrastructure, integrations, communication platforms, or information processed through the platform.

This section describes our general approach relating to cybersecurity incidents, unauthorized access events, operational disruptions, and personal information security incidents.

Security Incident Monitoring & Detection

We may utilize various monitoring, logging, detection, and security management processes intended to identify:

- Unauthorized access attempts;
- Suspicious platform activity;
- Cybersecurity threats;
- Malicious communications;
- Infrastructure vulnerabilities;
- Abuse of communication systems;
- API misuse;
- Spam or fraudulent activities;
- Unauthorized disclosure or alteration of information;
- Operational disruptions affecting platform integrity or security.

Monitoring and detection activities may involve:

- Automated systems;
- Analytics tools;
- Audit logging;
- Anomaly detection mechanisms;
- Third-party security providers;
- Infrastructure monitoring systems.

Incident Investigation & Response

Where we become aware of suspected or confirmed security incidents, we may take actions including:

- Investigating the nature and scope of the incident;
- Containing or mitigating the incident;
- Restricting or suspending access to affected systems;
- Isolating affected infrastructure or integrations;
- Implementing remediation measures;
- Preserving evidence and logs where appropriate;
- Engaging security, legal, technical, or forensic personnel;
- Coordinating with relevant third-party providers or sub processors;
- Implementing corrective and preventive measures.

The specific actions taken may depend upon:

- The nature and severity of the incident;
- Systems affected;
- Legal and regulatory obligations;
- Operational considerations;
- Risks to users, customers, or third parties.

Security Incident Notifications

Where required by:

- Applicable law;
- Regulatory requirements;
- Contractual obligations;
- Enterprise agreements;
- Data processing agreements (“DPA”);

we may notify affected users, enterprise customers, regulators, authorities, or other relevant parties regarding confirmed security incidents involving personal information or customer data.

Such notifications may include, where appropriate and reasonably available:

- General description of the incident;
- Categories of information potentially affected;
- Known or reasonably suspected impact;
- Mitigation measures implemented;
- Recommended protective actions;
- Available support or contact information.

Notification timelines may vary depending upon:

- Applicable legal obligations;
- Contractual commitments;
- The nature of the incident;
- Availability of verified information;
- Operational and investigative requirements;
- Law enforcement or regulatory restrictions.

No Guarantee Against Security Incidents

While we implement commercially reasonable safeguards and security measures, users acknowledge that:

- No system, infrastructure, communication network, AI platform, cloud environment, API integration, or internet-based service can be guaranteed to be completely secure;
- Cybersecurity incidents, unauthorized access attempts, malicious attacks, human error, infrastructure failures, or third-party vulnerabilities may occur despite reasonable safeguards.

Accordingly, we do not guarantee uninterrupted or completely secure operation of the Services at all times.

Customer Responsibilities During Security Events

Enterprise customers and users are responsible for:

- Maintaining appropriate internal security controls;
- Safeguarding account credentials and api keys;
- Implementing reasonable access restrictions;
- Promptly reporting suspected security incidents or unauthorized activity;
- Cooperating with incident response activities where reasonably necessary;
- Reviewing and managing security configurations available through the Services.

Customers utilizing integrations, third-party platforms, or connected systems remain responsible for managing the security of such external environments.

Third-Party Providers & Infrastructure

Certain Services may depend upon third-party providers including:

- Cloud hosting vendors;
- Telecom and communication providers;
- AI infrastructure providers;
- CRM systems;
- Analytics vendors;
- Messaging platforms;
- Meta and WhatsApp infrastructure;
- Sub processors and integration partners.

Security incidents affecting such third-party systems may impact the Services or information processed through the platform.

While we may coordinate with such providers where appropriate, we do not control the independent security practices, operational decisions, or incident response procedures of third-party systems outside our direct control.

Regulatory Cooperation & Legal Compliance

Where required or permitted under applicable law, we may:

- Cooperate with regulators, law enforcement agencies, or governmental authorities;
- Preserve logs, records, or evidence;
- Disclose relevant information relating to security incidents;
- Implement legally required reporting or notification measures.

Incident Response Improvements

We may review and update our security measures, incident response procedures, safeguards, and operational controls following security incidents, emerging threats, technological developments, legal changes, or operational assessments.

Such updates may include:

- Enhanced monitoring controls;
- Additional security safeguards;
- Revised operational procedures;
- Updated customer guidance;
- Modifications to platform architecture or integrations.

Limitation of Liability

Nothing in this Privacy Policy shall be interpreted as creating a guarantee, warranty, or contractual commitment that security incidents, cyberattacks, unauthorized access events, or operational disruptions will never occur.

Users acknowledge that use of internet-connected services, cloud infrastructure, communication platforms, artificial intelligence systems, and third-party integrations inherently involves cybersecurity and operational risks.

DATA CONTROLLER & DATA PROCESSOR ROLES

Depending on the nature of the Services provided, the relationship with the user or customer, and the manner in which information is processed, we may act either as a “Data Controller” (or equivalent concept under applicable law) or as a “Data Processor” / “Service Provider” processing information on behalf of another entity.

The specific role undertaken by us depends upon the context in which personal information is collected, submitted, processed, stored, or otherwise handled through the Services.

When We Act as a Data Controller

We act as a Data Controller where we independently determine the purposes and means of processing personal information for our own business and operational purposes.

This may include situations where we process information relating to:

- Visitors to our website;
- Account registration and administration;
- Billing and subscription management;
- Platform authentication and security;
- Product improvement and analytics;
- Direct communication with users;
- Customer support interactions;
- Fraud prevention and abuse detection;
- Legal and regulatory compliance;
- Marketing and business development activities;
- Operational monitoring and platform management.

In such cases, we determine:

- What information is collected;
- Why the information is processed;
- How the information is processed;
- Retention periods;
- Applicable safeguards and controls.

When We Act as a Data Processor / Service Provider

We act as a Data Processor or Service Provider where enterprise customers, businesses, organizations, or other authorized users utilize our Services to upload, store, synchronize, process, analyze, communicate, or manage information relating to their own customers, employees, leads, users, prospects, vendors, or other third parties.

This may include processing activities involving:

- AI-powered voice calls;
- Customer engagement automation;
- WhatsApp communication workflows;
- Instagram messaging automation;
- CRM synchronization;
- Email communication systems;
- Support ticket processing;
- Customer service automation;
- Call recordings and transcripts;
- Conversational AI processing;

- Communication analytics;
- Workflow automation;
- Lead qualification systems.

In such situations:

- The enterprise customer or business user generally acts as the Data Controller;
- We process information on behalf of and under instructions from such customer, subject to applicable agreements and laws.

Customer Responsibilities

Enterprise customers and business users utilizing the Services are responsible for:

- Ensuring that they possess lawful authority to collect, upload, share, synchronize, or process personal information through the Services;
- Obtaining all required notices, permissions, authorizations, and consents from affected individuals;
- Complying with applicable privacy, telecom, consumer protection, employment, and communication laws;
- Ensuring lawful use of AI-powered communications and automation systems;
- Complying with applicable anti-spam and DND requirements;
- Responding to requests from individuals relating to their personal information where legally required.

Customers are solely responsible for the legality, accuracy, quality, integrity, and appropriateness of information submitted to the Services.

Processing on Customer Instructions

Where we act as a Data Processor or Service Provider, we generally process personal information:

- In accordance with customer instructions;
- As necessary to provide the services;
- For platform security and operational purposes;
- To comply with applicable law;
- To prevent fraud, abuse, or misuse of the services.

We do not independently determine the purposes for which enterprise customer data is processed except as required for:

- Operational administration;
- Security;

- Compliance;
- Legal obligations;
- Limited internal service improvement activities where permitted by applicable agreements and law.

AI & Automated Processing Activities

Our Services may utilize artificial intelligence systems, conversational automation technologies, workflow engines, analytics tools, and machine learning systems to process customer-provided data and communication interactions.

Where enterprise customers enable such features, processing may include:

- Automated communication workflows;
- AI-generated responses;
- Conversational analysis;
- Lead scoring;
- Customer interaction summaries;
- Sentiment analysis;
- Workflow recommendations;
- Communication analytics;
- Support automation.

Enterprise customers remain responsible for ensuring that use of such AI-enabled functionality complies with applicable legal and regulatory obligations.

Data Processing Agreements (DPA)

Where required by applicable law, contractual obligations, or enterprise requirements, we may enter into separate Data Processing Agreements (“DPA”) or similar contractual arrangements governing:

- Processing activities;
- Security measures;
- Confidentiality obligations;
- Sub processor usage;
- International data transfers;
- Deletion and retention requirements;
- Audit and compliance provisions.

Such agreements may supplement this Privacy Policy and govern the processing of enterprise customer data.

Third-Party Platforms & Sub processors

In providing the Services, we may utilize third-party infrastructure, sub processors, communication providers, cloud hosting vendors, AI systems, CRM integrations, messaging providers, analytics tools, telecommunications providers, and related technology partners.

Where acting as a Data Processor, we may permit such sub processors to process customer data solely as necessary for providing and supporting the Services, subject to commercially reasonable safeguards and contractual protections where appropriate.

Individual Rights Requests

Where we process personal information on behalf of enterprise customers, requests relating to:

- Access;
- Correction;
- Deletion;
- Objection;
- Restriction;
- Portability;
- Communication preferences;

may need to be directed to the relevant enterprise customer acting as the Data Controller.

Where appropriate, we may assist enterprise customers in responding to such requests in accordance with applicable law and contractual arrangements.

Compliance with Applicable Laws

We endeavor to process information in accordance with applicable privacy, cybersecurity, telecom, communication, and data protection laws relevant to our operations and Services.

Nothing in this Privacy Policy shall be interpreted as transferring legal responsibility from enterprise customers to us where such customers independently determine the purposes and means of processing personal information through the Services.

Significant Data Fiduciary Compliance

Where applicable and if designated under applicable law as a “Significant Data Fiduciary,” we may implement additional compliance measures including:

- Appointment of a Data Protection Officer;
- Independent data audits;
- Data protection impact assessments;
- Enhanced risk management measures;
- Additional compliance and reporting mechanisms required under law.

AI MODEL TRAINING, MACHINE LEARNING & SERVICE IMPROVEMENT

Our Services may utilize artificial intelligence, machine learning, conversational automation, speech processing, analytics systems, and related technologies to provide AI-powered communication, workflow automation, customer engagement, and platform functionality.

This section explains how information may be used in connection with AI systems, machine learning technologies, model optimization, analytics, and service improvement activities.

Customer Data & AI Processing

In providing the Services, we may process customer-provided information, communication data, prompts, transcripts, recordings, workflows, and interaction data through AI-enabled systems for purposes including:

- Generating responses and communications;
- Conversational automation;
- Call handling and routing;
- Support automation;
- Workflow execution;
- Summarization and transcription;
- Analytics and reporting;
- Sentiment and engagement analysis;
- Fraud prevention and abuse detection;
- Operational support;
- Service delivery and platform functionality.

Such processing may involve internally developed systems as well as third-party AI infrastructure providers and sub processors.

No Use of Customer Data for Generalized AI Model Training Without Authorization

Unless expressly authorized by the relevant customer, agreement, platform settings, or applicable terms, we do not intentionally use enterprise customer data, customer communication content, call recordings, CRM records, or confidential business information to train generalized artificial intelligence models intended for unrelated third-party usage.

This includes, where applicable:

- Customer-uploaded CRM data;
- Enterprise communication content;
- Call recordings and transcripts;
- Customer support interactions;
- WhatsApp or Instagram communications;
- Confidential business workflows;
- Proprietary enterprise information.

Limited Internal Improvement Activities

We may use certain information, metadata, usage analytics, operational logs, system interactions, feedback, error reports, and de-identified or aggregated information for limited purposes such as:

- Improving platform performance;
- Enhancing system reliability;
- Monitoring platform usage;
- Troubleshooting and debugging;
- Improving conversational workflows;
- Strengthening security and fraud prevention;
- Analytics and reporting;
- Improving automation accuracy;
- Developing and improving features and integrations.

Where commercially appropriate and reasonably feasible, we seek to minimize the use of identifiable customer content for such purposes.

De-Identified & Aggregated Information

We may create and use anonymized, aggregated, statistical, or de-identified information that does not reasonably identify individual users or customers for purposes including:

- Service analytics;
- Benchmarking;
- Operational insights;
- Platform optimization;
- Usage statistics;
- Security monitoring;
- Research and development;
- Business reporting.

Such information may be retained and used in accordance with applicable law.

Third-Party AI Providers & Infrastructure

Certain AI-powered functionalities may rely upon third-party providers offering:

- AI language models;
- Speech processing;
- Voice synthesis;
- Analytics systems;
- Automation infrastructure;
- Conversational processing technologies.

As part of providing the Services, information submitted through the platform may be processed through such third-party systems subject to:

- Applicable agreements;
- Platform configurations;
- Security safeguards;
- Operational requirements;
- Third-party policies and practices.

We endeavor to work with providers that maintain commercially reasonable security and privacy standards where feasible.

Customer Controls & Configuration

Depending on the Services and subscription plan, customers may be provided with controls or configuration options relating to:

- AI processing features;
- Retention settings;
- Integrations;
- Automation workflows;
- Analytics functionality;
- Communication storage;
- Training or optimization settings.

Enterprise customers are encouraged to review and configure such settings based on their internal compliance requirements and legal obligations.

AI Output Disclaimer

Artificial intelligence and machine learning technologies may generate outputs that are:

- Inaccurate;
- Incomplete;
- Misleading;

- Inconsistent;
- Unintended;
- Contextually incorrect.

Users and enterprise customers should independently review and validate important outputs, communications, recommendations, and decisions generated through the Services before relying upon them.

Enterprise Customer Responsibility

Enterprise customers utilizing AI-enabled functionality remain responsible for:

- Ensuring lawful use of AI systems;
- Obtaining necessary notices and consents;
- Complying with applicable privacy, telecom, employment, consumer protection, and industry-specific laws;
- Evaluating the suitability of AI-generated outputs for their intended use cases.

Future AI Features & Policy Updates

As AI technologies, regulations, and platform capabilities evolve, we may introduce new AI-enabled features, controls, safeguards, or processing practices.

We may update this Privacy Policy from time to time to reflect such operational, technological, legal, or regulatory developments.

NO PROFESSIONAL ADVICE & AI OUTPUT DISCLAIMER

Our Services may utilize artificial intelligence, machine learning systems, conversational automation technologies, workflow engines, predictive analytics, speech processing systems, and related technologies to generate communications, recommendations, summaries, insights, classifications, responses, workflows, or other outputs.

While we strive to provide reliable and useful Services, users acknowledge and agree that AI-generated or automated outputs may contain inaccuracies, errors, omissions, incomplete information, unintended responses, or contextually incorrect content.

Informational & Operational Purposes Only

Unless expressly stated otherwise in a separate written agreement, the Services and all AI-generated outputs are provided solely for:

- Informational purposes;
- Operational assistance;

- Workflow automation;
- Customer engagement support;
- Communication facilitation;
- Analytics and reporting;
- Business process assistance.

The Services are not intended to replace independent human judgment, professional expertise, or qualified advisory services.

No Legal, Financial, Medical, or Professional Advice

The Services and any AI-generated outputs, recommendations, responses, summaries, analytics, classifications, or communications should not be interpreted, relied upon, or treated as:

- Legal advice;
- Financial advice;
- Tax advice;
- Accounting advice;
- Medical advice;
- Healthcare advice;
- Insurance advice;
- Investment advice;
- Employment advice;
- Regulatory advice;
- Compliance advice;
- Professional consulting services;
- Emergency services guidance;
- Binding business decisions;
- Authoritative factual conclusions.

Users and enterprise customers should obtain advice from appropriately qualified professionals before making decisions based on AI-generated outputs or automated recommendations.

AI Limitations & Potential Inaccuracies

Artificial intelligence systems may:

- Generate incorrect or misleading responses;
- Misunderstand context or intent;
- Produce incomplete information;
- Fail to account for legal, regulatory, commercial, cultural, or factual nuances;
- Generate biased or inconsistent outputs;
- Provide outdated or unsuitable recommendations;
- Produce unintended or unexpected responses.

Accordingly:

- AI-generated outputs should be independently reviewed and validated;
- Important business, legal, financial, operational, compliance, employment, healthcare, or customer-impacting decisions should not rely solely on automated outputs;
- Human oversight and independent verification are strongly recommended.

Customer Responsibility for Use of Outputs

Enterprise customers and users utilizing the Services remain solely responsible for:

- Evaluating the accuracy and suitability of outputs;
- Reviewing AI-generated communications before use where appropriate;
- Implementing appropriate human oversight;
- Complying with applicable laws and regulations;
- Determining whether outputs are appropriate for their intended use cases;
- Monitoring customer-facing communications generated through the services.

Customers are responsible for all actions, communications, workflows, decisions, recommendations, campaigns, and business activities conducted using the Services.

Customer-Facing Communications

Where the Services are used for:

- AI voice calling;
- Sales outreach;
- Customer engagement;
- Support automation;
- Conversational AI;
- Messaging automation;
- CRM-driven workflows;
- Lead qualification;
- Customer analytics;

enterprise customers remain responsible for ensuring that communications:

- Are lawful;
- Are accurate where required;
- Comply with applicable telecom and consumer protection laws;
- Contain appropriate disclosures where necessary;
- Are reviewed for suitability based on the relevant context.

No Guarantee of Business Outcomes

We do not guarantee:

- Sales performance;
- Customer conversion rates;
- Business outcomes;
- Lead quality;
- Operational efficiency gains;
- Communication effectiveness;
- Regulatory compliance outcomes;
- Customer satisfaction results;
- Uninterrupted service availability;
- Accuracy of AI-generated outputs.

Actual outcomes may vary depending upon:

- Customer usage patterns;
- Integrations;
- Data quality;
- AI model limitations;
- Workflow configurations;
- External systems and communication infrastructure.

Third-Party Data & External Integrations

Certain outputs may rely upon:

- Third-party integrations;
- CRM data;
- Communication platform data;
- External APIs;
- Third-party AI systems;
- Customer-provided information.

We do not independently verify all such information and are not responsible for inaccuracies originating from external systems or customer-provided data.

Limitation of Reliance

Users and enterprise customers acknowledge that:

- AI-generated outputs are probabilistic in nature;
- Outputs may vary over time;
- Automated recommendations should not be solely relied upon for material decisions;

- Professional review may be necessary depending on the context and intended use.

Use of the Services and reliance upon AI-generated outputs is at the user's and customer's own discretion and risk.

Evolving AI Technologies

Artificial intelligence technologies continue to evolve rapidly, and the capabilities, limitations, risks, and reliability of AI systems may change over time.

We may modify, improve, restrict, suspend, or update AI-powered features, outputs, safeguards, workflows, or functionality from time to time in accordance with operational, technological, legal, or regulatory requirements.

AUTOMATED DECISION-MAKING, AI ANALYTICS & PROFILING

Our Services may utilize artificial intelligence, machine learning systems, automation technologies, conversational analytics, predictive systems, workflow engines, and data-driven processing tools to facilitate automated or semi-automated operational decisions, communication workflows, customer engagement activities, and business process optimization.

Depending on the Services used, integrations enabled, and customer configurations, certain processing activities may involve automated analysis, classification, prioritization, recommendations, routing, scoring, or profiling of interactions, communications, users, leads, customers, or business workflows.

Automated Processing Activities

Our platform may perform automated or AI-assisted processing activities including, without limitation:

- Lead qualification and categorization;
- Customer prioritization;
- Ticket routing and assignment;
- Communication sequencing and workflow automation;
- AI-generated recommendations;
- Conversational intent analysis;
- Sentiment analysis;
- Customer engagement scoring;
- Sales opportunity scoring;
- Communication summarization;
- Support classification;
- Spam, fraud, or abuse detection;
- Automated follow-up workflows;
- Escalation recommendations;

- Predictive engagement analytics;
- Workflow triggering and orchestration;
- Behavioral pattern analysis;
- Customer interaction analytics;
- Campaign optimization;
- Response prioritization.

AI-Generated Insights & Recommendations

Our Services may generate automated insights, recommendations, predictions, classifications, summaries, or analytics based on:

- Communication history;
- Customer interactions;
- CRM information;
- Behavioral data;
- Conversational inputs;
- Engagement metrics;
- Workflow activity;
- System interactions.

Such outputs may be used to:

- Assist customer support teams;
- Optimize communication workflows;
- Prioritize leads or tickets;
- Automate engagement processes;
- Improve operational efficiency;
- Enhance analytics and reporting;
- Support decision-making processes.

No Guarantee of Accuracy

Artificial intelligence systems and automated analytics tools may produce outputs that are:

- Incomplete;
- Inaccurate;
- Inconsistent;
- Biased;
- Contextually incorrect;
- Unintended;
- Unsuitable for specific decisions.

Accordingly:

- Automated outputs should not be treated as guaranteed factual conclusions;
- Users should independently evaluate important recommendations or decisions;
- Enterprise customers remain responsible for reviewing and validating critical outcomes generated through the services.

Human Review & Oversight

Depending on platform configuration, certain automated workflows may involve:

- Human review;
- Manual approval processes;
- Escalation to support personnel;
- Override capabilities;
- Administrative supervision.

However, some workflows may operate automatically without continuous human intervention based on customer-defined settings, triggers, or automation rules.

Enterprise customers are responsible for configuring workflows appropriately based on their operational, legal, and compliance requirements.

Profiling & Behavioral Analysis

Our Services may analyze interactions, engagement patterns, communication behaviors, workflow activity, and usage trends in order to:

- Personalize communications;
- Optimize workflows;
- Improve automation systems;
- Generate analytics;
- Improve service delivery;
- Detect abuse or fraud;
- Enhance customer engagement strategies.

Such profiling activities may be conducted using automated tools, machine learning systems, or AI-enabled analytics technologies.

Enterprise Customer Responsibility

Enterprise customers utilizing automated decision-making or AI-enabled workflow functionality remain responsible for:

- Evaluating the suitability of such systems for their intended use cases;

- Ensuring lawful use of profiling and automation technologies;
- Obtaining necessary notices and consents where required;
- Implementing appropriate human oversight where legally or operationally necessary;
- Complying with applicable privacy, telecom, employment, consumer protection, and sector-specific laws.

Customers should independently assess whether automated outputs are appropriate for making business, operational, employment, financial, compliance, or customer-impacting decisions.

Communications & AI-Based Prioritization

Communications facilitated through the Services may be:

- Automatically prioritized;
- Categorized;
- Scheduled;
- Routed;
- Escalated;
- Filtered;
- Analyzed;
- Summarized;
- Scored;

based on AI models, automation logic, workflow rules, customer-defined configurations, or system-generated analytics.

This may affect:

- Response timing;
- Lead handling;
- Support escalation;
- Communication routing;
- Workflow sequencing;
- Customer engagement processes.

User Rights & Requests

Where required under applicable law, users may have rights relating to:

- Access to their personal information;
- Correction of inaccurate information;
- Objection to certain processing activities;
- Restriction of certain automated processing activities.

Certain requests may need to be directed to the relevant enterprise customer or business utilizing the Services where such customer acts as the primary Data Controller.

Evolving AI Technologies

As artificial intelligence technologies, automation systems, legal requirements, and platform capabilities evolve, we may update our automated processing practices, safeguards, controls, and disclosures from time to time.

Any material updates will be reflected through updates to this Privacy Policy or related documentation where appropriate.

YOUR RIGHTS

You have certain rights this includes

- **Right to access.** This right allows you to obtain a copy of your personal data, as well as other supplementary information.
- **Right to restrict processing.** You have the right to restrict the processing of your personal data in certain circumstances.
- **Right to rectification.** You have the right to have any incomplete or inaccurate information we hold about you corrected.
- **Right to object to processing.** The right to object allows you to stop or prevent us from processing your personal data. This right exists where we are relying on a legitimate interest as the legal basis for processing your personal Data. You also have the right to object where we are processing your personal data for direct marketing purposes.
- **Right to erasure.** You have the right to ask us to delete or remove personal data when the personal data is no longer necessary for the purpose which you originally collected or processed.
- **Right to opt out.** You have the right to choose (opt out) of having your personal information be (i) disclosed to a third party or (ii) used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized.
- **Right to Nominate.** Subject to applicable law, individuals may nominate another person to exercise rights relating to their personal data in the event of death or incapacity, in accordance with procedures prescribed under applicable law.
- Additionally, for sensitive personal data (such as data related to health, biometric identifiers, or racial/ethnic origin), we will obtain your affirmative consent (opt-in) before processing or sharing it

Subject to applicable law, individuals may also have the following rights:

- Right to access information regarding processing of personal data;
- Right to correction and erasure of personal data;

- Right to withdraw consent;
- Right to grievance redressal;
- Right to nominate another individual in case of death or incapacity;
- Right to request summaries of personal data being processed, where applicable.

Certain rights may be subject to legal limitations, security requirements, technical feasibility, and lawful exemptions.

To exercise your rights, you can contact us at support@getit.express

DATA DELETION, RETENTION & ACCOUNT TERMINATION

We retain personal information, communication data, AI interaction data, customer records, operational logs, and related information only for as long as reasonably necessary to fulfill the purposes described in this Privacy Policy, comply with applicable legal and regulatory obligations, maintain platform security and integrity, resolve disputes, enforce agreements, and support legitimate business and operational requirements.

This section describes how information may be retained, deleted, anonymized, or managed following account closure, deletion requests, termination of Services, or expiration of applicable retention periods.

User & Customer Deletion Requests

Subject to applicable law, contractual obligations, operational requirements, and legitimate business interests, users and enterprise customers may request:

- Deletion of personal information;
- Deletion of account information;
- Removal of communication records;
- Deletion of call recordings or transcripts;
- Deletion of AI interaction data;
- Deletion of CRM synchronization data;
- Deletion of integrations or connected platform data.

Requests may be submitted through:

- account settings where available;
- customer support channels;
- enterprise account representatives;
- designated privacy or grievance contact channels.

We may require reasonable verification of identity or authorization before processing deletion requests.

Processing of Deletion Requests

Upon receipt of a valid deletion request, we may:

- Delete applicable information;
- Anonymize or de-identify information;
- Restrict further processing;
- Remove access to certain data;
- Disconnect integrations;
- Schedule deletion through operational workflows and backup cycles.

Deletion may not always occur immediately and may require reasonable processing time depending on:

- System architecture;
- Backup schedules;
- Platform dependencies;
- Legal obligations;
- Enterprise customer instructions;
- Technical feasibility;
- Security and fraud prevention requirements.

Backup & Archived Information

Certain information may continue to exist temporarily in:

- Encrypted backups;
- Disaster recovery systems;
- Audit logs;
- System archives;
- Security monitoring systems;
- Redundancy storage environments.

Such retained information is generally:

- Restricted from active operational use;
- Protected through applicable safeguards;
- Retained only for limited operational, security, compliance, or recovery purposes.

Backup or archived information may be deleted, overwritten, anonymized, or isolated in accordance with internal retention schedules and operational procedures.

Legal, Regulatory & Compliance Retention Obligations

Notwithstanding deletion requests or account closure, we may retain certain information where necessary to:

- Comply with applicable laws and regulations;
- Satisfy tax or accounting obligations;
- Maintain legally required business records;
- Comply with telecom or communication regulations;
- Resolve disputes;
- Investigate fraud, abuse, or security incidents;
- Enforce contractual rights;
- Comply with lawful requests from authorities;
- Maintain suppression or opt-out records;
- Protect platform integrity and security.

Such retained information will generally be limited to what is reasonably necessary for the applicable purpose.

Enterprise Customer-Controlled Data

Where enterprise customers use our Services to process information relating to their own customers, employees, leads, prospects, or users:

- The enterprise customer may control applicable retention settings and deletion instructions;
- We may process deletion requests in accordance with contractual obligations and customer instructions;
- Certain deletion requests may need to be directed to the relevant enterprise customer acting as the primary data controller.

Enterprise customers remain responsible for:

- Defining appropriate retention periods;
- Ensuring lawful deletion practices;
- Complying with applicable legal and regulatory obligations relating to retained records.

Account Termination & Service Suspension

If accounts are:

- Closed;
- Suspended;
- Terminated;
- Abandoned;
- Inactive for extended periods;

we may:

- Deactivate account access;
- Restrict platform functionality;
- Archive certain information;
- Delete information in accordance with applicable retention policies;
- Retain limited information for security, compliance, fraud prevention, dispute resolution, or operational continuity purposes.

Termination of Services does not automatically require immediate deletion of all associated information.

Communication Records & AI Interaction Data

Depending on the Services used, certain communication-related information may be retained for limited periods for purposes including:

- Quality assurance;
- Communication history;
- Fraud prevention;
- Troubleshooting;
- Analytics and reporting;
- Customer support;
- Compliance and audit requirements;
- AI workflow continuity;
- Operational recovery.

Such information may include:

- Call recordings;
- Transcripts;
- AI-generated summaries;
- Support interactions;
- Workflow logs;
- Messaging history;
- CRM activity records;
- Authentication and audit logs.

Anonymized & Aggregated Information

We may retain anonymized, aggregated, statistical, or de-identified information that does not reasonably identify individuals for purposes including:

- Analytics;
- Service improvement;
- Benchmarking;
- Security monitoring;

- Research and development;
- Operational reporting.

Such information may continue to be used after deletion of identifiable data where permitted under applicable law.

Deletion Limitations

In certain circumstances, deletion, restriction, or removal of information may be limited or delayed due to:

- Technical constraints;
- Security considerations;
- Legal obligations;
- Dispute resolution requirements;
- Fraud prevention;
- Backup retention cycles;
- Operational dependencies;
- Contractual obligations;
- Lawful requests from authorities.

Where appropriate, we may instead restrict processing or isolate information from active use.

Data Portability & Export

Where technically feasible and legally required, users or enterprise customers may request export or retrieval of certain information prior to deletion or account termination, subject to:

- Verification procedures;
- Contractual limitations;
- Operational feasibility;
- Security safeguards.

Retention Policy Updates

Retention periods, deletion procedures, backup practices, and operational requirements may evolve over time based on:

- Technological developments;
- Legal requirements;
- Regulatory obligations;
- Security considerations;
- Platform functionality;
- Operational needs.

We may update this Privacy Policy and related retention practices from time to time to reflect such changes.

OUR POLICY CONCERNING CHILDREN & THEIR DATA

Our Sites are not directed to children under the age of Eighteen, and we do not knowingly collect personally identifiable information from children or distribute such information to third parties. We screen users who wish to provide personal information in order to prevent children from providing such information. If we become aware that we have inadvertently received personally identifiable information from a child, we will delete such information from our records. If we change our practices in the future, we will obtain prior, verifiable parental consent before collecting any personally identifiable information from children.

LINKS TO OTHER WEBSITES

Our sites may contain links to other websites that are not operated by us. If you click on a third-party link, you will be directed to that third-party's site. We strongly advise you to review the Privacy Policy of every site you visit.

Third parties are under no obligation to comply with this Privacy Policy with respect to personal data that you provide directly to those third parties or that those third parties collect for themselves. We do not control the third-party sites that may be accessible through our services. Thus, this Privacy Policy does not apply to information you provide to third-party sites or gathered by the third parties that operate them.

CHANGES TO THIS POLICY

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page. If we make any material change/s to the Policy, we will notify you via email, through a notification posted on the Services, or as required by applicable law. You can see when the Policy was last updated by checking the date at the bottom of this page. You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective from when they are posted on this page.

GRIEVANCE REDRESSAL OFFICER

In accordance with applicable Indian data protection laws, users may contact our designated Grievance Officer regarding:

- Questions relating to personal data processing;
- Exercise of data protection rights;
- Withdrawal of consent;
- Complaints relating to privacy practices;

- Requests relating to correction or deletion of personal data.

Grievance Officer Details:

Name: Pratik Jatale

Email: pratik@getit.express

Address: Indore

We shall endeavor to respond to grievances within timelines prescribed under applicable law.

Escalation Rights

If an individual is dissatisfied with the resolution provided by the Grievance Officer, such individual may have the right to lodge a complaint with the Data Protection Board of India or other competent authority in accordance with applicable law.

CONTACT US

If you have any questions about this Privacy Policy, you can contact us at support@getit.express

Last Updated: 13th May 2026

Name of DPO - Mr. Pratik Jatale

Contact - pratik@getit.express