

Terms and Policies

Generated on 03 Oct 2026

SARKARI HUMSAFAR

VOLUME I – TERMS OF USE

CHAPTER 1 – PRELIMINARY PROVISIONS

1. TITLE

1.1 Title of the Agreement

These Terms and Conditions shall be known as the "Terms of Use of SarkariHumsafar.com" (hereinafter referred to as the "Terms", "Terms of Use", "User Agreement", or "Agreement").

These Terms constitute a legally valid and binding electronic contract executed between Ramisht Kripa

Private Limited, a company incorporated under the provisions of the Companies Act, 2013, having its registered office at Flat No. 9188, 1st Floor, LIG Flat,B-9 Vasant Kunj New Delhi-110070 (hereinafter referred to as the "Company",

"SarkariHumsafar", "Platform", "Website", "we", "our", or "us"), and every individual or legal entity accessing or using the Platform (hereinafter referred to as the "User", "Member", "Subscriber",

"Customer", "you", or "your").

This Agreement governs the access to and use of:

- www.sarkarihumsafar.com;
- all associated mobile applications;
- Progressive Web Applications (PWA);
- APIs;
- software applications;
- communication portals;
- customer support services;
- premium membership services;
- verification services;
- AI-powered recommendation services;
- offline assistance services;

- advertisements;
- social media pages operated by the Company; and
- every other service presently offered or introduced in the future by the Company.

These Terms shall be read together with and form an integral part of the following documents, each of which is incorporated herein by reference:

- (a) Privacy Policy;
- (b) Cookie Policy;
- (c) Refund, Cancellation & Subscription Policy;
- (d) Website Disclaimer;
- (e) Community Guidelines and Safety Policy;
- (f) Intellectual Property Policy;
- (g) Grievance Redressal Policy;
- (h) Child Safety Standards Policy;
- (i) Law Enforcement & Regulatory Compliance Policy; and
- (j) every guideline, policy, notice, circular or instruction published by the Company from time to time.

In the event of any inconsistency between these Terms and any supplementary policy, the specific policy governing the relevant subject matter shall prevail to the extent of such inconsistency unless expressly stated otherwise.

2. EFFECTIVE DATE

2.1 Effective Date : 14/9/2026

These Terms shall become effective from [14/9/2026] and shall remain in force unless modified, superseded, or terminated by the Company in accordance with these Terms.

The latest version of these Terms shall always be available on the Platform, and Users are encouraged to review them periodically.

2.2 Binding Nature

These Terms constitute a legally enforceable electronic agreement between the Company and every User who accesses or uses the Platform. No physical signature shall be required for the validity or enforceability of these Terms. Acceptance of these Terms through electronic means shall have the same legal force and effect as execution of a written agreement.

2.3 Commencement of Contractual Relationship

The contractual relationship between the Company and the User shall commence immediately upon the occurrence of any one or more of the following events:

- a) visiting the Website;
- b) accessing any webpage of the Platform;
- c) creating a user account;
- d) clicking "I Agree", "Accept", "Continue", "Register", "Subscribe", or any similar electronic acceptance button;
- e) verifying a mobile number or email address;
- f) uploading any information or documents;
- g) purchasing any paid subscription;
- h) using any free or premium feature;
- i) communicating with another Member through the Platform; or j) otherwise accessing or using any Service offered by the Company.

Such conduct shall constitute unconditional acceptance of these Terms.

2.4 Duration

These Terms shall continue to apply throughout the period during which the User accesses or uses the

Platform and shall survive termination to the extent necessary for the enforcement of rights and obligations relating to: payments; refunds; intellectual property; confidentiality; privacy; dispute resolution; arbitration; limitation of liability; indemnification; fraud investigations; electronic evidence; regulatory compliance; and any other provisions intended by their nature to survive termination.

3. SCOPE AND APPLICABILITY

3.1 General Scope

These Terms govern every aspect of the relationship between the Company and the User arising out of the access to or use of the Platform. The User acknowledges that these Terms apply irrespective of whether the Services are provided free of charge or upon payment of subscription fees.

3.2 Persons Covered

These Terms shall apply to every:

visitor; registered member; subscriber; premium member; applicant; customer; advertiser; business partner; affiliate; vendor; consultant; service provider; API user; authorised representative; organisation; company; governmental body; and every other person who accesses or interacts with the Platform in any manner whatsoever.

3.3 Services Covered

These Terms govern, without limitation:

(a) account registration; (b) profile creation; (c) profile verification; (d) profile browsing; (e) search functionality; (f) AI-powered matchmaking recommendations; (g) compatibility tools; (h) communication facilities; (i) messaging services; (j) premium subscriptions; (k) verification services; (l) customer support; (m) advertisements; (n) promotional campaigns; (o) referral programmes; (p) loyalty programmes; (q) rewards; (r) profile boosting; (s) featured listings; (t) payment processing; (u) grievance mechanisms; (v) security services; (w) fraud detection systems; (x) data analytics; (y) automated decision-making systems; and (z) every other existing or future service introduced by the Company.

3.4 Territorial Applicability

The Platform is primarily intended for use within the Republic of India.

However, Users located outside India may access the Platform subject to:

- applicable Indian laws;
- laws of their country of residence;
- international sanctions;
- export control regulations; and
- any other applicable legal requirements.

The User alone shall be responsible for ensuring that the use of the Platform is lawful in the jurisdiction from which access is made.

3.5 Nature of the Platform

The User expressly acknowledges that:

- a) SarkariHumsafar.com is a technology-enabled online matrimonial platform;
- b) the Platform merely facilitates interaction between Users;
- c) the Company is not a marriage bureau, marriage broker, relationship counsellor, recruiter, employment agency, immigration consultant, legal advisor, or financial advisor;
- d) the Company does not solemnise marriages;
- e) the Company does not arrange marriages;
- f) the Company does not guarantee matrimonial alliances;
- g) the Company does not guarantee compatibility;
- h) the Company does not verify every profile or every statement made by Users unless expressly represented under a specific verification service.

3.6 Independent Decision-Making

Every User acknowledges and agrees that:

- a) all matrimonial decisions shall be taken solely by the User;
- b) Users must independently verify the identity, educational qualifications, employment, marital status, family background, financial condition, health condition, criminal antecedents, and all other material particulars of another User before taking any matrimonial or financial decision;
- c) no representation made on the Platform shall be treated as professional advice or a recommendation by the Company;
- d) the Platform merely provides technological infrastructure and shall not be responsible for personal decisions taken by Users.

3.7 Excluded Activities

Nothing contained on the Platform shall be construed as:

legal advice; financial advice; investment advice; immigration advice; employment placement; counselling services; psychological assessment; medical advice; verification certification; background investigation; guarantee of marriage; or guarantee of compatibility.

3.8 Future Services

The Company reserves the unrestricted right to introduce, discontinue, suspend, modify, merge, split, replace, or withdraw any feature, functionality, technology, software, subscription plan, verification mechanism, AI system, payment model, advertisement programme, or business model at any time without prior notice, unless otherwise required under applicable law.

3.9 Third-Party Services

Certain features of the Platform may utilise services provided by independent third parties, including but not limited to:

- payment gateways;
- cloud service providers;
- SMS gateway providers;
- email service providers;
- identity verification agencies;
- analytics providers;
- cybersecurity vendors;
- communication platforms;
- AI service providers; and
- government-authorised verification agencies.

The Company shall exercise reasonable care in selecting such service providers but shall not be

responsible for their independent acts, omissions, service interruptions, or failures, except to the extent mandated by applicable law.

3.10 Reservation of Rights

The Company expressly reserves all rights not specifically granted to Users under these Terms. Nothing contained herein shall be interpreted as granting any ownership right, licence, proprietary interest, intellectual property right, or commercial exploitation right in favour of any User except the limited, revocable, non-exclusive, non-transferable right to access and use the Platform strictly in accordance with these Terms.

The Company further reserves the right to refuse access to the Platform, suspend or terminate Accounts, restrict access to specific Services, investigate suspected misuse, cooperate with law enforcement agencies, preserve electronic records, and take such legal or technical measures as may be necessary to protect the integrity, security, reputation, and lawful operation of the Platform.

PART II – GENERAL & CORPORATE DEFINITIONS

4. DEFINITIONS

For the purposes of these Terms, unless the context otherwise requires, the following words and expressions shall have the meanings assigned to them below. Words used in the singular shall include the plural and vice versa, and words importing one gender shall include every gender.

4.1 "Account"

"Account" means the unique electronic account created by a User upon successful registration on the

Platform, enabling such User to access, use, manage, subscribe to, or otherwise avail the Services offered by the Company, including any associated profile, login credentials, communication history, subscription details, preferences, and account settings.

An Account shall remain the exclusive responsibility of the User in whose name it is registered.

4.2 "Affiliate"

"Affiliate" means any individual, company, corporation, partnership, limited liability partnership, trust, joint venture, subsidiary, holding company, associate company, successor, assign, parent entity, or any other legal entity which directly or indirectly:

- controls the Company;
- is controlled by the Company; or
- is under common control with the Company, whether presently existing or incorporated in the future.

For the purpose of this definition, the expression "control" shall include direct or indirect ownership, management control, voting rights, contractual control, or the ability to direct management or policies of an entity.

4.3 "Agreement"

"Agreement" means these Terms of Use together with every policy, guideline, schedule, annexure, notice, disclaimer, supplementary terms, subscription conditions, community standards, privacy notice, cookie policy, refund policy, intellectual property policy, grievance policy, child safety policy, law enforcement policy, amendments, modifications, and all other legal documents published by the Company from time to time, all of which collectively constitute one integrated and legally binding electronic contract between the Company and the User.

4.4 "Applicable Law"

"Applicable Law" means all laws, statutes, ordinances, regulations, notifications, circulars, directions, governmental orders, judicial precedents, administrative instructions, guidelines, rules, subordinate legislation, industry standards, codes of practice, regulatory requirements, licences, permits, governmental approvals, and all amendments or replacements thereof that are applicable to the

Company, the Platform, or the User, including, without limitation:

- the Information Technology Act, 2000;
- the Digital Personal Data Protection Act, 2023;
- the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021;
- the Consumer Protection Act, 2019;
- the Bharatiya Nyaya Sanhita, 2023;
- the Bharatiya Nagarik Suraksha Sanhita, 2023;
- the Bharatiya Sakshya Adhinyam, 2023;
- the Arbitration and Conciliation Act, 1996;
- the Companies Act, 2013;
- applicable tax laws;
- CERT-In Directions;
- RBI directions applicable to digital payments; and
- any other law or regulation having legal force in India.

4.5 "Artificial Intelligence" or "AI"

"Artificial Intelligence" or "AI" means any software system, machine learning model, neural

network, recommendation engine, predictive analytics model, large language model (LLM), natural language processing system, automated decision-making system, ranking algorithm, behavioural analytics tool, fraud detection engine, computer vision system, generative AI model, chatbot, or any similar computational technology used by or on behalf of the Company for providing, enhancing, securing, moderating, analysing, personalising, or improving the Services.

4.6 "Business Day"

"Business Day" means any day other than:

- Saturday;
- Sunday; or
- a day declared as a public holiday by the Central Government or the Government of the National Capital Territory of Delhi.

4.7 "Company"

"Company", "We", "Us", "Our", "Platform Owner", or "SarkariHumsafar" means Ramisht Kripa Private Limited, a company incorporated under the Companies Act, 2013, together with its: Directors; shareholders; promoters; officers; employees; consultants; agents; representatives; affiliates; subsidiaries; successors; assigns; licensors; contractors; service providers; and authorised representatives, unless the context otherwise requires.

Where the context permits, references to the Company shall include every person acting on its lawful behalf.

4.8 "Corporate User"

"Corporate User" means any company, body corporate, partnership firm, LLP, government organisation, recruitment agency, marriage bureau, advertising agency, institution, NGO, trust, society, association, or any other legal entity using the Platform for any lawful commercial, administrative, advertising, promotional, recruitment, verification, partnership, or business purpose authorised by the Company.

4.9 "Government Authority"

"Government Authority" includes:

Central Government; State Governments; Union Territory Administrations; Courts; Tribunals; Regulatory Authorities; Law Enforcement Agencies; Police Authorities; CERT-In; RBI; Income Tax Authorities; Consumer Commissions; Statutory Bodies; Municipal Authorities; Government Departments; Ministries; Public Sector Undertakings; and every authority exercising executive, judicial, quasi-judicial, legislative, investigative, regulatory, or administrative powers under

Applicable Law.

4.10 "Law Enforcement Agency"

"Law Enforcement Agency" includes any police authority, investigating agency, cybercrime cell, intelligence agency, court, tribunal, prosecutor, governmental authority, statutory authority, regulatory authority, or any other agency empowered under Applicable Law to investigate, prosecute, regulate, or enforce legal rights and obligations.

4.11 "Member"

"Member" means a User who has successfully completed registration on the Platform and whose Account has been activated or otherwise permitted by the Company for accessing one or more Services.

The term includes:

-
- Free Members;
-
- Premium Members;
-
- Verified Members;
-
- Trial Members;
-
- Corporate Members; and
- every category of registered user introduced by the Company from time to time.

4.12 "Person"

"Person" includes:

a natural person; Hindu Undivided Family; sole proprietorship; partnership; LLP; company; corporation; society; trust; association of persons; governmental authority; statutory authority; foreign entity; joint venture; cooperative society; or every other juridical person recognised under Applicable

Law.

4.13 "Platform"

"Platform" means:

SarkariHumsafar.com; every associated domain; sub-domain; microsite; mobile application; software application; progressive web application (PWA); API; digital portal; communication

platform; customer dashboard; chatbot; AI interface; verification portal; payment portal; admin dashboard; social media page operated by the Company; and every digital service operated or controlled by the Company now existing or developed in the future.

4.14 "Registered User"

"Registered User" means any User who has successfully created an Account by providing the information required by the Platform, irrespective of whether such User has subscribed to any paid Services.

4.15 "Services"

"Services" means every service, facility, feature, function, technology, software, tool, subscription, advertisement, verification service, customer support service, AI-powered recommendation, profile hosting, profile promotion, search functionality, communication system, payment facility, security mechanism, fraud detection service, analytics tool, or any other service offered by the Company through the Platform from time to time.

4.16 "Subscriber"

"Subscriber" means any User who has purchased, renewed, upgraded, or otherwise subscribed to any paid membership, premium plan, value-added service, or recurring subscription offered by the Company.

4.17 "User"

"User" means every individual or legal entity who visits; browses; accesses; registers; logs into; communicates through; uploads information to; subscribes to; purchases services from; or otherwise interacts with the Platform in any manner whatsoever, whether or not such person creates an Account.

Unless the context otherwise requires, the expressions "User," "Member," "Subscriber," "Visitor," and

"You" shall include every person using the Platform.

4.18 "Visitor"

"Visitor" means any person accessing or browsing the Platform without creating an Account or purchasing any Service.

4.19 "Writing" or "Written"

"Writing" or "Written" includes physical documents as well as electronic records, emails, electronic communications, digital signatures, click-wrap agreements, OTP-based confirmations, electronic acknowledgements, scanned documents, and every other form of communication

recognised under

Applicable Law.

4.20 "Website"

"Website" means the official online platform accessible through www.sarkarihumssafar.com, together with all associated webpages, subdomains, mobile interfaces, APIs, and any successor domain names owned or operated by the Company.

VOLUME I – TERMS OF USE

CHAPTER 1 – PRELIMINARY PROVISIONS

PART III – PLATFORM & SERVICE DEFINITIONS

Unless the context otherwise requires, the following terms shall have the meanings assigned to them below and shall apply throughout these Terms and all related policies published by the Company.

4.21 "Account"

"Account" means the unique electronic account created by or on behalf of a User upon successful registration on the Platform for accessing the Services. An Account includes, without limitation:

- (a) login credentials;
- (b) user identification number;
- (c) registered mobile number;
- (d) registered email address;
- (e) Profile information;
- (f) subscription history;
- (g) communication history;
- (h) payment records;
- (i) verification status;
- (j) user preferences;
- (k) security settings;
- (l) activity logs; and
- (m) all information associated with such account.

An Account is personal, non-transferable, revocable, and may only be used by the registered User unless expressly authorised in writing by the Company.

4.22 "Profile"

"Profile" means the electronic matrimonial profile created by a User containing personal, matrimonial, educational, professional, social, cultural, religious, lifestyle, family, and other information voluntarily uploaded or submitted to the Platform.

A Profile may include, without limitation name; age; gender; marital status; religion; caste; community; profession; occupation; employer; income; educational qualifications; residential address; photographs; videos; government identification details (where voluntarily submitted); interests; partner preferences; horoscope details; biometric information (where applicable); verification badges; AI- generated compatibility indicators; profile completion score; and any other information permitted by the Platform.

The Company reserves the right to modify the format, structure, fields, or display of Profiles from time to time.

4.23 "Verified Profile"

"Verified Profile" means a Profile that has undergone one or more verification processes offered by the

Company, such as:

- mobile verification;
- email verification;
- identity verification;
- photograph verification;
- educational verification;
- employment verification;
- address verification;
- marital status verification; or
- any other verification service.

Verification indicates only that a specified verification process has been completed and does not constitute a guarantee, warranty, endorsement, or certification of the accuracy, authenticity, completeness, suitability, character, or continued validity of the information contained in the Profile.

4.24 "Services"

"Services" means every facility, feature, functionality, product, software, technology, tool, digital interface, customer support mechanism, communication system, subscription offering,

verification service, artificial intelligence service, security feature, advertisement service, analytics service, or other service made available by the Company through the Platform, whether presently existing or introduced in the future.

Services include, without limitation:

- (a) Profile creation;
- (b) Profile hosting;
- (c) Profile editing;
- (d) Search functionality;
- (e) Match recommendations;
- (f) AI-powered compatibility suggestions;
- (g) Messaging services;
- (h) Voice and video communication (where available);
- (i) Verification services;
- (j) Premium memberships;
- (k) Profile boosting;
- (l) Featured listings;
- (m) Customer support;
- (n) Complaint handling;
- (o) Safety tools;
- (p) Fraud prevention systems;
- (q) Digital payment facilities;
- (r) Notifications;
- (s) Mobile applications;
- (t) APIs;
- (u) Offline assistance; and
- (v) all ancillary or supplementary services.

4.25 "Premium Services"

"Premium Services" means any paid service, subscription, feature, or value-added offering made available by the Company in consideration of payment of prescribed fees.

Premium Services may include Premium Memberships; Featured Profiles; Express Interest Credits;

Unlimited Messaging; Contact Viewing; Profile Boosting; Priority Listing; Background Verification Services; Assisted Matchmaking; Dedicated Relationship Manager Services; AI Premium

Matching;

Consultation Services; Promotional Packages; and any future premium services introduced by the Company.

The scope of Premium Services may vary depending upon the subscription plan selected by the User.

4.26 "Subscription"

"Subscription" means a paid contractual arrangement under which a User obtains access to Premium

Services for a specified duration subject to payment of applicable fees and compliance with these Terms.

Subscriptions may include:

- monthly plans;
- quarterly plans;
- half-yearly plans;
- annual plans;
- lifetime plans (if introduced);
- promotional subscriptions;
- complimentary subscriptions;
- enterprise subscriptions; and
- any customised subscription approved by the Company.

4.27 "Subscription Fees"

"Subscription Fees" means the consideration payable by the User for availing Premium Services, inclusive or exclusive of applicable taxes, convenience fees, payment gateway charges, renewal charges, or other statutory levies, as specified by the Company.

4.28 "Membership Plan"

"Membership Plan" means a structured package of Services offered by the Company at specified prices, durations, and benefits.

The Company may introduce, modify, suspend, merge, or discontinue Membership Plans at its sole discretion.

4.29 "Verification Services"

"Verification Services" means optional or mandatory services through which the Company may verify one or more particulars submitted by a User, including identity; mobile number; email

address;

educational qualifications; employment; income; address; marital status; photograph; social media profile; or any other information.

Verification Services shall be performed only to the extent represented by the Company and shall not amount to a guarantee of authenticity.

4.30 "AI Match Recommendation"

"AI Match Recommendation" means any profile recommendation, ranking, compatibility score, behavioural prediction, search result, suggested match, preference analysis, or automated recommendation generated by Artificial Intelligence, Machine Learning, statistical models, predictive analytics, or algorithmic systems deployed by the Company.

Such recommendations are probabilistic in nature and shall not be construed as advice, certification, endorsement, or guarantee of compatibility or successful matrimonial alliance.

4.31 "Profile Visibility"

"Profile Visibility" means the manner, frequency, order, ranking, prominence, or audience to whom a

User's Profile is displayed on the Platform through manual selection, search algorithms, AI systems, recommendation engines, Premium Services, or promotional campaigns.

The Company reserves the right to determine Profile Visibility using automated or manual processes.

4.32 "Communication Services"

"Communication Services" means all facilities enabling interaction between Users, including:

- internal messaging;
- instant messaging;
- email notifications;
-

SMS alerts;

- voice calls;
- video calls;
-

AI chat assistance;

- customer support communications;
- system-generated alerts; and
- any future communication technology integrated into the Platform.

4.33 "Profile Boost"

"Profile Boost" means a paid or promotional feature enabling temporary enhanced visibility of a User's

Profile within search results, recommendations, featured listings, or other display mechanisms.

A Profile Boost shall not guarantee increased responses, successful matches, or matrimonial alliances.

4.34 "Featured Profile"

"Featured Profile" means a Profile highlighted by the Platform for promotional visibility pursuant to a

Premium Service or promotional campaign.

The Company does not guarantee any minimum number of profile views, enquiries, responses, or successful matrimonial outcomes.

4.35 "Search Services"

"Search Services" means facilities enabling Users to search, filter, sort, browse, or discover Profiles based on criteria including, without limitation:

age; gender; religion; caste; profession; education; income; location; language; marital status; lifestyle;

partner preferences; and AI-generated recommendations.

4.36 "Offline Services"

"Offline Services" means any assistance, consultation, verification, documentation, relationship management, customer support, event, or ancillary service provided by the Company outside the digital

Platform.

4.37 "Customer Support Services"

"Customer Support Services" means all support channels maintained by the Company for assisting

Users, including:

- telephone support;
- email support;
- chatbot assistance;
- live chat;
-

WhatsApp support (if provided);

- ticketing systems;
- grievance handling; and
- escalation mechanisms.

4.38 "Promotional Offer"

"Promotional Offer" means any discount, coupon, cashback, referral reward, loyalty benefit, complimentary upgrade, limited-period subscription, promotional campaign, or marketing incentive offered by the Company subject to specified terms and conditions.

The Company reserves the right to modify, withdraw, suspend, or cancel any Promotional Offer without prior notice unless otherwise required by Applicable Law.

4.39 "Platform Content"

"Platform Content" means all content owned, licensed, developed, generated, or otherwise controlled by the Company, including software, databases, logos, trademarks, source code, graphics, designs, layouts, algorithms, AI models, user interfaces, documentation, text, compilations, metadata, and all other proprietary material, excluding User Content.

4.40 "User Content"

"User Content" means all information, Profiles, photographs, videos, voice recordings, messages, reviews, ratings, comments, documents, certificates, communications, testimonials, and any other material uploaded, submitted, transmitted, shared, displayed, or otherwise made available by a User through the Platform.

The User retains ownership of User Content, subject to the licence granted to the Company under these Terms to host, reproduce, process, display, distribute, moderate, and use such content solely for the operation, maintenance, improvement, security, and promotion of the Platform, or as otherwise permitted by these Terms or Applicable Law.

4.41 "Algorithm"

"Algorithm" means any computational logic, mathematical model, formula, rule set, artificial intelligence model, machine learning model, software instruction, statistical methodology, ranking engine, recommendation engine, predictive model, decision tree, heuristic process, neural network, natural language processing model, or any other automated computational process used by the Platform for performing, facilitating, or improving any Service.

4.42 "Application Programming Interface (API)"

"Application Programming Interface" or "API" means any software interface, protocol, communication framework, software development kit (SDK), gateway, webhook, endpoint, integration mechanism, authentication interface, or similar technology that enables

communication, interoperability, data exchange, or functionality sharing between the Platform and any internal or external software application, service, device, or system.

Unless expressly authorised in writing by the Company, no User shall access, reproduce, reverse engineer, scrape, monitor, or integrate with any API of the Platform.

4.43 "Artificial Intelligence" or "AI"

"Artificial Intelligence" or "AI" means any computational technology capable of performing tasks that ordinarily require human intelligence, including but not limited to Machine Learning (ML); Deep

Learning; Neural Networks; Large Language Models (LLMs); Natural Language Processing (NLP); Computer Vision; Recommendation Engines; Behavioural Analytics; Predictive Analytics; Expert Systems; Generative AI; Intelligent Automation; Conversational AI; Decision Support Systems; Reinforcement Learning; and any future artificial intelligence technologies.

AI includes both proprietary systems developed by the Company and third-party AI technologies lawfully integrated into the Platform.

4.44 "Automated Decision-Making"

"Automated Decision-Making" means any decision, recommendation, ranking, prioritisation, moderation, fraud assessment, compatibility analysis, profile visibility determination, search result ordering, communication filtering, risk assessment, subscription recommendation, or similar activity carried out wholly or partly through automated systems without direct human intervention.

Such decisions may utilise:

- Artificial Intelligence;
- Machine Learning;
- statistical models;
- behavioural analytics;
- predictive modelling;
- data analysis;
- rule-based systems; or
- other computational technologies.

4.45 "Behavioural Analytics"

"Behavioural Analytics" means the automated collection, processing, interpretation, modelling,

and analysis of User interactions with the Platform for purposes including:

- improving Services;
- fraud prevention;
- cybersecurity;
- recommendation systems;
- usability enhancement;
- performance optimisation;
- abuse detection;
- customer experience; and
- platform security.

4.46 "Biometric Information"

"Biometric Information" means any measurable biological, behavioural, or physiological characteristic capable of identifying or assisting in identifying an individual, including facial recognition data, voiceprints, fingerprints, iris scans, or similar data, where collected in accordance with Applicable Law and with appropriate consent where required.

4.47 "Bot"

"Bot" means any automated software application, script, crawler, robot, autonomous software agent, artificial intelligence agent, browser automation tool, headless browser, macro, or similar technology capable of interacting with the Platform without direct human control.

4.48 "Browser Fingerprint"

"Browser Fingerprint" means a collection of technical characteristics relating to a browser, operating system, device configuration, fonts, plugins, language settings, screen resolution, hardware configuration, or similar identifiers capable of distinguishing one device or browser from another.

4.49 "Cache"

"Cache" means any temporary storage mechanism used for improving system performance, reducing network traffic, increasing response speed, enhancing security, or facilitating efficient delivery of

Services.

4.50 "Cloud Infrastructure"

"Cloud Infrastructure" means any cloud computing environment, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), storage infrastructure, content delivery network (CDN), virtual machine, container platform, or similar hosted

technology used in connection with the Platform.

4.51 "Cookie"

"Cookie" means a small text file, pixel, software tag, local storage object, web beacon, SDK identifier, tracking technology, or similar digital mechanism placed or stored on a User's browser or device for purposes including:

- authentication; • session management; • remembering preferences; • improving security; • analytics; • fraud prevention; • advertising; • personalisation; and • improving user experience.
- Cookies include:

4.52 "Cyber Incident"

"Cyber Incident" means any actual, suspected, attempted, or reasonably anticipated event affecting the confidentiality, integrity, availability, authenticity, or security of the Platform, including: • hacking; • malware; • ransomware; • phishing; • data breaches; • denial-of-service attacks; • credential compromise; • unauthorised access; • account takeover; • data exfiltration; • insider threats; • software vulnerabilities; or • any similar cyber event.

4.53 "Device Identifier"

"Device Identifier" means any unique or semi-unique identifier assigned to a User's device, browser, operating system, mobile application, hardware component, SIM card, or communication device, including advertising identifiers and similar technical identifiers.

4.54 "Digital Evidence"

"Digital Evidence" means every electronic record, log, communication, metadata, technical record, audit trail, or electronically stored information generated, collected, preserved, or maintained by the Company in connection with the Platform, including: • login history; • logout records; • timestamps; • IP addresses;

- browser fingerprints; • cookies; • device identifiers; • communication logs; • payment records; • OTP verification records; • subscription history; • moderation history; • account activity; • fraud detection records; • server logs; • metadata; • API logs; • security alerts; • audit logs; and • any other electronic information capable of evidentiary use.

Digital Evidence may be preserved, disclosed, or relied upon for regulatory compliance, fraud prevention, internal investigations, dispute resolution, arbitration, litigation, or compliance with Applicable Law.

4.55 "Electronic Record"

"Electronic Record" means any information created, generated, transmitted, received, stored, processed, or maintained in electronic form, including emails, electronic messages, digital

contracts, click-wrap agreements, OTP verification records, system logs, databases, electronic communications, metadata, electronic signatures, scanned documents, cloud records, server records, and any other information recognised as an electronic record under Applicable Law.

4.56 "Electronic Signature"

"Electronic Signature" means any electronic method adopted by a User to indicate acceptance, consent, approval, execution, authentication, or acknowledgement of any agreement, policy, communication, or transaction, including click-wrap acceptance, OTP verification, digital signature certificates, electronic acknowledgements, biometric confirmation (where legally permissible), or any other legally recognised method.

4.57 "Generative Artificial Intelligence"

"Generative Artificial Intelligence" means any artificial intelligence model capable of generating text, images, audio, video, code, recommendations, summaries, translations, conversations, or other content through automated computational processes.

4.58 "IP Address"

"IP Address" means the Internet Protocol address or any equivalent network identifier assigned to a User's device, network, gateway, proxy, virtual private network (VPN), or communication endpoint.

4.59 "Large Language Model (LLM)"

"Large Language Model" or "LLM" means any transformer-based, neural network-based, or similar language model trained to understand, generate, analyse, summarise, classify, or process natural language, whether proprietary or third-party.

4.60 "Machine Learning" or "ML"

"Machine Learning" means any computational methodology enabling software systems to improve performance or generate predictions based upon data analysis, statistical modelling, or algorithmic learning without requiring explicit programming for every decision.

4.61 "Metadata"

"Metadata" means information describing, relating to, or generated in connection with electronic information, including timestamps, file attributes, communication details, device information, network information, geolocation information (where applicable), account activity, audit information, and technical characteristics associated with digital content.

4.62 "Natural Language Processing (NLP)"

"Natural Language Processing" means computational technologies enabling software to

understand, interpret, analyse, translate, generate, classify, or otherwise process human language.

4.63 "Security Credentials"

"Security Credentials" means usernames, passwords, PINs, passphrases, OTPs, authentication tokens, biometric identifiers (where applicable), security questions, digital certificates, encryption keys, access credentials, and every other authentication mechanism used for securing access to the Platform.

4.64 "Server Log"

"Server Log" means automatically generated electronic records relating to the operation, security, maintenance, performance, or use of the Platform, including system events, access logs, error logs, transaction logs, API logs, audit logs, and security logs.

4.65 "Session"

"Session" means the period commencing when a User successfully authenticates access to the Platform and ending upon logout, expiry, timeout, termination, or other cessation of authenticated access.

4.66 "Software"

"Software" means every application, source code, object code, executable file, script, program, database, operating system, mobile application, web application, API, SDK, firmware, algorithm, AI model, or similar technology owned, licensed, developed, or used by the Company.

4.67 "Technology Infrastructure"

"Technology Infrastructure" means the complete technological ecosystem supporting the Platform, including software, hardware, servers, cloud infrastructure, databases, APIs, AI systems, cybersecurity systems, networking infrastructure, telecommunications systems, storage infrastructure, monitoring systems, disaster recovery systems, and business continuity arrangements.

4.68 "Two-Factor Authentication (2FA)"

"Two-Factor Authentication" or "2FA" means any authentication mechanism requiring two or more independent factors to verify a User's identity, including passwords, OTPs, biometric verification, hardware tokens, authentication applications, or similar security methods.

4.69 "User Device"

"User Device" means any computer, laptop, smartphone, tablet, wearable device, smart television, IoT device, communication equipment, or other electronic device through which the Platform is accessed.

4.70 "Virtual Private Network (VPN)"

"VPN" means any technology designed to route internet communications through encrypted tunnels or intermediary servers to obscure or modify the originating network address or geographic location of a User.

4.71 "Anonymisation"

"Anonymisation" means the irreversible process of transforming Personal Data into a form in which an individual cannot be identified, directly or indirectly, by any person using reasonably available means, such that the data ceases to constitute Personal Data under Applicable Law.

4.72 "Consent"

"Consent" means any free, specific, informed, unconditional, unambiguous, and affirmative indication of the User's agreement whereby the User signifies approval for the collection, processing, storage, sharing, transfer, retention, disclosure, or other use of Personal Data by the Company for one or more specified purposes.

Consent may be obtained through: • click-wrap agreements; • checkbox confirmations; • OTP verification; • digital signatures; • electronic acknowledgements; • in-app confirmations; • written declarations; • recorded verbal consent (where legally permissible); or • any other lawful method recognised under Applicable Law.

Consent shall include express consent where required by law.

4.73 "Data"

"Data" means any representation of information, facts, concepts, opinions, instructions, records, communications, images, videos, audio recordings, metadata, electronic records, logs, analytics, identifiers, or any other information capable of being processed by electronic means.

4.74 "Data Breach" or "Personal Data Breach"

"Data Breach" means any confirmed or reasonably suspected event resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, unauthorised access to, corruption of, misuse of, or inability to access Personal Data or other protected information processed by or on behalf of the

Company.

This includes, without limitation:

- hacking; • ransomware attacks; • phishing; • malware infections; • insider misuse; • accidental disclosure; • unauthorised database access; • cloud storage compromise; • credential theft; • API compromise; • system vulnerability exploitation; and • any similar cybersecurity

incident.

4.75 "Data Fiduciary"

"Data Fiduciary" shall have the meaning assigned under the Digital Personal Data Protection Act, 2023, and refers to any person or entity that alone or jointly with others determines the purpose and means of Processing Personal Data. For the purposes of these Terms, the Company shall act as a Data

Fiduciary to the extent prescribed by Applicable Law.

4.76 "Data Principal"

"Data Principal" shall have the meaning assigned under the Digital Personal Data Protection Act, 2023, and refers to the individual to whom the Personal Data relates, including any lawful representative acting on behalf of such individual where permitted by law.

4.77 "Data Processor"

"Data Processor" means any natural or legal person, third-party service provider, contractor, cloud provider, payment processor, verification agency, analytics provider, customer support vendor, artificial intelligence provider, or any other entity that Processes Personal Data on behalf of the Company under contractual or legal authority.

4.78 "Data Protection Laws"

"Data Protection Laws" means all Applicable Laws governing privacy, Personal Data, electronic communications, cybersecurity, information security, and digital rights, including any amendments, replacements, subordinate legislation, regulatory directions, or governmental guidelines issued from time to time.

4.79 Data Retention"

"Data Retention" means the storage and preservation of Personal Data, User Content, Digital Evidence,

Electronic Records, transaction records, security logs, communication records, audit trails, and other information for such duration as may be necessary for providing the Services; legal compliance; fraud prevention; dispute resolution; taxation; accounting; cybersecurity; enforcement of legal rights;

regulatory investigations; or for any other lawful purpose.

4.80 "Data Sharing"

"Data Sharing" means the disclosure, transmission, transfer, exchange, publication, dissemination, provision, or making available of Data or Personal Data to any third party, affiliate, service provider, governmental authority, or other lawful recipient, whether

electronically or otherwise, in accordance with Applicable Law and these Terms.

4.81 "De-identification"

"De-identification" means the process of removing, masking, encrypting, pseudonymising, or otherwise reducing identifying characteristics from Personal Data while recognising that such information may remain capable of re-identification under certain circumstances.

4.82 "Personal Data"

"Personal Data" means any data relating to an identified or identifiable natural person, whether directly or indirectly, including any information recognised as Personal Data under Applicable Law.

Personal Data may include, without limitation:

- name;
- photograph;
- date of birth;
- gender;
- marital status;
- religion;
- caste or community information voluntarily provided by the User;
- educational qualifications;
- occupation;
- employer details;
- income information voluntarily disclosed;
- residential address;
- correspondence address;
- email address;
- mobile number;
- government-issued identity details voluntarily submitted for verification;
- IP address;
- device identifiers;
- geolocation data (where collected with appropriate notice or consent);
- payment-related information (excluding full payment card credentials where not stored);
- communication records;
- preferences;
- behavioural information;
- technical identifiers;
- metadata; and
- any other information capable of identifying an individual.

4.83 "Privacy Notice" or "Privacy Policy"

"Privacy Notice" or "Privacy Policy" means the Company's privacy policy published on the Platform, as amended from time to time, describing the manner in which Personal Data is collected, processed, stored, shared, retained, secured, and otherwise handled.

4.84 "Processing"

"Processing" means any operation or set of operations performed on Data or Personal Data, whether by automated means or otherwise, including:

- collection;
- recording;
- organisation;
- structuring;
- storage;
- adaptation;
- alteration;
- retrieval;
- consultation;
- analysis;
- use;
- profiling;
- disclosure;
- transmission;
- dissemination;
- sharing;
- alignment;
- combination;
- anonymisation;
- pseudonymisation;
- restriction;
- encryption;
- archival;
- deletion; and
- destruction.

4.85 "Profiling"

"Profiling" means any form of automated Processing of Personal Data used to evaluate, analyse,

predict, classify, recommend, score, rank, or assess a User's preferences, interests, compatibility, behaviour, or interactions for providing or improving the Services.

4.86 "Pseudonymisation"

"Pseudonymisation" means the Processing of Personal Data in such a manner that the data can no longer be attributed to a specific individual without the use of additional information that is separately maintained and protected by appropriate technical and organisational safeguards.

4.87 "Sensitive Information"

"Sensitive Information" means any category of information that requires enhanced protection under

Applicable Law or by reason of its nature, including authentication credentials, government-issued identification documents, financial account information, biometric information (where processed), or other information designated by Applicable Law as requiring additional safeguards.

4.88 "Third-Party Recipient"

"Third-Party Recipient" means any person or entity, other than the User or the Company, to whom Data or Personal Data may lawfully be disclosed or made available, including:

- cloud service providers;
- payment gateways;
- verification agencies;
- analytics providers;
- cybersecurity vendors;
- communication service providers;
- legal advisors;
- auditors;
- insurers;
- regulators;
- law enforcement authorities; and
- other authorised service providers.

4.89 "Usage Data"

"Usage Data" means information automatically generated through the User's interaction with the

Platform, including:

- pages visited;
- session duration;
- clicks;
- navigation patterns;
- feature usage;
- browser type;
- operating system;
- device characteristics;
- application version;
- crash reports;
- diagnostics;
- referral sources;
- IP address;
- timestamps; and
- similar technical or behavioural information.

4.90 "User Preferences"

"User Preferences" means the settings, selections, filters, partner preferences, notification choices, privacy settings, language preferences, communication preferences, search criteria, subscription options, and other configurable choices selected by a User while using the Platform.

4.91 "Cross-Border Data Transfer"

"Cross-Border Data Transfer" means any transfer, access, storage, processing, backup,

replication, hosting, or availability of Personal Data outside the territorial jurisdiction of India, whether directly or through third-party infrastructure, subject to Applicable Law and the Company's Privacy Policy.

4.92 "Encryption"

"Encryption" means the use of cryptographic techniques or other recognised security mechanisms to protect Data or Personal Data from unauthorised access, disclosure, alteration, interception, or misuse during storage, transmission, or Processing.

4.93 "Security Measures"

"Security Measures" means the administrative, organisational, contractual, physical, and technical safeguards implemented by the Company to protect Data, Personal Data, Digital Evidence, Electronic

Records, and Technology Infrastructure against accidental, unlawful, or unauthorised access, disclosure, destruction, loss, alteration, misuse, or compromise.

4.94 "Data Portability Request"

"Data Portability Request" means any lawful request made by a Data Principal, where recognised under

Applicable Law, seeking a copy or transfer of Personal Data maintained by the Company in a structured, commonly used, and technically feasible format, subject to legal limitations, technical feasibility, and the rights of other persons.

4.95 "Privacy Incident"

"Privacy Incident" means any actual or suspected event involving the unauthorised collection, use, disclosure, alteration, retention, or Processing of Personal Data in a manner inconsistent with Applicable

Law, these Terms, or the Company's Privacy Policy, irrespective of whether such event constitutes a reportable Data Breach.

4.96 "Billing Cycle"

"Billing Cycle" means the recurring period for which Subscription Fees or Charges become due and payable by the User, whether monthly, quarterly, half-yearly, annually, lifetime (where applicable), usage-based, transaction-based, or any other billing model introduced by the Company.

4.97 "Cancellation"

"Cancellation" means the voluntary or involuntary termination, discontinuation, withdrawal, suspension, or non-renewal of a Subscription, Premium Service, Membership Plan, Order,

Transaction, or User Account, whether initiated by the User, the Company, a Payment Service Provider, or pursuant to Applicable Law.

4.98 "Charge" or "Charges"

"Charge" or "Charges" means every amount payable by a User to the Company for the use of the

Platform or any Services, including but not limited to: • Subscription Fees; • Membership Fees; • Verification Charges; • Service Charges; • Processing Fees; • Convenience Fees; • Platform Fees; •

Administrative Charges; • Upgrade Charges; • Renewal Charges; • Profile Promotion Charges; • Consultation Fees; • Event Participation Fees; • Advertising Charges; • Third-Party Service Fees; and • any other lawful fee notified by the Company from time to time.

4.99 "Chargeback"

"Chargeback" means any reversal, cancellation, dispute, recovery, or forced refund of a payment initiated by the issuing bank, card network, payment gateway, financial institution, digital wallet provider, Unified

Payments Interface (UPI) service provider, or any other Payment Service Provider at the request of the

User or otherwise. A Chargeback includes any payment dispute initiated on the grounds of alleged fraud, unauthorised transaction, service dissatisfaction, duplicate payment, merchant dispute, cardholder claim, or any similar reason.

4.100 "Commercial Communication"

"Commercial Communication" means any promotional, transactional, marketing, informational, educational, customer relationship, loyalty programme, referral programme, subscription-related, or advertising communication sent by or on behalf of the Company through email, SMS, WhatsApp, in-app notifications, push notifications, telephone calls, social media platforms, or any other communication channel permitted under Applicable Law.

4.101 "Convenience Fee"

"Convenience Fee" means an additional amount charged by the Company or Payment Service Provider for facilitating online payments, digital transactions, premium support, express processing, specialised payment methods, or similar conveniences.

4.102 "Discount"

"Discount" means any reduction in the listed price of a Service, Subscription, Membership Plan,

Product,

Promotional Offer, or other commercial offering granted by the Company subject to applicable terms and conditions.

4.103 "Digital Payment"

"Digital Payment" means any payment made electronically using debit cards, credit cards, prepaid instruments, UPI, net banking, mobile wallets, bank transfers, QR codes, payment links, recurring mandates, auto-debit facilities, digital banking platforms, or any other electronic payment mechanism recognised under Applicable Law.

4.104 "Invoice"

"Invoice" means any electronic or physical tax invoice, receipt, bill, statement of account, payment confirmation, debit note, credit note, or commercial document issued by or on behalf of the Company evidencing Charges payable or paid by a User.

Electronic Invoices shall constitute valid legal records.

4.105 "Membership Fee"

"Membership Fee" means the consideration payable for registration under any paid Membership Plan offered by the Company.

4.106 "Order"

"Order" means any request, purchase, booking, subscription, renewal, upgrade, verification request, consultation request, advertisement booking, promotional purchase, or other commercial transaction initiated by a User through the Platform.

4.107 "Payment Gateway"

"Payment Gateway" means any third-party payment processing system, payment aggregator, acquiring bank, payment institution, financial intermediary, card network, or licensed payment service provider authorised to facilitate Digital Payments on behalf of the Company.

The Company does not own or control Payment Gateways and shall not be liable for delays, failures, or errors attributable solely to such third-party providers, except as required by Applicable Law.

4.108 "Payment Instrument"

"Payment Instrument" means any lawful instrument used to complete a Digital Payment, including: • credit cards; • debit cards; • prepaid cards; • UPI applications; • internet banking; • mobile wallets; • electronic mandates; • payment links; • QR code payments; • bank transfers; • NEFT; • RTGS; • IMPS; • recurring payment mandates; and • any future digital payment technology recognised under Applicable

Law.

4.109 "Payment Service Provider" or "PSP"

"Payment Service Provider" means any licensed bank, payment aggregator, payment gateway, acquiring institution, wallet operator, UPI service provider, fintech company, card network, or other financial intermediary involved in processing payments made through the Platform.

4.110 "Platform Credits"

"Platform Credits" means any non-cash promotional credit, wallet balance, reward points, referral incentive, loyalty benefit, or digital value issued by the Company that may be redeemed for eligible

Services in accordance with the Company's policies.

Platform Credits shall:

- have no independent cash value unless expressly stated;
- not constitute legal tender;
- not accrue interest; and
- be subject to expiry, cancellation, suspension, or forfeiture in accordance with applicable terms.

4.111 "Pricing"

"Pricing" means the schedule of Charges, Fees, Taxes, discounts, promotional pricing, subscription rates, or commercial consideration published by the Company from time to time.

The Company reserves the right to revise Pricing prospectively, subject to Applicable Law.

4.112 "Promotional Offer"

"Promotional Offer" means any limited-period campaign, coupon, voucher, referral programme, cashback, complimentary subscription, loyalty programme, introductory offer, discount code, bundled package, festive promotion, corporate offer, student offer, or other marketing incentive offered by the

Company subject to specific eligibility conditions.

The Company reserves the right to modify, suspend, withdraw, or terminate any Promotional Offer at its sole discretion, except where prohibited by Applicable Law.

4.113 "Refund"

"Refund" means the return, reversal, repayment, adjustment, or credit of any amount paid by a User in accordance with the Company's Refund & Cancellation Policy, Applicable Law, or a final judicial or regulatory direction.

Unless expressly provided otherwise:

-

Refunds shall not include compensation, damages, or interest.

-

Refunds shall be processed only through the original payment method or another lawful method determined by the Company.

-

Processing timelines may depend on banks, Payment Service Providers, and financial institutions.

4.114 "Recurring Payment"

"Recurring Payment" means any payment authorised by the User to be automatically debited at predetermined intervals for renewal of a Subscription or Premium Service through a standing instruction, e-mandate, card-on-file arrangement, UPI AutoPay, or any other legally recognised recurring payment mechanism.

4.115 "Renewal"

"Renewal" means the continuation or extension of a Subscription or Membership Plan beyond its original term, whether automatically, manually, or pursuant to the User's instructions.

4.116 "Service Fee"

"Service Fee" means any fee payable by the User for a specific feature, facility, transaction, consultation, verification, event, or ancillary service offered by the Company separately from Membership Fees or Subscription Fees.

4.117 "Subscription"

"Subscription" means a contractual arrangement under which the User obtains access to Premium

Services for a specified duration or usage period upon payment of applicable Charges.

Subscriptions may be fixed-term; recurring; enterprise; promotional; complimentary; usage-based; or customised.

4.118 "Subscription Fee"

"Subscription Fee" means the consideration payable for obtaining or continuing a Subscription. Subscription Fees may include applicable taxes, gateway charges, convenience fees, or statutory levies unless expressly stated otherwise.

4.119 "Tax" or "Taxes"

"Tax" or "Taxes" means all applicable present and future governmental levies, duties, imposts,

cess, surcharge, GST, value-added tax, sales tax, withholding tax, service tax (where applicable), customs duties, stamp duties, or similar fiscal impositions payable under Applicable Law.

Unless expressly stated otherwise, Users shall be responsible for payment of all applicable Taxes arising from their use of the Platform.

4.120 "Transaction"

"Transaction" means every commercial interaction involving payment, subscription, purchase, renewal, refund, cancellation, promotional redemption, wallet utilisation, verification request, advertisement booking, or any other financial activity carried out through the Platform.

Electronic records maintained by the Company relating to a Transaction shall constitute prima facie evidence of such Transaction, subject to Applicable Law.

4.121 "Wallet"

"Wallet" means any digital value storage mechanism, prepaid balance, Platform Credit account, or electronic wallet made available by or integrated with the Platform for making payments or redeeming eligible benefits, subject to Applicable Law and applicable terms.

4.122 "Wrongful Payment"

"Wrongful Payment" means any payment received by the Company due to fraud, mistake, technical error, duplicate transaction, unauthorised use of a Payment Instrument, banking error, or any other circumstance requiring investigation or corrective action under Applicable Law.

4.123 "Settlement"

"Settlement" means the final transfer of funds between the User, the Company, acquiring banks, Payment Service Providers, or other authorised financial institutions in respect of any Transaction carried out through the Platform.

4.124 "Financial Fraud"

"Financial Fraud" means any fraudulent, dishonest, deceptive, or unlawful act intended to obtain money, services, subscriptions, refunds, credits, Promotional Offers, or other financial benefits through misrepresentation, identity theft, stolen payment instruments, chargeback abuse, phishing, account takeover, money laundering, or any other unlawful means.

4.125 "Chargeback Abuse"

"Chargeback Abuse" means the initiation of a Chargeback in bad faith, including where a User knowingly disputes a valid Transaction after receiving the relevant Services or otherwise seeks to obtain an unjustified financial advantage.

The Company reserves the right to suspend or terminate Accounts, recover losses, deny future

Services, and pursue legal remedies in cases of Chargeback Abuse, subject to Applicable Law.

4.126 "Applicable Regulatory Authority"

"Applicable Regulatory Authority" means any governmental, statutory, judicial, quasi-judicial, regulatory, administrative, investigative, licensing, supervisory, taxation, cybersecurity, consumer protection, or law enforcement authority having jurisdiction over the Company, the Platform, the User, or any transaction conducted through the Platform.

4.127 "Arbitration"

"Arbitration" means the private dispute resolution mechanism agreed between the Parties under these

Terms whereby disputes are referred to one or more independent arbitrators for final and binding adjudication in accordance with the Arbitration and Conciliation Act, 1996, as amended from time to time.

4.128 "Business Continuity Event"

"Business Continuity Event" means any occurrence affecting the Company's ability to provide uninterrupted Services, including disasters, infrastructure failures, cyber incidents, pandemics, governmental restrictions, cloud outages, or any Force Majeure Event requiring activation of business continuity or disaster recovery procedures.

4.129 "Claim"

"Claim" means every allegation, complaint, notice, demand, dispute, action, suit, proceeding, arbitration, inquiry, investigation, prosecution, appeal, petition, writ, regulatory action, or legal process of every nature whatsoever.

4.130 "Confidential Information"

"Confidential Information" means all proprietary, confidential, commercially sensitive, technical, operational, financial, legal, strategic, security-related, business, customer, or technological information belonging to the Company or lawfully entrusted to it, whether disclosed orally, electronically, visually, or in writing.

Confidential Information includes, without limitation: source code; object code; databases; algorithms; AI models; pricing models; software architecture; APIs; cybersecurity measures; trade secrets; business strategies; customer databases; internal communications; legal opinions; audit reports; financial records; verification methodologies; fraud detection systems; commercial agreements; and all non-public information.

Confidential Information shall not include information that:

- (a) is lawfully in the public domain;
- (b) becomes publicly available without breach of confidentiality;
- (c) is independently developed without reference to the confidential information; or
- (d) is lawfully received from a third party without restriction.

4.131 "Dispute"

"Dispute" means every disagreement, controversy, difference, complaint, claim, action, counterclaim, legal issue, contractual disagreement, tortious allegation, regulatory issue, or question arising directly or indirectly out of or relating to:

these Terms; use of the Platform; Services; subscriptions; payments; User Content; privacy; intellectual property; AI-generated recommendations; electronic records; advertisements; or any relationship between the Company and the User.

4.132 "Electronic Evidence"

"Electronic Evidence" means every Electronic Record, Digital Evidence, metadata, server log, communication record, transaction log, audit trail, system log, security log, authentication record, timestamp, device identifier, browser fingerprint, or other electronically stored information that may be relied upon as evidence under Applicable Law.

4.133 "Force Majeure Event"

"Force Majeure Event" means any event beyond the reasonable control of the Company, including but not limited to:

acts of God; earthquakes; floods; cyclones; fires; lightning; epidemics; pandemics; public health emergencies; war; terrorism; riots; civil unrest; labour strikes; governmental restrictions; judicial orders;

internet failures; cloud infrastructure failures; cyberattacks; ransomware; denial-of-service attacks;

telecommunications failures; power outages; satellite failures; changes in Applicable Law; embargoes;

sanctions; failures of third-party service providers; and any similar event beyond the Company's reasonable control.

4.134 "Fraud"

"Fraud" means any dishonest, deceptive, misleading, unlawful, or fraudulent act intended to obtain an unlawful benefit or cause wrongful loss to the Company, another User, or any third party, including:

identity theft; fake profiles; forged documents; phishing; impersonation; payment fraud; account

takeover; chargeback abuse; social engineering; money laundering; financial scams; and fraudulent matrimonial representations.

4.135 "Governing Law"

"Governing Law" means the laws of the Republic of India applicable to these Terms, irrespective of conflict of law principles.

4.136 "Indemnified Parties"

"Indemnified Parties" means the Company together with its: directors; shareholders; officers; employees; consultants; agents; affiliates; subsidiaries; licensors; contractors; service providers; successors; assigns; and authorised representatives.

4.137 "Intellectual Property"

"Intellectual Property" means every present and future proprietary right recognised under Applicable

Law, including: copyrights; neighbouring rights; trademarks; service marks; trade names; logos; trade dress; patents; utility models; industrial designs; domain names; business names; software; databases;

algorithms; APIs; source code; object code; AI models; datasets; documentation; confidential know-how;

trade secrets; goodwill; and every other intellectual property right.

4.138 "Intellectual Property Rights"

"Intellectual Property Rights" means every statutory, common law, equitable, contractual, moral, neighbouring, proprietary, or other right relating to Intellectual Property existing now or arising in the future anywhere in the world.

4.139 "Investigation"

"Investigation" means every internal inquiry, audit, verification exercise, compliance review, fraud detection exercise, regulatory inspection, law enforcement investigation, or judicial inquiry relating to the Platform or its Users.

4.140 "Legal Process"

"Legal Process" includes:

notices; summons; warrants; court orders; injunctions; subpoenas; governmental directions; arbitral proceedings; mediation; investigations; regulatory actions; execution proceedings; appeals; and every lawful judicial or administrative process.

4.141 "Notice"

"Notice" means any communication issued under these Terms through:

email; registered post; courier; in-app notification; dashboard notification; SMS; WhatsApp (where supported); electronic messaging; publication on the Platform; or any other legally recognised communication method.

4.142 "Party"

"Party" means either the Company or the User individually, and "Parties" means both collectively.

4.143 "Proceedings"

"Proceedings" means every judicial, arbitral, administrative, regulatory, criminal, civil, consumer, tax, or quasi-judicial proceeding instituted before any competent authority.

4.144 "Regulatory Compliance"

"Regulatory Compliance" means compliance with every Applicable Law, governmental direction, judicial order, industry standard, regulatory requirement, cybersecurity direction, tax obligation, or statutory compliance applicable to the Company or the User.

4.145 "Sanctions"

"Sanctions" means any trade restriction, embargo, financial sanction, export control measure, anti- money laundering requirement, or governmental restriction imposed by a competent authority that affects the provision or receipt of Services.

4.146 "Settlement"

"Settlement" means any negotiated resolution, compromise, mediation outcome, arbitral award, consent order, or judicial settlement entered into for resolving a Dispute.

4.147 "Surviving Obligations"

"Surviving Obligations" means obligations which continue notwithstanding suspension, cancellation, expiration, or termination of these Terms, including obligations relating to: payment; refunds;

confidentiality; privacy; intellectual property; limitation of liability; indemnity; dispute resolution; arbitration; electronic records; fraud investigations; regulatory cooperation; and any provision intended by its nature to survive.

4.148 "Third-Party Claim"

"Third-Party Claim" means every claim, complaint, action, demand, investigation, proceeding, or allegation initiated by any person other than the Company and the concerned User.

4.149 "Trade Secret"

"Trade Secret" means confidential commercial information, technical knowledge, software architecture, algorithms, business methods, AI models, verification methodologies, pricing

strategies, databases, customer information, security procedures, operational manuals, and every other proprietary information providing commercial value due to its confidentiality.

4.150 "Waiver"

"Waiver" means the intentional relinquishment by a Party of a specific legal right, provided that no waiver shall be effective unless made expressly in writing by the authorised representative of the

Company. No delay, omission, or partial exercise of any right shall constitute a waiver of that or any other right.

4.151 "Jurisdiction"

"Jurisdiction" means the exclusive territorial and subject-matter jurisdiction of the competent courts specified in these Terms for matters not required to be resolved through arbitration, including proceedings relating to interim relief, enforcement of arbitral awards, or matters expressly reserved to courts under Applicable Law.

4.152 "Interim Relief"

"Interim Relief" means any temporary, urgent, or interlocutory remedy, including injunctions, preservation orders, attachment orders, or other protective measures sought before, during, or after arbitration or legal proceedings to safeguard rights, assets, evidence, confidential information, or the subject matter of a Dispute.

4.153 "Compliance Audit"

"Compliance Audit" means any internal or external review, inspection, assessment, verification, or examination conducted by or on behalf of the Company to ensure compliance with Applicable Law, these

Terms, internal policies, contractual obligations, cybersecurity requirements, privacy standards, or regulatory directives.

4.154 "Legal Hold"

"Legal Hold" means the preservation of Electronic Records, Digital Evidence, User Content, communications, logs, or other information by the Company due to pending or anticipated litigation, arbitration, investigation, regulatory inquiry, or other Legal Process, notwithstanding any ordinary data retention or deletion schedule.

PART IV – RULES OF INTERPRETATION

5. Rules of Interpretation

Unless the context otherwise expressly requires, the following rules shall govern the interpretation, construction, implementation, administration, and enforcement of these Terms of

Use, together with every policy, guideline, schedule, annexure, notice, agreement, and legal document incorporated herein by reference or published by the Company from time to time.

5.1 Purpose of Interpretation

These Rules of Interpretation are intended to ensure that these Terms are construed fairly, consistently, and in accordance with their commercial purpose. They shall apply not only to these Terms of Use but also to the Privacy Policy, Cookie Policy, Refund and Cancellation Policy, Website Disclaimer, Community

Guidelines, Intellectual Property Policy, Child Safety Policy, Grievance Redressal Policy, AI and Automated

Systems Policy (if adopted), subscription agreements, promotional terms, and every supplementary legal document or policy issued by the Company from time to time. Each such document shall, unless expressly stated otherwise, be deemed an integral part of these Terms and shall be interpreted harmoniously with them.

5.2 Singular and Plural

Words denoting the singular shall include the plural and vice versa whenever the context so admits or requires. Accordingly, references to a User shall include multiple Users, references to a Service shall include multiple Services, and similar expressions shall be interpreted in a manner that best gives effect to the intent and purpose of these Terms.

5.3 Gender

Words importing any gender shall include every other gender. Pronouns and expressions referring to masculine, feminine, or neutral genders shall be construed interchangeably wherever the context permits, and these Terms shall be interpreted in a gender-neutral manner.

5.4 References to Persons

Any reference to a person shall include a natural person, sole proprietorship, Hindu Undivided Family, partnership firm, limited liability partnership, company, corporation, trust, society, association, governmental authority, statutory body, regulatory authority, international organisation, foreign entity, or any other juridical or legal person recognised under Applicable Law, including its successors and permitted assigns where the context so requires.

5.5 References to the Company

Any reference to the Company shall, unless the context otherwise requires, include its holding companies, subsidiaries, affiliates, successors, assigns, directors, officers, employees, consultants, contractors, licensors, authorised representatives, service providers, agents, and every person lawfully acting on its behalf.

5.6 References to Laws

Any reference to any Act, statute, regulation, rule, notification, circular, guideline, governmental direction, judicial precedent, regulatory framework, or other legal instrument shall include every amendment, modification, substitution, re-enactment, consolidation, delegated legislation, subordinate legislation, successor enactment, or statutory instrument issued thereunder from time to time.

5.7 Headings and Titles

The headings, chapter titles, clause titles, captions, numbering, indexes, and descriptive titles contained in these Terms are inserted solely for convenience of reference and organisational purposes. They shall not affect the interpretation, legal effect, scope, meaning, or enforceability of any provision contained herein.

5.8 Interpretation of Inclusive Expressions

Unless expressly stated otherwise, the words "including", "includes", "include", "such as", "for example", and similar expressions shall be interpreted as meaning "including, without limitation". The inclusion of illustrative examples shall not restrict or limit the generality of the provision in which they appear.

5.9 Writing and Electronic Records

Wherever these Terms require any communication, notice, agreement, approval, acknowledgement, consent, record, or document to be in writing, such requirement shall be satisfied by any legally recognised electronic form, including emails, electronic records, click-wrap agreements, browse-wrap agreements, digital signatures, OTP verifications, online forms, electronic acknowledgements, system-generated notifications, customer support communications, AI-assisted communications, and any other electronic method recognised under Applicable Law.

5.10 Electronic Communications

Every communication transmitted electronically by the Company through the Platform, registered email address, registered mobile number, dashboard notification, in-application notification, SMS, WhatsApp

(where supported), or any other authorised digital communication channel shall be deemed to have been validly delivered and received upon successful transmission, unless the User establishes otherwise by clear and convincing evidence.

5.11 References to Time

Unless expressly specified otherwise, all references to time shall refer to Indian Standard Time

(IST). A reference to a day shall mean a calendar day, a month shall mean a calendar month, and a year shall mean a calendar year.

5.12 Currency

Unless expressly stated otherwise, every monetary reference contained in these Terms shall be construed as a reference to Indian Rupees (INR). Any display of equivalent foreign currency values shall be for convenience only and shall not create any independent contractual or legal entitlement.

5.13 Technology-Neutral Interpretation

These Terms shall be interpreted in a technology-neutral manner. References to software, platforms, devices, communication systems, security measures, cloud infrastructure, digital technologies, payment systems, or technological processes shall automatically include future technological developments, upgrades, replacements, successor technologies, and substantially similar systems introduced after the

Effective Date without requiring amendment of these Terms.

5.14 Artificial Intelligence and Automated Systems

References to Artificial Intelligence shall include Generative Artificial Intelligence, Machine Learning,

Deep Learning, Neural Networks, Large Language Models, Predictive Analytics, Recommendation Engines, Intelligent Automation, Decision Support Systems, AI Agents, autonomous systems, and every other substantially similar or successor technology capable of performing automated computational functions.

5.15 Electronic Acceptance

Acceptance of these Terms may be manifested through any legally recognised electronic means, including clicking an "Accept", "Continue", "Register", "Subscribe", or similar button, completing account registration, verifying identity through OTP, making a payment, accessing or continuing to use the

Platform, uploading content, or otherwise using any Service after these Terms have been made available.

Such acceptance shall constitute a valid, binding, and enforceable electronic agreement between the User and the Company.

5.16 Entire Agreement

These Terms, together with every policy, guideline, schedule, annexure, and supplementary document expressly incorporated by reference, constitute the complete and exclusive

agreement between the

Company and the User concerning the subject matter hereof. They supersede all prior negotiations, discussions, proposals, representations, understandings, oral communications, correspondence, and agreements relating to the same subject matter, except where expressly preserved in writing.

5.17 Order of Precedence

Where any inconsistency arises between documents forming part of the contractual framework, mandatory provisions of Applicable Law shall prevail to the extent of such inconsistency. Subject thereto, these Terms shall prevail over all other policies unless a specific document expressly states that it overrides these Terms in relation to a particular subject matter. More specific provisions shall prevail over general provisions concerning the same subject.

5.18 Severability

If any provision of these Terms is declared invalid, illegal, void, unenforceable, or contrary to Applicable

Law by a court or competent authority, such provision shall be modified to the minimum extent necessary to render it valid and enforceable. If such modification is not possible, the affected provision shall be severed, and the remaining provisions shall continue in full force and effect.

5.19 Survival

The expiration, suspension, cancellation, or termination of these Terms or of any User Account shall not affect those provisions which by their nature are intended to survive, including provisions relating to payments, refunds, taxes, confidentiality, privacy, cybersecurity, intellectual property, licences, electronic records, digital evidence, limitation of liability, indemnification, dispute resolution, arbitration, governing law, investigations, compliance obligations, and record retention.

5.20 Waiver

No failure, delay, omission, or partial exercise by the Company of any right, remedy, power, or privilege under these Terms shall constitute a waiver thereof or prevent the subsequent exercise of that or any other right. Any waiver shall be effective only if expressly made in writing by a duly authorised representative of the Company.

5.21 Construction of the Agreement

The Parties acknowledge that these Terms constitute a commercial agreement governing the use of a technology platform. Accordingly, to the fullest extent permitted by Applicable Law, these Terms shall be interpreted fairly and reasonably to give effect to their commercial purpose

and shall not be construed adversely against either Party solely on the ground that one Party prepared or drafted them.

5.22 Independent Obligations

Each covenant, representation, warranty, obligation, restriction, and undertaking contained in these

Terms shall constitute an independent and severable obligation. The invalidity or unenforceability of one obligation shall not affect the validity or enforceability of any remaining obligations.

5.23 Future Services

Any reference to the Platform or the Services shall automatically include future products, software applications, mobile applications, APIs, artificial intelligence systems, subscription models, payment mechanisms, verification services, communication technologies, and any successor or replacement services introduced by the Company from time to time.

5.24 Digital Records

References to documents, records, books, registers, writings, evidence, communications, or similar materials shall include electronic records, cloud-based records, blockchain records (where implemented), metadata, audit trails, server logs, AI-generated records, transaction histories, and every other form of legally recognised digital record.

5.25 Good Faith

These Terms shall be interpreted in good faith, in a commercially reasonable manner, and consistently with their lawful purpose, so as to promote certainty, fairness, enforceability, and the legitimate commercial expectations of the Parties, always subject to Applicable Law.

5.26 Language

These Terms are executed in the English language. Any translation provided by the Company is for convenience only. In the event of any inconsistency, ambiguity, or conflict between the English version and any translated version, the English version shall prevail to the fullest extent permitted by Applicable Law.

5.27 Dynamic References

Any reference in these Terms to a policy, feature, law, technology, document, standard, service, or process shall be deemed to include its amended, updated, revised, substituted, replaced, successor, or equivalent version, unless the context expressly requires otherwise.

5.28 Interpretation Consistent with Applicable Law

Nothing contained in these Terms shall be interpreted as requiring either Party to perform any act prohibited by Applicable Law. Where any provision is capable of more than one interpretation, it shall be construed in a manner that preserves its validity, legality, enforceability, and commercial purpose to the maximum extent permitted by Applicable Law.

Below is a professionally drafted Part 4, Part 5 and Part 6 in the same enterprise drafting style suitable for a technology platform, e-commerce platform and matrimonial portal. These provisions are designed to work seamlessly with the preceding Definitions and Rules of Interpretation.

6. Acceptance of Terms

6.1 Binding Agreement

These Terms constitute a legally valid and binding electronic agreement between Ramisht Kripa Private

Limited ("Company") and every User accessing or using the Platform. By accessing, browsing, registering on, subscribing to, interacting with, or otherwise using the Platform or any part of the Services, the User acknowledges that the User has carefully read, understood, and voluntarily agreed to be bound by these Terms, together with the Privacy Policy, Refund & Cancellation Policy, Community

Guidelines, Cookie Policy, Website Disclaimer, and every other policy incorporated herein by reference, each of which forms an integral part of this Agreement.

The User further acknowledges that continued access to or use of the Platform after any modification to these Terms shall constitute renewed acceptance of the revised Terms, unless Applicable Law requires fresh or express consent.

6.2 Electronic Acceptance

Acceptance of these Terms may be manifested by any lawful electronic means, including but not limited to creating an Account, clicking an "Accept", "Continue", "Register", "Sign Up", "Login", "Proceed",

"Subscribe", or similar button, completing registration, verifying a mobile number or email address through OTP, making any payment, uploading information, using any feature of the Platform, or otherwise continuing to access or use the Services after these Terms have been made available.

Such acceptance shall constitute valid electronic consent and shall have the same legal force and effect as a handwritten signature or physical execution of a written agreement to the fullest extent permitted under Applicable Law.

6.3 Deemed Acceptance

Where a User accesses or continues to use the Platform without expressly clicking an acceptance button, such access or continued use after reasonable notice of these Terms shall be deemed to constitute acceptance of these Terms, provided that such deemed acceptance is recognised under Applicable Law.

6.4 Authority to Accept

The User represents and warrants that the individual accepting these Terms possesses full legal authority and capacity to bind himself, herself, itself, or the entity on whose behalf the acceptance is made. Where the User accepts these Terms on behalf of a company, partnership, trust, society, government body, or any other legal entity, the individual represents that he or she is duly authorised to bind such entity.

6.5 Continuing Acceptance

Acceptance of these Terms shall continue throughout the period during which the User maintains an

Account, accesses the Platform, receives Services, communicates with the Company, or otherwise benefits from any facility provided through the Platform. Suspension, temporary inactivity, or intermittent use shall not affect the continued applicability of these Terms unless expressly agreed in writing by the Company.

6.6 No Acceptance by Implication of Additional Rights

Acceptance of these Terms shall not create any employment relationship, agency, partnership, joint venture, franchise, fiduciary relationship, or exclusive contractual relationship between the Company and the User except as expressly provided herein.

PART V – ELIGIBILITY, LEGAL CAPACITY & CORPORATE USERS

7. Eligibility

Access to and use of the Platform is permitted only to Persons who possess the legal capacity to enter into a binding contract under Applicable Law. By accessing or using the Platform, every User represents, warrants, and undertakes that the User satisfies all eligibility requirements prescribed by these Terms and Applicable Law.

The Company reserves the absolute right to refuse registration, suspend Services, reject applications, seek additional verification, or terminate any Account where it reasonably believes that a User does not satisfy the eligibility criteria.

8. Legal Capacity

Every User represents and warrants that:

the User has attained the minimum legal age prescribed under Applicable Law to enter into binding contracts; the User is not disqualified from entering into contractual obligations by reason of minority, insolvency, mental incapacity, judicial declaration, statutory prohibition, or any other legal disability;

all information submitted to the Company is true, complete, accurate, and capable of verification; and the User shall immediately notify the Company if any circumstance arises affecting the User's legal capacity to continue using the Platform.

The Company may require documentary proof of identity, age, legal status, or any other information necessary to verify legal capacity.

9. Matrimonial Eligibility

Without prejudice to Applicable Law, every User intending to create a matrimonial profile further represents that: the information relating to marital status, age, identity, religion, education, employment, and other particulars furnished on the Platform is true to the best of the User's knowledge;

the User is legally competent to enter into a valid marriage under Applicable Law;

the User is using the Platform solely for lawful matrimonial purposes; and the User shall not knowingly create false, misleading, duplicate, impersonated, or fraudulent matrimonial profiles.

The Company shall not be responsible for independently verifying every representation made by Users and may rely upon declarations made by them unless circumstances reasonably require additional verification.

10. Corporate, Institutional & Authorised Users

Where the Platform permits access by companies, recruiters, consultants, relationship managers, matrimonial agencies, authorised representatives, government organisations, or other legal entities, such entity represents and warrants that it is duly incorporated or otherwise legally constituted under

Applicable Law; the individual accessing the Platform is duly authorised to bind the entity; all activities performed on behalf of the entity shall be deemed authorised acts of the entity; and the entity shall remain jointly and severally liable for every act or omission committed by its employees, officers, consultants, agents, contractors, representatives, or authorised users while using the Platform. The

Company may require documentary evidence of authorisation at any time.

11. Verification of Eligibility

The Company may, at its sole discretion and at any time, require Users to furnish documents or information necessary to verify eligibility, identity, legal capacity, age, residence, employment, corporate authority, or any other relevant information. Failure to provide satisfactory verification within the prescribed period may result in suspension, restriction, rejection, or termination of access without creating any liability upon the Company.

PART VI – MODIFICATION OF TERMS

12. Modification of Terms

The Company reserves the unrestricted right to amend, revise, modify, replace, supplement, update, discontinue, or otherwise alter these Terms, any incorporated policy, feature, functionality, subscription plan, pricing structure, or Service at any time to reflect changes in Applicable Law, judicial decisions, technological developments, business requirements, security considerations, operational needs, regulatory requirements, or any other legitimate commercial reason.

Where required by Applicable Law or where the Company considers it reasonably appropriate, notice of material modifications shall be provided through the Platform, registered email address, mobile notification, dashboard notification, or any other lawful communication channel. Unless otherwise required by Applicable Law, every modification shall become effective from the date specified by the Company. Continued access to or use of the Platform after such effective date shall constitute the User's acceptance of the modified Terms.

If a User does not agree with any modification, the User's sole and exclusive remedy shall be to discontinue use of the Platform and, where applicable, close the User Account in accordance with these

Terms. Continued use after the effective date shall be deemed conclusive evidence of acceptance.

No employee, consultant, reseller, business partner, customer support executive, marketing representative, or other representative of the Company shall have authority to modify, waive, or vary these Terms except through a written amendment issued by an authorised officer of the Company.

These Terms shall be read together with every policy incorporated by reference, including the Privacy

Policy, Cookie Policy, Refund & Cancellation Policy, Community Guidelines, Website Disclaimer, Intellectual Property Policy, Grievance Redressal Policy, Child Safety Policy, AI Policy (if adopted), and any future policy published by the Company. In the event of any inconsistency, the order of

precedence specified under the Rules of Interpretation shall apply, subject always to Applicable Law.

The Company may maintain previous versions of these Terms for regulatory, evidentiary, compliance, audit, or record-retention purposes. The publication of revised Terms shall not create any obligation upon the Company to continue supporting or applying any earlier version except where expressly required by Applicable Law.

VOLUME II

PRIVACY POLICY

PRELIMINARY PROVISIONS

1. Title

1.1 Privacy Policy

This Privacy Policy ("Privacy Policy" or "Policy") is issued by Ramisht Kripa Private Limited, a company duly incorporated under the provisions of the Companies Act, 2013, having its registered office at

Flat No. 9188, 1st Floor, LIG Flat,B-9 Vasant Kunj New Delhi- 110070 (hereinafter referred to as the "Company", "we", "our", or "us"), and governs the collection, receipt, access, recording, storage, organisation, processing, analysis, sharing, disclosure, transfer, retention, protection, deletion, and other handling of Personal Data and other information relating to every individual or entity accessing or using the website, mobile application, software applications, digital platforms, products, or services operated under the brand name "SarkariHumsafar.com" (collectively referred to as the "Platform").

This Privacy Policy forms an integral and inseparable part of the contractual framework governing the relationship between the Company and every User of the Platform and shall be read together with the

Terms of Use and all other policies published by the Company.

2. Effective Date

2.1 Commencement

This Privacy Policy shall become effective from 14/9/2026 ("Effective Date") and shall remain in force until amended, replaced, withdrawn, or superseded by the Company in accordance with its terms and Applicable Law.

The Company reserves the right to revise or update this Privacy Policy periodically to reflect

changes in

Applicable Law, judicial precedents, regulatory directions, technological developments, cybersecurity requirements, business operations, industry standards, or legitimate business needs. Any revised version shall become effective from the date specified therein unless otherwise required by Applicable Law.

Where required by Applicable Law, reasonable notice of material changes shall be provided through the

Platform, electronic communication, or any other legally recognised means. Continued access to or use of the Platform after the effective date of such revisions shall constitute acknowledgement of the revised

Privacy Policy, subject to Applicable Law.

3. Purpose

3.1 Objective of this Privacy Policy

The primary purpose of this Privacy Policy is to ensure transparency regarding the manner in which the

Company collects, processes, stores, secures, uses, shares, transfers, retains, and otherwise handles

Personal Data and other information entrusted to it by Users or collected during the operation of the

Platform.

This Policy further aims to inform Users of the categories of information collected, the lawful purposes for which such information is processed, the rights available to Data Principals under Applicable Law, the safeguards adopted by the Company to protect Personal Data, the circumstances under which information may be disclosed to third parties or competent authorities, the Company's approach to cybersecurity and incident management, the use of Artificial Intelligence and automated processing systems, the retention and deletion of information, and the procedures through which Users may exercise their privacy-related rights or submit grievances.

The Company is committed to processing Personal Data in a lawful, fair, transparent, proportionate, secure, and accountable manner, while balancing the legitimate interests of the Company, the expectations of Users, and the requirements of Applicable Law.

4. Scope and Applicability

4.1 Persons Covered

This Privacy Policy applies to every individual or entity interacting with the Platform, including registered

Users, prospective Users, visitors, subscribers, premium members, corporate users, authorised representatives, business partners, service providers, vendors, consultants, advertisers, job applicants

(where applicable), and any other person whose Personal Data is collected or processed by or on behalf of the Company in connection with the Platform.

4.2 Activities Covered

This Privacy Policy governs every activity involving the collection or Processing of Personal Data, whether such information is obtained directly from the User, automatically through the use of the Platform, through cookies or similar technologies, from third-party service providers, verification agencies, payment gateways, publicly available sources, government authorities, affiliates, business partners, or any other lawful source.

4.3 Territorial Scope

This Privacy Policy applies irrespective of the geographical location from which the Platform is accessed, subject always to Applicable Law. Where the laws of a particular jurisdiction impose additional obligations upon the Company or confer additional rights upon Users, such obligations and rights shall apply only to the extent legally required.

4.4 Services Covered

This Privacy Policy applies to every website, mobile application, software application, communication channel, customer support service, Artificial Intelligence system, chatbot, digital interface, API, payment facility, verification service, marketing campaign, event, or ancillary service operated, controlled, or made available by the Company unless a separate privacy notice expressly applies.

5. Definitions

Unless the context otherwise requires, every capitalised term used in this Privacy Policy shall have the meaning assigned to it under the Terms of Use. In the event that a term is specifically defined in this

Privacy Policy, such definition shall prevail for the purposes of this Policy to the extent of any inconsistency.

Without limiting the foregoing, expressions such as "Applicable Law", "Personal Data", "Processing",

"Consent", "Data Principal", "Data Fiduciary", "Platform", "User", "Account", "Profile", "Services",

"Cookies", "Artificial Intelligence", "Automated Decision-Making", "Electronic Record", "Digital Evidence", "Security Measures", "Cross-Border Data Transfer", "Confidential Information", "Third-Party

Service Provider", and similar expressions shall bear the meanings assigned to them in the Definitions

Chapter of the Terms of Use.

6. Interpretation

This Privacy Policy shall be interpreted in accordance with the Rules of Interpretation contained in the

Terms of Use, which are incorporated herein by reference. Unless the context otherwise requires, words importing the singular shall include the plural and vice versa, references to one gender shall include every other gender, references to legislation shall include amendments and successor enactments, and references to technology shall include future technological developments.

Headings are inserted solely for convenience and shall not affect interpretation. References to electronic communications, electronic records, digital signatures, click-wrap agreements, AI systems, cloud infrastructure, or other technological concepts shall be construed broadly to ensure that this Privacy

Policy remains effective notwithstanding future technological advancements.

7. Acceptance of this Privacy Policy

By accessing, browsing, registering on, subscribing to, communicating through, or otherwise using the

Platform or any of its Services, the User acknowledges that he, she, or it has read, understood, and voluntarily accepted this Privacy Policy.

Acceptance may be communicated electronically through account registration, clicking an acceptance button, verifying identity by OTP, making a payment, continuing to use the Platform after this Privacy

Policy has been made available, or through any other legally recognised method of electronic acceptance.

Where Applicable Law requires separate or express consent for particular categories of Processing, such consent shall be obtained in accordance with Applicable Law. Withdrawal of consent shall not affect the lawfulness of Processing carried out prior to such withdrawal and may affect the availability of certain

Services where the Processing is necessary for their provision.

8. Relationship with the Terms of Use

This Privacy Policy forms an integral part of the Terms of Use governing access to and use of the Platform.

The Terms of Use, together with this Privacy Policy and every other policy incorporated therein by reference, constitute a unified contractual framework governing the relationship between the Company and the User.

In the event of any inconsistency between this Privacy Policy and the Terms of Use, the specific provisions of this Privacy Policy shall prevail only with respect to matters concerning the collection,

Processing, protection, retention, disclosure, and management of Personal Data. In all other respects, the

Terms of Use shall prevail unless Applicable Law requires otherwise.

Nothing contained in this Privacy Policy shall limit, exclude, or otherwise affect any contractual right, statutory obligation, or legal remedy available to the Company under the Terms of Use or Applicable Law.

9. Contact Details of the Company

For any questions, requests, complaints, grievances, or communications relating to this Privacy Policy or the Company's Processing of Personal Data, Users may contact the Company or its designated Grievance

Officer using the contact details published on the Platform or communicated from time to time.

The Company may designate a Grievance Officer, Data Protection Contact, Compliance Officer, or any other authorised representative as required under Applicable Law. The name, designation, postal address, email address, telephone number, office hours, and grievance redressal procedure of such authorised representative shall be published on the Platform and may be updated from time to time.

Users are encouraged to first contact the Company through the prescribed grievance mechanism before initiating any external complaint or legal proceeding, without prejudice to any statutory rights available under Applicable Law.

PERSONAL DATA WE COLLECT

PART I – PERSONAL INFORMATION, IDENTITY INFORMATION, PROFILE INFORMATION,
CONTACT INFORMATION & MATRIMONIAL INFORMATION

The Company may collect additional categories of information where such collection is lawful, necessary, proportionate, and consistent with the purposes described in this Privacy Policy or otherwise permitted under Applicable Law.

2. PERSONAL DATA WE COLLECT

The Company may collect, receive, generate, observe, infer, verify, record, organise, store, retrieve, use, analyse, combine, disclose, transfer, archive, anonymise, pseudonymise, delete, or otherwise Process

Personal Data relating to Users in connection with the provision, operation, administration, security, improvement, and lawful functioning of the Platform.

The categories of Personal Data described below are collected directly from Users, automatically through the Platform, from third-party service providers, verification agencies, payment intermediaries, publicly available sources, Artificial Intelligence systems, or other lawful sources, depending upon the nature of the Services used by the User.

2.1 Personal Information

The Company may collect Personal Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable individual.

Such Personal Information may include the User's full name, maiden name, nickname, preferred name, display name, username, gender, date of birth, age, marital status, nationality, religion, caste or community (where voluntarily provided for matrimonial matching), mother tongue, educational qualifications, occupation, employment details, annual income or income range, lifestyle preferences, interests, hobbies, family background, personal preferences, relationship expectations, photographs, videos, voice recordings, signatures, profile descriptions, and any other information voluntarily submitted by the User during registration or while using the Platform.

The Company may also collect any additional Personal Information that the User voluntarily provides through profile updates, customer support interactions, surveys, promotional campaigns, contests, testimonials, reviews, feedback forms, verification processes, or any other interaction with the Platform.

The Company shall Process such Personal Information solely for lawful purposes, including account creation, profile management, identity verification, matchmaking, customer support, fraud prevention, legal compliance, Platform improvement, security, analytics, research, and

other purposes described in this Privacy Policy.

2.2 Identity Information

The Company may collect and Process information necessary to establish, verify, authenticate, or confirm the identity of a User.

Identity Information may include the User's legal name, date of birth, age, gender, photograph, government-issued identity details, digital identity credentials, verification status, facial images voluntarily submitted for verification, selfie verification images, video verification recordings, digital signatures, authentication credentials, identity confirmation records, verification timestamps, verification history, risk assessment indicators, fraud screening results, identity confidence scores generated through automated systems, and any other information reasonably required to verify the authenticity of the User.

The Company may obtain Identity Information directly from the User, authorised verification partners, publicly available government records where legally permitted, regulated verification service providers, or other lawful sources.

Identity verification may be conducted manually, electronically, or through Artificial Intelligence-assisted verification systems. Successful verification does not constitute a guarantee regarding the User's identity, character, conduct, intentions, or suitability for matrimonial purposes, and the Company disclaims any representation or warranty in this regard except as expressly required under Applicable Law.

2.3 Profile Information

The Company may collect, create, maintain, organise, and Process Profile Information relating to every

User for the purpose of operating the Platform and facilitating lawful matrimonial interactions.
Profile

Information may include profile photographs, profile videos, profile descriptions, educational qualifications, professional details, employer information, occupation, salary or income range, physical characteristics, religion, caste, community, sub-caste, mother tongue, nationality, citizenship, family details, lifestyle choices, dietary preferences, smoking or drinking habits, disability status (where voluntarily disclosed), horoscope details, astrological preferences, relationship expectations, preferred partner criteria, residential preferences, language preferences, interests, hobbies, social preferences, verification badges, membership status, subscription details, profile visibility settings, search preferences, profile activity history, account status, compatibility indicators, AI-generated profile insights, profile completion percentage, and

every other profile-related information voluntarily provided or generated through use of the Platform.

The User acknowledges that certain Profile Information may be displayed to other Users in accordance with the User's privacy settings, profile visibility preferences, applicable subscription plan, and the operational functionality of the Platform.

The Company reserves the right to categorise, index, organise, recommend, rank, analyse, or otherwise Process Profile Information using automated systems, Artificial Intelligence technologies, recommendation engines, compatibility algorithms, behavioural analytics, or similar technologies for the purposes described in this Privacy Policy.

2.4 Contact Information

The Company may collect Contact Information necessary to communicate with the User, administer the User's Account, deliver Services, comply with legal obligations, maintain security, and provide customer support.

Contact Information may include residential address, permanent address, correspondence address, city, district, State, country, postal code, mobile number, alternate mobile number, landline number, email address, alternate email address, emergency contact details, communication preferences, preferred language of communication, notification preferences, messaging identifiers, and any other contact-related information voluntarily provided by the User.

The Company may verify Contact Information through one-time passwords (OTP), email verification, mobile verification, postal verification, third-party verification services, automated communication systems, or any other lawful verification mechanism.

The User shall remain responsible for ensuring that Contact Information remains complete, accurate, current, and updated. The Company shall not be responsible for any consequences arising from inaccurate, incomplete, outdated, or incorrect Contact Information supplied by the User.

2.5 Matrimonial Information

As a specialised matrimonial Platform, the Company may collect, Process, organise, analyse, display, verify, and use Matrimonial Information voluntarily submitted by the User for the primary purpose of facilitating matrimonial matchmaking and related Services.

Matrimonial Information may include marital status, previous marriages, divorce status, judicial separation, widow or widower status, number of children, family structure, family values, family occupation, family income range, educational background of family members, parental details,

siblings' details, cultural background, religion, caste, sub-caste, community, gotra, horoscope information, astrological preferences, nakshatra, manglik status, kundli details, lifestyle preferences, dietary preferences, health-related disclosures voluntarily provided by the User, disability information voluntarily disclosed, expectations regarding prospective life partners, preferred age range, preferred education, occupation preferences, geographical preferences, language preferences, relocation preferences, citizenship preferences, immigration preferences, matrimonial photographs, matrimonial videos, introduction recordings, references, matrimonial verification status, profile preferences, compatibility preferences, and every other information voluntarily submitted for matrimonial purposes.

The User acknowledges and agrees that the submission of Matrimonial Information is voluntary except where specific information is reasonably necessary for the provision of particular Services. The

Company shall Process such information in accordance with the User's privacy settings, consent preferences, subscription plan, and Applicable Law.

The Company may utilise Artificial Intelligence systems, automated recommendation engines, behavioural analytics, compatibility assessment tools, machine learning models, and other technological solutions to analyse Matrimonial Information for generating recommendations, improving search results, suggesting compatible profiles, detecting suspicious activities, preventing fraud, enhancing user experience, and improving the overall effectiveness of the Platform. Such recommendations are probabilistic in nature, do not constitute professional advice or guarantees of compatibility, and should not be relied upon as the sole basis for making matrimonial decisions.

Users are solely responsible for the accuracy, completeness, authenticity, legality, and currency of the Matrimonial Information submitted by them. The Company does not independently verify every statement made by Users unless expressly stated or required for a particular verification service and shall not be liable for any inaccuracy, omission, misrepresentation, concealment, or fraudulent disclosure made by any User, except to the extent required under Applicable Law.

The Company may retain historical versions of Matrimonial Information, profile modifications, verification records, and related metadata for security purposes, fraud prevention, legal compliance, audit requirements, dispute resolution, regulatory obligations, enforcement of contractual rights, maintenance of Digital Evidence, and other lawful purposes in accordance with the Company's Data Retention Policy and Applicable Law.

PART II – GOVERNMENT IDENTIFICATION, PAYMENT INFORMATION, COMMUNICATION

RECORDS, USER CONTENT & DEVICE INFORMATION

2.6 Government Identification Information

The Company may collect, receive, verify, record, Process, store, encrypt, retain, and otherwise handle

Government Identification Information where such collection is necessary for identity verification, fraud prevention, regulatory compliance, dispute resolution, account security, prevention of impersonation, lawful verification services, or any other lawful purpose permitted under Applicable Law.

Government Identification Information may include the type of identification document, document number (whether in full, masked, tokenised, or partially redacted form), issuing authority, date of issue, date of expiry, photograph appearing on the document, biometric photograph voluntarily submitted by the User for comparison, verification status, verification reference number, digitally generated verification tokens, authentication logs, timestamps, and any information reasonably necessary to establish the authenticity of the User's identity.

Depending upon the Services used, such information may relate to documents including passport, driving licence, voter identity card, Permanent Account Number (PAN), Aadhaar or any officially valid document recognised under Applicable Law, provided that the Company shall collect, Process, store, or authenticate such documents only where legally permissible and only to the extent necessary for the specific purpose for which they are collected.

Where identity verification is performed through authorised third-party verification agencies, regulated identity service providers, payment intermediaries, or governmental interfaces, the User authorises the

Company to securely transmit the minimum information necessary for carrying out such verification.

The Company does not guarantee the accuracy or continued validity of any Government Identification

Information supplied by the User or verified through third-party systems.

Government Identification Information shall be protected using appropriate technical and organisational security measures, including encryption, restricted access controls, audit logging, role-based access, secure transmission protocols, and retention controls proportionate to the sensitivity of such information.

The Company shall not publicly display Government Identification Information except where expressly authorised by the User or required under Applicable Law.

2.7 Payment Information

The Company may collect, receive, Process, record, reconcile, retain, and analyse Payment Information necessary for processing subscriptions, membership fees, premium services, purchases, refunds, renewals, chargebacks, taxation, accounting, fraud prevention, regulatory compliance, financial audits, and other legitimate commercial purposes.

Payment Information may include the transaction amount, payment method, payment instrument type, payment reference number, invoice details, subscription details, billing address, payment timestamps, merchant transaction identifiers, order numbers, refund history, recurring payment mandates, wallet utilisation, promotional credits, taxation information, GST details where applicable, bank reference numbers, payment gateway identifiers, and other information generated during the payment process.

The Company generally does not collect or permanently store complete debit card numbers, credit card numbers, CVV numbers, PINs, internet banking passwords, UPI PINs, or similar confidential authentication credentials unless expressly permitted by Applicable Law and required for a specific lawful purpose.

Electronic payment transactions may be processed through licensed Payment Service Providers, payment gateways, banks, financial institutions, payment aggregators, card networks, or other authorised intermediaries. Such entities may independently collect and Process payment-related information in accordance with their own privacy policies, contractual terms, and regulatory obligations, for which the

Company shall not be responsible except to the extent required by Applicable Law.

The Company may retain payment transaction records, invoices, taxation records, settlement records, refund records, chargeback records, accounting entries, and audit trails for the duration required under

Applicable Law, contractual obligations, accounting standards, taxation requirements, fraud investigations, legal proceedings, or dispute resolution.

2.8 Communication Records

The Company may collect, record, monitor, archive, analyse, and retain Communications exchanged between the User and the Company or generated through the use of the Platform where such Processing is necessary for providing Services, ensuring Platform security, maintaining service quality, resolving disputes, complying with legal obligations, or protecting the legitimate interests of the Company.

Communication Records may include customer support requests, grievance submissions, emails,

chat conversations, chatbot interactions, AI-assisted conversations, support tickets, SMS communications, in- application messages, push notifications, WhatsApp communications where supported, telephone call recordings, voice messages, video conference recordings, feedback forms, survey responses, complaint records, review submissions, moderation records, communication metadata, timestamps, delivery confirmations, read receipts, authentication messages, verification communications, and every other communication exchanged through or in connection with the Platform.

Where legally permissible, telephone calls, customer support interactions, online meetings, verification calls, or video verification sessions may be recorded for quality assurance, employee training, fraud prevention, dispute resolution, security monitoring, evidentiary purposes, regulatory compliance, and improvement of customer services.

The Company may also generate internal communication records, moderation logs, investigation reports, escalation notes, customer relationship records, and AI-generated summaries solely for lawful operational purposes.

Users acknowledge that Communications transmitted through electronic systems may contain metadata, technical information, timestamps, routing information, and system-generated records, which may be retained as Digital Evidence in accordance with this Privacy Policy.

2.9 User Content

The Company may collect, host, Process, analyse, index, display, transmit, reproduce, temporarily store, archive, moderate, or otherwise handle User Content voluntarily submitted, uploaded, transmitted, published, shared, or otherwise made available by Users through the Platform.

User Content may include profile descriptions, biographies, matrimonial preferences, photographs, videos, audio recordings, voice messages, profile updates, testimonials, reviews, ratings, comments, chat messages, discussion posts, introductions, verification documents, profile images, family photographs, event participation records, questionnaires, feedback, survey responses, documents uploaded for verification, complaint materials, grievance submissions, and any other content generated or submitted by the User.

The Company may utilise automated moderation tools, Artificial Intelligence systems, image recognition technologies, natural language processing systems, spam detection mechanisms, fraud detection systems, malware detection technologies, and human moderators to review, categorise, filter, moderate, detect prohibited content, enforce community standards, identify policy violations, improve Platform safety, and comply with Applicable Law.

The User represents and warrants that all User Content submitted to the Platform is accurate, lawful, authentic, non-infringing, and does not violate the rights of any third party. The User remains solely responsible for every item of User Content submitted to the Platform.

The Company does not claim ownership of User Content except to the limited extent necessary to operate, maintain, secure, improve, promote, backup, archive, moderate, and lawfully provide the Services in accordance with the licence granted under the Terms of Use.

The Company reserves the right, but not the obligation, to remove, restrict, suspend, archive, preserve, investigate, or disclose User Content where it reasonably believes such action is necessary to enforce these Terms, comply with Applicable Law, protect Users, prevent fraud, investigate misconduct, preserve

Digital Evidence, or respond to lawful requests from competent authorities.

2.10 Device Information

The Company may automatically collect, generate, receive, observe, analyse, and Process technical information relating to the devices used by Users to access the Platform for purposes including authentication, cybersecurity, fraud prevention, service optimisation, analytics, troubleshooting, personalisation, risk assessment, regulatory compliance, and Platform improvement.

Device Information may include Internet Protocol (IP) address, device identifiers, device model, manufacturer, operating system, browser type, browser version, language settings, device configuration, application version, screen resolution, network information, SIM information where available, device security status, hardware identifiers, software identifiers, unique device tokens, advertising identifiers where permitted, browser fingerprint, digital fingerprint, cookie identifiers, session identifiers, authentication logs, crash reports, error logs, system diagnostics, battery status where relevant, network latency, connection quality, time zone, device location derived from technical information, operating system permissions, application installation details, and similar technical information.

The Company may use Device Information to identify suspicious activities, prevent unauthorised access, detect multiple or duplicate accounts, monitor unusual login behaviour, recognise trusted devices, improve system performance, personalise user experience, optimise application functionality, investigate cybersecurity incidents, comply with regulatory obligations, generate analytics, and maintain the overall security and integrity of the Platform.

The Company may combine Device Information with other categories of Personal Data where such combination is reasonably necessary for fraud prevention, account security, lawful

verification, service delivery, or other legitimate purposes permitted under Applicable Law.

Users acknowledge that certain Device Information is automatically generated whenever electronic devices communicate with internet-based services and that disabling certain technical features may affect the availability, functionality, security, or performance of the Platform.

2.11 General Provisions Applicable to this Part

The categories of information described in this Part are illustrative and not exhaustive. Depending upon the nature of the Services used, the User's interactions with the Platform, applicable subscription plans, technological developments, security requirements, regulatory obligations, or lawful business needs, the

Company may collect additional categories of information that are reasonably necessary, proportionate, and consistent with the purposes described in this Privacy Policy or otherwise permitted under Applicable

Law.

The Company shall implement appropriate technical, organisational, contractual, and administrative safeguards to protect the confidentiality, integrity, availability, authenticity, and security of the information collected under this Chapter. Access to such information shall be restricted to authorised personnel, service providers, and other recipients strictly on a need-to-know basis and subject to appropriate confidentiality, security, and legal obligations.

Nothing contained in this Chapter shall be construed as requiring the Company to collect every category of information described herein. The actual categories of information collected shall depend upon the specific Services requested by the User, the functionality used, applicable legal requirements, and the operational needs of the Platform. Information that is not reasonably necessary for the provision of

Services or compliance with Applicable Law shall not be collected unless voluntarily provided by the User or otherwise authorised by law.

PART III – COOKIES & TRACKING TECHNOLOGIES, LOCATION DATA, USAGE ANALYTICS, AI-GENERATED INFORMATION & VERIFICATION DATA

2.12 Cookies & Tracking Technologies

The Company may use Cookies and similar tracking technologies to recognise Users, authenticate

Accounts, enhance Platform functionality, remember User preferences, personalise content, improve security, analyse Platform performance, detect fraud, measure advertising effectiveness, conduct research, and improve the overall quality and reliability of the Services.

Cookies may include session cookies, persistent cookies, authentication cookies, security cookies, functional cookies, preference cookies, performance cookies, analytics cookies, advertising cookies, affiliate tracking cookies, conversion tracking cookies, load-balancing cookies, consent management cookies, device recognition cookies, and any other similar technologies developed in the future.

In addition to Cookies, the Company may use web beacons, tracking pixels, software development kits

(SDKs), embedded scripts, browser local storage, HTML5 storage, cache technologies, application identifiers, fingerprinting technologies, digital tokens, server-side tracking mechanisms, API integrations, event logging systems, and similar technologies for operational, analytical, cybersecurity, fraud prevention, and service improvement purposes.

These technologies may automatically collect information including browser type, operating system, IP address, device identifiers, session identifiers, pages visited, referral URLs, search terms, clicks, interactions, page response times, download errors, browsing behaviour, feature usage, advertising interactions, application performance metrics, and similar technical information.

Users may manage certain Cookie preferences through browser settings, operating system controls, consent management tools, or Platform settings where available. However, disabling Cookies or similar technologies may affect the availability, security, performance, functionality, or user experience of certain features of the Platform.

The Company may also permit carefully selected third-party analytics providers, advertising partners, cloud service providers, security vendors, or other authorised service providers to use Cookies or similar technologies strictly for the purposes authorised by the Company and subject to contractual confidentiality, privacy, and security obligations.

2.13 Location Data

The Company may collect, generate, infer, receive, or Process Location Data for the purpose of providing location-based services, improving matchmaking results, enhancing user experience, detecting fraud, maintaining cybersecurity, complying with legal obligations, and improving Platform functionality.

Location Data may include precise location information, approximate location information, GPS coordinates, IP-based geolocation, Wi-Fi positioning data, Bluetooth proximity information, cell tower information, regional preferences, city, district, State, country, postal code, travel history voluntarily shared by the User, device-derived location estimates, and any other geographical

information reasonably associated with the User's use of the Platform.

Where precise Location Data is collected through mobile devices or similar technologies, the Company shall obtain appropriate permissions or consent as required under Applicable Law and the operating system of the User's device.

The Company may use Location Data to recommend nearby events or services, improve profile matching, personalise search results, verify account authenticity, detect suspicious login attempts, identify unusual account activity, prevent fraudulent transactions, comply with jurisdictional requirements, and maintain the security and integrity of the Platform.

Users may control the collection of certain categories of Location Data by modifying device settings, browser permissions, operating system permissions, or application permissions. Restricting access to

Location Data may limit the availability or functionality of certain Platform features.

2.14 Usage Analytics

The Company may automatically collect, generate, compile, analyse, and Process Usage Analytics to understand how Users interact with the Platform, evaluate Platform performance, improve Services, develop new features, optimise business operations, detect fraud, maintain cybersecurity, and fulfil regulatory obligations.

Usage Analytics may include login frequency, session duration, navigation paths, clickstream data, page views, search queries, profile visits, feature utilisation, interaction history, advertisement engagement, subscription behaviour, transaction patterns, communication frequency, device usage patterns, crash reports, error logs, performance metrics, latency information, network quality indicators, diagnostic reports, user preferences, behavioural trends, and similar analytical information.

The Company may generate aggregated, anonymised, pseudonymised, statistical, predictive, or derived analytical datasets from Usage Analytics for research, reporting, benchmarking, product development, operational planning, capacity management, fraud detection, Artificial Intelligence model improvement, cybersecurity monitoring, and other legitimate business purposes.

Where reasonably possible, the Company shall use anonymisation or pseudonymisation techniques before analysing information that is not required to identify individual Users.

The Company may use third-party analytics providers to assist in collecting and analysing Usage Analytics, provided such providers are subject to appropriate contractual obligations regarding confidentiality, privacy, information security, and Applicable Law

2.15 AI-Generated Information

The Company may utilise Artificial Intelligence systems, machine learning models, recommendation engines, predictive analytics, intelligent automation, natural language processing systems, computer vision technologies, behavioural analytics, fraud detection systems, and other automated technologies to generate, infer, analyse, organise, classify, score, recommend, or otherwise Process information relating to the operation of the Platform and the provision of Services.

AI-Generated Information may include compatibility scores, profile recommendations, search rankings, profile quality assessments, verification confidence scores, behavioural insights, fraud risk indicators, spam detection results, duplicate account detection, content moderation outcomes, language translations, automated summaries, suggested profile improvements, customer support responses, security alerts, anomaly detection reports, predictive analytics, recommendation outputs, account trust scores, and other information generated wholly or partly through automated computational processes.

Such AI-Generated Information may be created using Personal Data, Profile Information, Device Information, Usage Analytics, Verification Data, User Content, Communication Records, technical logs, metadata, and other information lawfully Processed by the Company.

The Company shall endeavour to design, develop, deploy, monitor, and improve Artificial Intelligence systems in a manner that promotes accuracy, fairness, security, transparency, accountability, and compliance with Applicable Law. However, Users acknowledge that AI systems are probabilistic by nature and may occasionally generate inaccurate, incomplete, biased, outdated, or incorrect outputs.

Accordingly, AI-generated recommendations, compatibility assessments, rankings, predictions, summaries, and similar outputs are intended solely to assist Users and shall not constitute legal advice, professional advice, matrimonial guarantees, factual certifications, or binding decisions. Users remain solely responsible for exercising independent judgment before relying upon AI-generated outputs.

The Company reserves the right to review, override, modify, suspend, or manually verify AI-generated outputs where necessary to maintain fairness, security, legal compliance, customer protection, or operational integrity.

2.16 Verification Data

The Company may collect, generate, receive, verify, retain, and Process Verification Data for the purposes of establishing the authenticity of Users, enhancing trust, preventing fraud, detecting impersonation, complying with regulatory obligations, improving Platform safety, and

maintaining the integrity of matrimonial interactions.

Verification Data may include identity verification records, document verification results, selfie verification records, facial comparison results, video verification records, email verification status, mobile verification status, OTP verification records, biometric comparison results where legally permitted, verification timestamps, verification reference numbers, digital verification certificates, third-party verification responses, fraud screening reports, account authenticity indicators, risk assessment scores, trust ratings, verification history, investigation records, moderation decisions, and every other record generated during verification processes.

Verification activities may be conducted directly by the Company or through authorised third-party verification agencies, technology providers, payment intermediaries, government-authorised databases where legally permissible, identity verification platforms, cybersecurity vendors, or other service providers engaged by the Company.

The Company may retain Verification Data for reasonable periods necessary to comply with Applicable

Law, investigate fraudulent activities, respond to legal proceedings, resolve disputes, preserve Digital

Evidence, conduct compliance audits, enforce contractual rights, maintain cybersecurity, improve verification systems, and fulfil regulatory obligations.

Successful verification of a User or Profile shall indicate only that specified verification procedures were completed based on the information available at the relevant time. Such verification shall not constitute a guarantee, warranty, certification, endorsement, recommendation, or representation regarding the

User's character, conduct, intentions, matrimonial suitability, financial condition, reputation, or future behaviour.

2.17 General Provisions Applicable to Technical and Analytical Information

The Company may combine Cookies, tracking information, Location Data, Usage Analytics, AI-Generated

Information, Verification Data, Device Information, Metadata, Digital Evidence, Communication Records,

User Content, and other categories of information described in this Privacy Policy where such Processing is reasonably necessary for account authentication, cybersecurity, fraud prevention, service delivery,

Platform optimisation, Artificial Intelligence development, customer support, dispute resolution,

legal compliance, regulatory reporting, or other legitimate purposes permitted under Applicable Law.

Where practicable and consistent with the intended purpose of Processing, the Company may anonymise, aggregate, pseudonymise, tokenise, encrypt, or otherwise de-identify technical and analytical information before using it for research, statistical analysis, product development, artificial intelligence training, security testing, quality assurance, business intelligence, or other lawful operational purposes.

The Company shall implement appropriate technical and organisational safeguards, including encryption, access controls, audit logging, monitoring systems, intrusion detection mechanisms, secure communication protocols, vulnerability management processes, and periodic security assessments, to protect the confidentiality, integrity, availability, and authenticity of the information collected under this

Part.

Nothing contained in this Part shall be interpreted as obligating the Company to collect every category of technical or analytical information described herein. The actual categories of information collected shall depend upon the User's interactions with the Platform, the Services utilised, device configurations, operating system permissions, browser settings, applicable subscription plans, technological capabilities, legal requirements, and the operational needs of the Company. Information shall be collected only to the extent reasonably necessary, proportionate, and lawful for the purposes described in this Privacy Policy or otherwise authorised under Applicable Law.

PART IV – SOCIAL MEDIA INFORMATION, THIRD-PARTY DATA, METADATA, DIGITAL EVIDENCE, SENSITIVE INFORMATION & INFORMATION COLLECTED AUTOMATICALLY

Professional Drafting Note: This Part governs the collection, receipt, generation, observation, storage,

Processing, disclosure, retention, protection, and lawful use of information originating from social media platforms, third-party sources, metadata, digital evidence, sensitive information, and information collected automatically through the operation of the Platform. These provisions are intended to ensure transparency while protecting the legitimate interests of the Company and complying with the Digital

Personal Data Protection Act, 2023, the Information Technology Act, 2000, the CERT-In Directions, and other Applicable Laws.

2.18 Social Media Information

The Company may collect, receive, access, verify, analyse, Process, store, and otherwise handle information that the User voluntarily provides or authorises the Company to obtain through social networking platforms, social media services, messaging platforms, professional networking platforms, content-sharing platforms, or other third-party online services.

Such Social Media Information may include the User's display name, username, profile photograph, email address, verified status, profile URL, publicly available profile information, profile biography, interests, language preferences, social login credentials (excluding passwords), profile visibility settings, publicly shared content, profile verification indicators, social media identifiers, communication preferences, publicly available connections where authorised, and other information that the User has chosen to make available through the relevant third-party platform.

Where the Platform permits registration or authentication through social login services, the Company may receive information from the relevant provider in accordance with the permissions granted by the

User and the privacy settings maintained on that platform.

The Company shall access only such information as is authorised by the User, made publicly available by the User, or otherwise lawfully available under Applicable Law and the applicable policies of the third- party platform.

The Company shall not be responsible for the privacy practices, security measures, availability, functionality, policies, or actions of any third-party social media platform. Users are encouraged to review the privacy policies and terms of use of such platforms before connecting their accounts to the Platform.

The Company may discontinue, suspend, or modify social media integrations at any time without prior notice where necessary for operational, security, legal, or commercial reasons.

2.19 Third-Party Data

The Company may receive, collect, generate, verify, combine, or otherwise Process Personal Data and other information obtained from lawful third-party sources for the purpose of providing Services, improving Platform functionality, preventing fraud, complying with Applicable Law, enhancing security, conducting verification, and protecting the legitimate interests of the Company and its Users.

Third-Party Data may be obtained from payment service providers, identity verification agencies, government authorities where legally authorised, business partners, marketing partners, advertising networks, analytics providers, cloud service providers, cybersecurity

vendors, fraud prevention agencies, recruitment agencies, public databases, publicly available sources, financial institutions, customer support providers, communication service providers, technology vendors, data processors, affiliates, subsidiaries, and every other lawful source authorised under Applicable Law.

Such information may include identity verification responses, payment confirmations, fraud indicators, transaction confirmations, authentication results, publicly available profile information, demographic information, risk assessments, compliance reports, service usage information, communication records, verification certificates, or any other information reasonably necessary for the lawful operation of the Platform.

Where Third-Party Data is received, the Company shall Process such information only for lawful purposes, subject to contractual obligations, applicable privacy laws, and reasonable security safeguards.

The Company shall not be responsible for the accuracy, completeness, reliability, legality, or continued availability of information supplied by independent third parties, except to the extent required under Applicable Law.

2.20 Metadata

The Company may automatically generate, collect, observe, analyse, store, retain, and Process Metadata created through the operation of the Platform, electronic communications, digital transactions, authentication systems, Artificial Intelligence systems, verification processes, and other technological interactions.

Metadata may include timestamps, file properties, communication routing information, transmission records, document identifiers, server logs, audit trails, browser information, application identifiers, device fingerprints, digital signatures, authentication logs, transaction identifiers, access history, session identifiers, event logs, API request logs, IP addresses, geolocation estimates, file creation dates, modification history, communication headers, delivery confirmations, read receipts, encryption information, system-generated identifiers, network information, and every other technical information generated as a consequence of electronic processing.

Metadata may not always directly identify an individual when viewed independently; however, when combined with other information available to the Company, it may constitute Personal Data under

Applicable Law.

The Company may Process Metadata for purposes including cybersecurity, fraud prevention, forensic investigations, regulatory compliance, dispute resolution, system administration, service optimisation,

Artificial Intelligence model improvement, business analytics, audit requirements, legal proceedings,

Digital Evidence preservation, and operational continuity.

2.21 Digital Evidence

The Company may create, preserve, collect, maintain, archive, retrieve, analyse, disclose, and otherwise

Process Digital Evidence where reasonably necessary for protecting the Company, Users, the Platform, or complying with Applicable Law.

Digital Evidence may include Electronic Records, audit trails, authentication logs, login history, communication records, payment records, transaction logs, verification records, IP logs, device identifiers, browser fingerprints, server logs, access records, system logs, CCTV recordings (where applicable), customer support records, Artificial Intelligence decision logs, moderation records, investigation reports, fraud detection records, metadata, digital signatures, blockchain records (where implemented), electronic documents, uploaded files, photographs, audio recordings, video recordings, deleted content retained under lawful preservation obligations, and every other electronically stored information capable of evidentiary use.

The Company may preserve Digital Evidence beyond ordinary data retention periods where necessary for litigation, arbitration, mediation, regulatory investigations, governmental inquiries, law enforcement requests, fraud investigations, contractual enforcement, cybersecurity incidents, legal holds, compliance audits, or the protection of legal rights.

The Company reserves the right to establish legal hold procedures whereby relevant Electronic Records and Digital Evidence may be preserved notwithstanding any ordinary deletion or retention schedule.

Nothing contained in this Privacy Policy shall obligate the Company to disclose Digital Evidence except where required under Applicable Law, judicial order, lawful governmental direction, contractual obligation, or where disclosure is reasonably necessary to protect the legal rights, safety, security, or property of the Company or any person.

2.22 Sensitive Information

The Company recognises that certain categories of Personal Data may require enhanced

protection due to their nature and sensitivity.

Where applicable and permitted under Applicable Law, Sensitive Information may include government- issued identification details, financial account information, biometric information voluntarily submitted for verification, photographs used for identity verification, health-related information voluntarily disclosed by the User, disability information voluntarily provided, religious affiliation, caste or community information voluntarily furnished for matrimonial matching, marital history, divorce records voluntarily submitted, information relating to children voluntarily disclosed, and any other category of information designated as sensitive under Applicable Law.

The Company shall collect Sensitive Information only where such collection is reasonably necessary for providing Services, complying with legal obligations, preventing fraud, conducting lawful verification, protecting Users, or where the User voluntarily provides such information for matrimonial or related purposes.

Sensitive Information shall be subject to enhanced technical, organisational, contractual, and administrative safeguards, including encryption, role-based access controls, strict confidentiality obligations, secure transmission protocols, access logging, periodic security reviews, and restricted retention periods appropriate to the nature of the information.

The Company shall not intentionally collect or Process Sensitive Information beyond what is reasonably necessary for the purposes described in this Privacy Policy or otherwise authorised by Applicable Law.

Where Applicable Law requires explicit consent for the Processing of specific categories of Sensitive Information, the Company shall obtain such consent before commencing the relevant Processing activities.

2.23 Information Collected Automatically

In addition to information voluntarily submitted by Users, the Company may automatically collect, observe, generate, infer, analyse, record, and Process information whenever a User accesses, browses, registers on, communicates through, or otherwise interacts with the Platform.

Automatically collected information may include technical identifiers, browser characteristics, operating system information, device configuration, IP address, internet service provider details, application version, language preferences, network information, browsing behaviour, search history within the

Platform, clickstream data, page response times, crash reports, session duration, authentication records, feature usage statistics, communication logs, advertising interactions, referral URLs, cookie identifiers, event logs, security events, error diagnostics, performance metrics, Device Information, Metadata, Usage

Analytics, approximate location information, AI interaction records, verification events, and every other information automatically generated through the normal operation of internet-based technologies.

Such information may be collected through Cookies, SDKs, APIs, server logs, web beacons, tracking pixels, browser storage, Artificial Intelligence systems, cybersecurity tools, fraud detection technologies, cloud infrastructure, analytics platforms, and other technologies reasonably necessary for the secure and efficient operation of the Platform.

Automatically collected information may be combined with other categories of information described in this Privacy Policy where such Processing is reasonably necessary for authentication, personalisation, cybersecurity, fraud detection, service optimisation, compliance, analytics, customer support, Artificial

Intelligence development, dispute resolution, legal compliance, or other lawful purposes.

2.24 General Provisions Applicable to this Chapter

The categories of information described in this Chapter are intended to be comprehensive but illustrative in nature and shall not be interpreted as an exhaustive list of every category of information that may be

Processed by the Company. Depending upon the Services used, technological developments, operational requirements, security considerations, regulatory obligations, or lawful business needs, the Company may collect and Process additional categories of information that are reasonably necessary, proportionate, transparent, and consistent with the purposes described in this Privacy Policy or otherwise authorised under Applicable Law.

The Company shall implement appropriate technical and organisational measures designed to protect the confidentiality, integrity, availability, authenticity, and resilience of all Personal Data and related information Processed under this Chapter. Such measures may include encryption of data at rest and in transit, pseudonymisation or anonymisation where appropriate, multi-factor authentication, role-based access controls, continuous security monitoring, vulnerability assessments, penetration testing, audit logging, incident response procedures, disaster recovery mechanisms, secure software development practices, periodic employee training, contractual confidentiality obligations, and regular reviews of information security controls.

The Company shall Process Personal Data in accordance with the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability, to the extent applicable under the Digital Personal Data Protection

Act, 2023, the Information Technology Act, 2000, and other Applicable Laws. Nothing contained in this Chapter shall be construed as authorising the Company to collect information that is unnecessary, disproportionate, or otherwise prohibited by Applicable Law.

SOURCES OF DATA COLLECTION

3. SOURCES OF DATA COLLECTION

The Company may collect, receive, generate, observe, infer, verify, or otherwise obtain Personal Data and related information from multiple lawful sources in connection with the operation of the Platform, the provision of Services, regulatory compliance, fraud prevention, cybersecurity, dispute resolution, research, analytics, and other legitimate business purposes.

The categories described in this Chapter are illustrative and not exhaustive. Depending upon the nature of the Services, technological developments, legal requirements, or operational needs, the Company may obtain information from additional lawful sources consistent with this Privacy Policy and Applicable Law.

3.1 Direct Collection

The Company may collect Personal Data directly from Users whenever they voluntarily interact with the

Platform or communicate with the Company.

Direct Collection may occur during account registration, profile creation, identity verification, subscription purchase, payment transactions, profile updates, uploading photographs or documents, participation in surveys, contests, promotional campaigns, matrimonial events, webinars, customer support interactions, grievance submissions, interviews, verification calls, feedback forms, review submissions, AI-assisted conversations, chatbot interactions, community forums, or any other communication with the Company.

Information may also be collected when Users submit forms, execute electronic agreements, provide declarations, upload verification documents, complete questionnaires, communicate with customer support representatives, or otherwise voluntarily disclose information to obtain or improve Services.

Users remain solely responsible for ensuring that the information directly provided is accurate, complete, lawful, current, and not misleading.

3.2 Automatic Collection

The Company may automatically collect technical, behavioural, operational, security-related, and analytical information whenever a User accesses, browses, registers on, communicates through, or otherwise interacts with the Platform.

Automatic Collection may occur through Cookies, web beacons, pixels, SDKs, APIs, browser storage, server logs, authentication systems, mobile applications, operating systems, cloud infrastructure, fraud detection technologies, Artificial Intelligence systems, cybersecurity monitoring tools, performance monitoring systems, application diagnostics, and similar technologies.

Automatically collected information may include Device Information, IP addresses, browser characteristics, operating system information, application identifiers, usage patterns, search history within the Platform, session duration, authentication logs, performance metrics, communication metadata, approximate location information, crash reports, event logs, security alerts, referral URLs, clickstream information, and every other category of automatically generated information described in this Privacy Policy.

Such collection is undertaken to maintain Platform functionality, improve user experience, enhance cybersecurity, detect fraud, optimise performance, comply with legal obligations, and support legitimate business operations.

3.3 Third-Party Sources

The Company may receive Personal Data and related information from independent third parties where such disclosure is authorised by the User, permitted under Applicable Law, reasonably necessary for providing Services, or otherwise lawfully available.

Third-party sources may include affiliates, subsidiaries, business partners, technology vendors, customer relationship management providers, cloud infrastructure providers, communication service providers, fraud prevention service providers, cybersecurity vendors, recruitment agencies, marketing partners, advertising partners, authorised resellers, event organisers, customer support providers, identity management providers, financial institutions, insurance providers where applicable, logistics partners, legal advisors, consultants, auditors, and other service providers engaged by the Company.

Information obtained from third parties may be combined with information collected directly from Users where such Processing is reasonably necessary for identity verification, customer support, fraud prevention, analytics, security, compliance, Platform improvement, or other legitimate purposes.

The Company shall exercise reasonable diligence in selecting third-party service providers and shall require such parties to comply with applicable contractual, confidentiality, privacy, and security obligations.

3.4 Government Sources

Where permitted or required under Applicable Law, the Company may collect, verify, receive, or obtain information from Government authorities, statutory bodies, regulatory agencies, judicial authorities, law enforcement agencies, public registries, government databases, or other competent authorities.

Such information may be collected for identity verification, legal compliance, prevention and investigation of fraud, compliance with judicial directions, regulatory reporting, anti-money laundering obligations where applicable, cybersecurity investigations, law enforcement cooperation, or protection of the legal rights of the Company and its Users.

The Company shall obtain such information only where authorised by Applicable Law, judicial order, statutory requirement, regulatory direction, or lawful governmental request.

3.5 Verification Agencies

The Company may engage authorised verification agencies, identity verification service providers, background verification agencies, fraud prevention service providers, document authentication providers, biometric verification vendors, facial recognition providers (where legally permissible), address verification agencies, employment verification agencies, educational verification agencies, or similar entities for verifying the authenticity of information provided by Users.

Such agencies may verify identity documents, contact information, educational qualifications, employment records, photographs, government-issued identification documents, profile authenticity, payment information, communication details, or other information reasonably necessary for the provision of verification Services.

The Company may exchange only the minimum information reasonably necessary to complete the relevant verification process and shall require verification agencies to maintain appropriate confidentiality and security safeguards.

Verification conducted by third parties shall not constitute a guarantee regarding the future conduct, integrity, financial standing, matrimonial suitability, or character of any User.

3.6 Payment Gateways and Financial Institutions

The Company may receive information from licensed payment gateways, payment aggregators, banks, card networks, Unified Payments Interface (UPI) service providers, financial institutions,

wallet providers, recurring payment processors, taxation service providers, invoicing systems, and other regulated financial intermediaries.

Such information may include payment confirmations, transaction identifiers, subscription status, invoice information, settlement confirmations, refund status, chargeback notifications, payment disputes, fraud indicators, taxation information, billing records, merchant identifiers, payment timestamps, and related transactional information.

The Company generally does not receive or permanently store complete payment credentials such as card numbers, CVV numbers, PINs, internet banking passwords, or similar confidential authentication information unless specifically authorised under Applicable Law.

3.7 Analytics Providers

The Company may obtain information from analytics providers engaged for measuring Platform performance, understanding user behaviour, improving Services, enhancing user experience, conducting statistical analysis, identifying operational trends, monitoring security events, and improving Artificial Intelligence models.

Analytics providers may generate aggregated usage reports, behavioural insights, engagement metrics, feature utilisation statistics, conversion data, diagnostic information, traffic analysis, performance measurements, and similar analytical information.

Where reasonably practicable, such information shall be anonymised or pseudonymised before being used for research, reporting, benchmarking, or product development.

3.8 Advertising Networks and Marketing Partners

The Company may receive information from advertising networks, marketing agencies, campaign management platforms, affiliate partners, communication service providers, promotional partners, and similar entities engaged for lawful marketing and promotional purposes.

Such information may include advertising identifiers, campaign performance metrics, conversion data, engagement statistics, referral information, promotional participation records, marketing preferences, communication preferences, and audience segmentation information.

The Company shall not knowingly obtain Personal Data from advertising networks in violation of Applicable Law or without appropriate legal basis where required.

Users may manage advertising preferences through Platform settings, browser controls, device settings, consent management tools, or other mechanisms made available by the Company or relevant third parties.

3.9 Social Login Providers

Where the Platform permits authentication through social login services or third-party identity providers, the Company may receive information directly from such providers in accordance with the permissions granted by the User and the privacy settings maintained on the relevant platform.

Such information may include the User's name, email address, profile photograph, verified status, language preference, public profile information, authentication token, unique user identifier, account status, and other information expressly authorised by the User.

The Company does not control the privacy practices or data collection activities of social login providers and encourages Users to review the applicable privacy policies before connecting third-party accounts to the Platform.

The User may revoke such permissions through the relevant third-party platform or through available

Platform settings, subject to operational limitations.

3.10 Publicly Available Sources

The Company may collect or verify information that has been lawfully made available in the public domain or otherwise made publicly accessible by the User or authorised third parties.

Publicly available sources may include publicly accessible websites, government publications, judicial records, corporate filings, professional directories, public social media profiles, press releases, official announcements, public databases, regulatory disclosures, academic publications, or other lawful public records.

The Company shall Process publicly available information only where reasonably necessary for identity verification, fraud prevention, profile authentication, legal compliance, dispute resolution, cybersecurity,

Platform safety, research, or other legitimate purposes.

The collection of publicly available information shall not authorise the Company to misuse, misrepresent, or exploit such information beyond the purposes described in this Privacy Policy or otherwise permitted under Applicable Law.

3.11 Artificial Intelligence Systems

The Company may generate, infer, classify, organise, analyse, enrich, predict, score, recommend, summarise, or otherwise create information through Artificial Intelligence systems, machine learning models, automated analytics, behavioural analysis engines, recommendation algorithms, natural language processing systems, computer vision technologies, fraud detection

systems, cybersecurity platforms, and intelligent automation tools.

AI systems may derive information from Personal Data, Device Information, Usage Analytics, Communication Records, Metadata, Verification Data, User Content, Cookies, behavioural interactions, technical logs, and other information lawfully Processed by the Company.

AI-generated information may include compatibility recommendations, profile rankings, fraud risk indicators, trust scores, anomaly detection reports, behavioural insights, automated summaries, profile quality assessments, moderation recommendations, search optimisation data, customer support suggestions, spam detection results, cybersecurity alerts, and predictive analytics.

The Company shall use reasonable efforts to ensure that Artificial Intelligence systems operate in a secure, fair, accountable, transparent, and lawful manner. However, Users acknowledge that AI-generated outputs are probabilistic and may occasionally contain inaccuracies, incomplete information, or unintended results. AI-generated information shall assist in the provision of Services and operational decision-making but shall not constitute professional advice, legal advice, factual certification, or any guarantee regarding the conduct, identity, intentions, or suitability of any User.

3.12 General Provisions Applicable to Data Sources

The Company may combine information obtained from multiple lawful sources described in this Chapter where such combination is reasonably necessary for identity verification, fraud prevention, cybersecurity, customer support, Platform administration, analytics, service improvement, Artificial Intelligence development, legal compliance, dispute resolution, regulatory reporting, enforcement of contractual rights, or other legitimate purposes permitted under Applicable Law.

The Company shall implement appropriate technical, organisational, administrative, and contractual safeguards to ensure that information obtained from external sources is Processed securely, lawfully, fairly, and only for authorised purposes. Access to such information shall be restricted to authorised personnel and authorised service providers on a strict need-to-know basis.

Nothing contained in this Chapter shall be construed as obligating the Company to collect information from every source described herein. The actual sources of data collection shall depend upon the nature of the Services used, the User's interactions with the Platform, technological capabilities, contractual arrangements, operational requirements, and Applicable Law. The Company shall collect information only from lawful sources and only to the extent

reasonably necessary, proportionate, and consistent with the purposes set out in this Privacy Policy.

PURPOSE OF PROCESSING

4. PURPOSE OF PROCESSING

The Company shall Process Personal Data only to the extent reasonably necessary for operating the Platform, providing Services, protecting Users, complying with Applicable Law, safeguarding the Company's legitimate business interests, and fulfilling the contractual relationship established under the Terms of Use and this Privacy Policy.

The purposes described below are illustrative and not exhaustive. Depending upon technological developments, business operations, legal obligations, or future Platform features, the Company may Process Personal Data for additional lawful purposes consistent with this Privacy Policy.

4.1 Account Creation and Administration

The Company may Process Personal Data for establishing, registering, activating, administering, maintaining, updating, suspending, restricting, restoring, or permanently closing User Accounts. Such Processing may include identity registration, account authentication, profile creation, password management, account recovery, profile customisation, user preferences, notification management, account verification, communication management, security monitoring, duplicate account detection, account migration, subscription activation, customer onboarding, account administration, and maintaining historical account records.

The Company may also Process Personal Data to enforce account restrictions, investigate misuse, monitor compliance with the Terms of Use, maintain audit trails, and preserve account-related Digital Evidence.

4.2 Identity Verification

The Company may Process Personal Data for verifying the identity, authenticity, eligibility, legal capacity, contact details, and legitimacy of Users.

Verification activities may include document authentication, mobile number verification, email verification, OTP verification, photograph comparison, selfie verification, facial comparison where legally permissible, video verification, employment verification, educational verification, address verification, fraud screening, duplicate profile detection, risk assessment, profile authenticity verification, corporate authority verification, and verification through authorised third-party agencies.

Identity verification helps reduce impersonation, fake profiles, fraudulent activities, identity theft, spam, abuse, and other unlawful conduct.

Successful verification shall not constitute a guarantee regarding the future conduct, character, matrimonial suitability, or intentions of any User.

4.3 Matchmaking and Compatibility Services

As a matrimonial Platform, the Company primarily Processes Personal Data to facilitate lawful matrimonial introductions, compatibility assessments, profile discovery, profile recommendations, search functionality, communication between Users, relationship management services, and related matrimonial services.

Personal Data may be Processed to generate compatibility indicators, recommend suitable profiles, improve search relevance, filter search results according to User preferences, personalise profile visibility, manage profile privacy settings, facilitate introductions, improve matching accuracy, and provide premium matchmaking features.

The Company makes no representation or warranty that any recommendation, compatibility assessment, or suggested profile will necessarily result in a successful matrimonial relationship.

4.4 Artificial Intelligence and Automated Recommendations

The Company may Process Personal Data through Artificial Intelligence systems, machine learning models, automated analytics, behavioural analysis tools, recommendation engines, predictive models, natural language processing systems, and intelligent automation technologies.

Such Processing may be undertaken to generate compatibility scores, improve profile recommendations, personalise search results, optimise user experience, detect spam, identify suspicious behaviour, automate moderation, improve customer support, enhance Platform security, perform language translation, generate automated summaries, improve fraud detection systems, optimise business operations, and improve Artificial Intelligence models.

AI-generated outputs are intended solely as decision-support tools. They are probabilistic in nature and shall not constitute professional advice, legal advice, factual certification, or guarantees regarding compatibility, authenticity, or future conduct.

Where required under Applicable Law, Users shall be informed of material automated decision-making processes and may exercise any rights available under Applicable Law.

4.5 Fraud Prevention, Risk Management and Abuse Detection

The Company may Process Personal Data to prevent, detect, investigate, monitor, mitigate, report, and respond to fraudulent activities, identity theft, impersonation, phishing, cyberattacks, payment fraud, fake profiles, spam, malicious activities, money laundering

indicators where applicable, platform abuse, policy violations, intellectual property infringement, harassment, stalking, scams, financial fraud, and other unlawful or prohibited conduct.

Processing may include behavioural analysis, anomaly detection, device fingerprinting, IP monitoring, risk scoring, transaction monitoring, account monitoring, communication analysis, Artificial Intelligence-assisted fraud detection, cybersecurity monitoring, investigation records, forensic analysis, Digital Evidence preservation, and cooperation with competent authorities.

The Company reserves the right to suspend, restrict, or terminate Accounts where fraud or abuse is reasonably suspected.

4.6 Customer Support and Service Management

The Company may Process Personal Data to provide customer support, respond to enquiries, investigate complaints, resolve grievances, process requests, improve customer experience, maintain service quality, conduct follow-up communications, verify User identity during support interactions, and maintain customer relationship records.

Customer support activities may include telephone support, email correspondence, live chat, chatbot interactions, AI-assisted support, ticket management, complaint handling, escalation management, technical troubleshooting, verification calls, quality assurance, employee training, and service improvement.

Customer support interactions may be recorded where legally permissible.

4.7 Marketing, Promotions and Communications

The Company may Process Personal Data to communicate with Users regarding Services, Platform updates, promotional campaigns, offers, newsletters, invitations, educational materials, surveys, customer engagement programmes, referral programmes, loyalty programmes, seasonal campaigns, announcements, and other lawful marketing activities.

Marketing communications may be delivered through email, SMS, push notifications, WhatsApp, telephone calls where permitted, in-app notifications, or other communication channels authorised by the User or permitted under Applicable Law.

Users may withdraw consent or opt out of non-essential marketing communications through available preference settings or by following unsubscribe instructions, subject to communications necessary for legal compliance, account administration, security, or contractual performance.

4.8 Subscription and Membership Management

The Company may Process Personal Data to administer subscription plans, premium memberships, renewals, upgrades, downgrades, promotional offers, discount programmes, trial

memberships, subscription benefits, membership eligibility, usage limits, cancellations, refunds, recurring billing, and related commercial activities.

The Company may maintain historical subscription records for accounting, auditing, taxation, legal compliance, fraud prevention, customer support, and dispute resolution.

4.9 Payment Processing and Financial Administration

The Company may Process Personal Data to facilitate payments, issue invoices, process subscriptions, reconcile transactions, administer refunds, manage chargebacks, detect payment fraud, maintain accounting records, calculate taxes, comply with financial reporting obligations, resolve payment disputes, and protect the Company's financial interests.

Payment-related Processing may involve licensed payment gateways, banks, payment aggregators, financial institutions, taxation authorities, auditors, accounting professionals, and authorised financial service providers.

The Company may retain financial records for the duration required under Applicable Law, taxation laws, accounting standards, contractual obligations, litigation requirements, or regulatory investigations.

4.10 Legal and Regulatory Compliance

The Company may Process Personal Data to comply with Applicable Law, judicial orders, governmental directions, regulatory requirements, statutory obligations, law enforcement requests, taxation obligations, corporate governance requirements, audit obligations, reporting requirements, data protection laws, cybersecurity laws, consumer protection laws, and other legal responsibilities.

Such Processing may include responding to lawful requests from courts, tribunals, government authorities, regulators, law enforcement agencies, and other competent authorities.

The Company reserves the right to disclose Personal Data where disclosure is required or authorised by Applicable Law or reasonably necessary to protect legal rights or public safety.

4.11 Cybersecurity and Information Security

The Company may Process Personal Data for maintaining the confidentiality, integrity, availability, authenticity, resilience, and security of the Platform and its information systems.

Such Processing may include security monitoring, intrusion detection, vulnerability assessments, penetration testing, malware detection, threat intelligence, authentication management, access control, security logging, forensic investigations, incident response, disaster recovery, Digital Evidence preservation, security audits, compliance monitoring, cybersecurity risk assessments, and implementation of security controls.

The Company may Process security-related information continuously to identify and respond to actual or suspected cybersecurity incidents.

4.12 Analytics, Reporting and Business Intelligence

The Company may Process Personal Data to analyse Platform performance, understand User behaviour, generate business intelligence, prepare statistical reports, measure service quality, optimise operational efficiency, evaluate customer satisfaction, identify usage trends, monitor system performance, forecast demand, improve decision-making, and support business planning.

Where reasonably practicable, analytics shall utilise anonymised, aggregated, or pseudonymised information.

4.13 Research, Innovation and Product Development

The Company may Process Personal Data to conduct research, develop new products and services, improve existing features, train Artificial Intelligence systems, test software, evaluate user experience, conduct security research, improve fraud detection systems, validate business models, and support innovation initiatives.

Research activities may utilise anonymised, aggregated, or de-identified information wherever reasonably practicable and consistent with the intended purpose.

4.14 Platform Improvement and Quality Assurance

The Company may Process Personal Data to improve Platform functionality, optimise user interfaces, enhance search performance, improve compatibility algorithms, reduce technical errors, maintain software quality, identify system defects, improve accessibility, enhance service reliability, and develop future Platform features.

Such Processing may include software testing, quality assurance reviews, beta testing, user experience evaluations, feature performance assessments, bug investigations, and system optimisation.

4.15 Business Continuity and Corporate Operations

The Company may Process Personal Data to ensure uninterrupted business operations, maintain backups, support disaster recovery, preserve operational resilience, conduct internal audits, manage corporate governance, support mergers, acquisitions, restructuring, financing transactions, asset transfers, insurance claims, risk management, and other legitimate corporate activities.

Where ownership or control of the Company changes, Personal Data may be transferred as part of the relevant transaction, subject to Applicable Law and appropriate confidentiality obligations.

4.16 Legal Proceedings, Enforcement and Protection of Rights

The Company may Process Personal Data to establish, exercise, enforce, defend, preserve, or protect its legal rights and obligations, whether in judicial proceedings, arbitration, mediation, regulatory investigations, internal investigations, disciplinary proceedings, insurance claims, intellectual property disputes, contractual disputes, or other legal matters.

Such Processing may include preservation of Digital Evidence, litigation holds, forensic analysis, legal review, witness preparation, evidence management, compliance reporting, and cooperation with legal advisors, courts, arbitrators, tribunals, regulators, or law enforcement agencies.

4.17 Dispute Resolution and Grievance Redressal

The Company may Process Personal Data to investigate complaints, resolve disputes, administer grievance mechanisms, facilitate mediation, arbitration, settlement negotiations, customer complaints, consumer disputes, payment disputes, subscription disputes, chargeback proceedings, and other disagreements arising from the use of the Platform.

Processing may include review of Communication Records, transaction history, verification records, Digital Evidence, audit logs, customer support records, AI-generated moderation logs, security logs, and other relevant information reasonably necessary for resolving disputes fairly and efficiently.

4.18 General Principles Governing the Purpose of Processing

The Company shall Process Personal Data only for lawful, fair, transparent, specified, and legitimate purposes consistent with this Privacy Policy, the Terms of Use, Applicable Law, contractual obligations, or valid User consent.

Where Personal Data is required for multiple compatible purposes, the Company may Process such information for all such purposes, provided that such Processing remains proportionate, reasonably necessary, and compliant with Applicable Law.

Where reasonably practicable, the Company shall apply data minimisation, purpose limitation, pseudonymisation, anonymisation, encryption, access controls, retention limitations, and other privacy-enhancing measures to reduce privacy risks while maintaining operational efficiency.

Nothing contained in this Chapter shall prevent the Company from Processing Personal Data for any additional purpose that is:

- expressly authorised by the User;
- required or permitted under Applicable Law;

- necessary for the performance of a contract;
- necessary to protect the rights, safety, security, or legitimate interests of the Company, its Users, or the public; or
- reasonably compatible with the purposes originally disclosed in this Privacy Policy.

This Chapter shall be read harmoniously with the Terms of Use, Data Retention provisions, Information Security provisions, User Rights, Consent Management provisions, and all other applicable policies forming part of the Company's legal framework.

CONSENT MANAGEMENT

5. CONSENT MANAGEMENT

The Company recognises that lawful Processing of Personal Data requires transparency, accountability, and, where required under Applicable Law, the free, specific, informed, unconditional, and unambiguous consent of the User or Data Principal.

The Company shall implement reasonable administrative, technical, organisational, and contractual measures to obtain, maintain, record, verify, update, and manage User consent throughout the lifecycle of the User's interaction with the Platform.

Nothing contained in this Chapter shall limit any lawful basis for Processing available to the Company under Applicable Law.

5.1 Obtaining Consent

The Company may obtain Consent before or at the time of collecting Personal Data where Consent is required under Applicable Law.

Consent may be obtained electronically or through any other legally recognised method, including but not limited to:

- clicking an "I Agree," "Accept," "Continue," "Register," "Submit," or similar electronic acceptance button;
- creating or activating a User Account;
- verifying a mobile number or email address through OTP or similar authentication methods;
- voluntarily uploading Personal Data, documents, photographs, videos, or other information;
- enabling Cookies or location permissions through consent banners or device settings;
- providing consent through digital signatures, electronic signatures, biometric authentication, or other legally recognised authentication mechanisms;
- expressly opting into marketing communications, newsletters, promotional campaigns, AI-enabled services, or premium features;

- participating in surveys, research programmes, verification services, or optional Platform features; or
- any other affirmative action that clearly indicates agreement to the Processing of Personal Data.

Consent shall be sought in clear, plain, intelligible, and easily accessible language and shall specify, to the extent reasonably practicable, the categories of Personal Data to be Processed, the purposes of Processing, the categories of recipients, the availability of User rights, and the method of withdrawing Consent.

The Company shall not obtain Consent through misleading, deceptive, coercive, or unfair means.

5.2 Withdrawal of Consent

Where Processing is based upon Consent, the User or Data Principal may withdraw such Consent at any time through the mechanisms provided on the Platform or by contacting the Company through the prescribed grievance or privacy channels.

Withdrawal of Consent shall operate prospectively and shall not affect:

- (a) the lawfulness of any Processing undertaken before the withdrawal became effective;
- (b) Processing undertaken on any other lawful basis recognised under Applicable Law;
- (c) the Company's obligation to retain information required for legal, regulatory, taxation, accounting, audit, fraud prevention, cybersecurity, contractual, or evidentiary purposes;
- (d) anonymised, aggregated, statistical, or de-identified information that no longer constitutes Personal Data under Applicable Law; or
- (e) the exercise or defence of legal rights or compliance with judicial or governmental directions.

The Company shall, within a reasonable period and subject to Applicable Law, cease Processing Personal Data for those purposes that rely exclusively upon the withdrawn Consent.

5.3 Consent Records

The Company may maintain comprehensive electronic records demonstrating that valid Consent has been obtained, modified, renewed, withdrawn, or otherwise managed.

Consent Records may include: date and time of Consent; method by which Consent was obtained; version of the Privacy Policy or Terms accepted;

IP address; device information; browser information; transaction identifiers; account identifiers; authentication records; digital signatures; OTP verification records; system logs; electronic acknowledgements; audit trails; screenshots where reasonably necessary; Consent history; withdrawal records; and any other Digital Evidence reasonably necessary to demonstrate legal

compliance.

Such records may be retained for evidentiary purposes, dispute resolution, regulatory compliance, legal proceedings, audit requirements, fraud prevention, cybersecurity investigations, contractual enforcement, and protection of the Company's legal rights.

Electronic Consent Records maintained by the Company shall, to the extent permitted under Applicable Law, constitute prima facie evidence of User consent.

5.4 Parental Consent and Processing Relating to Children

The Platform is intended only for individuals legally eligible to use the Services under Applicable Law and the Terms of Use.

Where Applicable Law requires verifiable parental or lawful guardian consent before collecting or Processing Personal Data relating to a child or person lacking legal capacity, the Company shall implement reasonable verification mechanisms before commencing such Processing.

The Company reserves the right to request documentary proof of age, parental authority, guardianship, identity, or legal capacity where reasonably necessary.

If the Company becomes aware that Personal Data relating to a child has been collected without the legally required authorisation, the Company may suspend the relevant Account, restrict access, seek additional verification, delete such information, or take any other action required under Applicable Law.

Nothing in this Privacy Policy shall require the Company to independently investigate the age of every User unless circumstances reasonably indicate otherwise or Applicable Law imposes such an obligation.

5.5 Additional, Separate and Purpose-Specific Consent

Certain Processing activities may require separate, specific, or additional Consent beyond the general acceptance of this Privacy Policy.

Such Processing may include, without limitation:

- collection of precise geolocation information;
- use of biometric information where legally permissible;
- identity verification services;
-

AI-assisted profile analysis where required by law;

- facial recognition technologies where legally permitted;
- optional marketing communications;
- promotional campaigns;

- participation in surveys or research initiatives;
- recording of customer support interactions where legally required;
- processing of certain categories of Sensitive Information;
- integration with third-party social media platforms;
- cross-platform data sharing initiated by the User;
- participation in beta testing programmes; and
- any other activity requiring separate Consent under Applicable Law.

The Company may seek renewed Consent where there is a material change in the purpose of Processing or where Applicable Law otherwise requires renewed authorisation.

Failure to provide additional Consent may result in the relevant optional feature or Service being unavailable without affecting the availability of the core Services, unless such Processing is necessary for providing the requested Service.

5.6 Legitimate Uses and Other Lawful Bases of Processing

The User acknowledges that not every Processing activity requires Consent.

To the extent permitted under Applicable Law, the Company may Process Personal Data without obtaining separate Consent where such Processing is:

- necessary for the performance, administration, or enforcement of a contract with the User;
- required to comply with Applicable Law, judicial orders, governmental directions, or regulatory obligations;
- necessary for responding to lawful requests from competent authorities;
- necessary for preventing, detecting, investigating, or prosecuting fraud, cybercrime, financial crime, identity theft, abuse, or other unlawful activities;
- necessary for protecting the life, health, safety, or vital interests of any individual;
- necessary for cybersecurity, network security, information security, incident response, or business continuity;
- necessary for preserving Electronic Records or Digital Evidence;
- necessary for establishing, exercising, defending, or enforcing legal rights;
- undertaken for internal administration, corporate governance, auditing, risk management, compliance monitoring, or insurance purposes;
- based upon information that has lawfully been made publicly available by the User or authorised under Applicable Law;
- undertaken for research, statistical analysis, innovation, product development, or Artificial Intelligence improvement using anonymised or appropriately safeguarded information;

or

- otherwise authorised, recognised, or permitted under the Digital Personal Data Protection Act, 2023, or any other Applicable Law.

Where the Company relies upon a lawful basis other than Consent, such Processing shall remain subject to the principles of necessity, proportionality, fairness, security, accountability, and purpose limitation.

5.7 Consequences of Refusal or Withdrawal of Consent

The User acknowledges that certain categories of Personal Data are essential for the provision of the Company's Services.

Accordingly, refusal to provide Consent, or subsequent withdrawal of Consent, may result in one or more of the following consequences i.e. the User being unable to create or maintain a User Account, verify identity or eligibility, access premium or subscription- based Services, or use certain matchmaking functionalities, including communication with other Users or receipt of personalised recommendations. It may also lead to suspension or restriction of Platform features, inability to complete payment transactions, failure of authentication or other security mechanisms, discontinuation of marketing communications, and inability to participate in verification programmes or obtain customer support for issues requiring identity verification. In certain cases, it may further result in termination of Services where Processing is strictly necessary for contractual performance or legal compliance.

The Company shall not be liable for any loss, inconvenience, reduced functionality, inability to provide Services, or adverse consequences arising solely because a User refuses or withdraws Consent necessary for providing the requested Services.

5.8 Consent Review, Renewal and Management

The Company may periodically review the validity, adequacy, and continued necessity of User Consent.

Where appropriate, the Company may:

- request renewed Consent;
- update Consent preferences;
- provide revised privacy notices;
- seek additional authorisations for new Processing activities;
- reconfirm marketing preferences;
- refresh Cookie preferences;
- require acceptance of revised Terms or Privacy Policies; or

- implement enhanced authentication before permitting modifications to Consent settings.

The Company reserves the right to suspend or limit certain Processing activities until updated Consent is obtained where such Consent is required under Applicable Law.

5.9 Burden of Proof and Evidentiary Value

The Company may rely upon electronically maintained Consent Records, audit trails, authentication logs, OTP records, system-generated records, Digital Evidence, Electronic Records, and other technological records to demonstrate compliance with Applicable Law and the validity of User Consent.

To the fullest extent permitted by Applicable Law, such electronically maintained records shall be admissible and may be relied upon in judicial proceedings, arbitration, mediation, regulatory investigations, governmental proceedings, internal investigations, audits, and dispute resolution processes.

The User acknowledges that electronic records generated through the normal operation of the Platform may constitute valid evidence regarding the existence, scope, modification, withdrawal, or renewal of Consent.

5.10 General Principles Governing Consent

The Company shall maintain appropriate governance mechanisms to ensure that Consent is obtained, managed, and documented in a lawful, transparent, secure, and accountable manner.

Nothing contained in this Chapter shall:

- restrict any lawful basis of Processing available under Applicable Law;
- prevent the Company from complying with statutory or regulatory obligations;
- affect the Company's right to retain information where legally required;
- prejudice the Company's ability to preserve Digital Evidence, Electronic Records, or audit logs;
- prevent the Company from Processing anonymised or aggregated information that no longer constitutes Personal Data; or
- limit any contractual, statutory, or legal rights available to the Company under the Terms of Use, this Privacy Policy, or Applicable Law.

USE OF ARTIFICIAL INTELLIGENCE

6. USE OF ARTIFICIAL INTELLIGENCE

The Company may design, develop, license, acquire, deploy, train, operate, monitor, improve, modify, suspend, replace, or discontinue Artificial Intelligence systems, machine learning models, automated analytics, behavioural algorithms, recommendation engines, predictive

models, natural language processing technologies, intelligent automation tools, and other computational systems for the purpose of operating, securing, enhancing, and improving the Platform and the Services.

Users acknowledge that certain functionalities of the Platform may be wholly or partly powered by Artificial Intelligence and that interaction with the Platform may involve automated Processing, predictive analysis, behavioural modelling, or algorithmic recommendations.

The Company shall endeavour to ensure that AI systems are designed and operated responsibly; however, Users acknowledge that AI technologies are probabilistic in nature and may occasionally produce inaccurate, incomplete, inconsistent, outdated, or unintended outputs.

6.1 AI Matching

The Company may utilise Artificial Intelligence, machine learning algorithms, behavioural analytics, predictive modelling, statistical analysis, compatibility engines, semantic analysis, and other computational technologies to facilitate matrimonial matching and compatibility recommendations.

AI Matching may consider various categories of information lawfully Processed by the Company, including profile information, matrimonial preferences, demographic information, educational background, occupation, interests, communication behaviour, activity history, subscription preferences, search behaviour, compatibility indicators, and other information voluntarily provided by Users.

The objective of AI Matching is to improve the relevance, efficiency, personalisation, and quality of profile recommendations.

The Company reserves the right to modify, recalibrate, suspend, or replace any matching algorithm at any time without prior notice where reasonably necessary for improving accuracy, fairness, security, operational efficiency, regulatory compliance, or business requirements.

The Company does not disclose proprietary algorithms, weighting methodologies, model architectures, source code, training methodologies, or confidential technical parameters used in AI Matching.

6.2 Automated Decision-Making

The Company may employ automated systems to support operational decisions relating to account security, fraud prevention, spam detection, duplicate profile identification, content moderation, recommendation ranking, subscription administration, search optimisation, cybersecurity, identity verification, communication filtering, and other Platform functions.

Automated decisions may include temporary account restrictions, additional verification requests, fraud alerts, automated moderation actions, profile visibility adjustments, spam filtering, recommendation prioritisation, and security-related interventions.

Where reasonably practicable and consistent with Applicable Law, significant automated decisions that may materially affect a User may be subject to additional review mechanisms or appropriate safeguards.

Nothing contained herein shall prevent the Company from taking immediate automated action where necessary to protect the Platform, Users, cybersecurity infrastructure, or to prevent fraud, abuse, unlawful activities, or security incidents.

6.3 AI Profiling

The Company may create automated profiles, behavioural models, statistical classifications, compatibility assessments, risk indicators, trust scores, engagement models, or similar analytical outputs through Artificial Intelligence systems.

AI Profiling may involve the analysis of:

This information comprises user preferences, profile completeness, behavioral interactions, communication patterns, browsing activity, and feature utilization.

Additionally, it includes verification status, transaction history, security indicators, fraud risk factors, account activity, subscription history, and other lawfully processed information.

Such profiling is intended solely for improving user experience, enhancing Platform security, preventing fraud, personalising Services, improving recommendations, and supporting legitimate operational purposes.

AI-generated profiles are dynamic analytical models and do not constitute factual statements regarding the User's personality, intentions, reputation, financial condition, legal status, matrimonial suitability, or future behaviour.

6.4 Recommendation Engines

The Company may operate recommendation engines that automatically generate personalised recommendations, search rankings, compatibility suggestions, profile ordering, premium suggestions, content recommendations, customer support suggestions, educational materials, safety alerts, promotional offers, and other personalised experiences.

Recommendation engines may utilise historical interactions, behavioural analytics, profile preferences, demographic information, communication patterns, subscription status, Platform usage, AI-generated insights, statistical models, and contextual information.

Recommendations generated by AI are intended solely to assist Users in navigating the

Platform efficiently and shall not be construed as endorsements, certifications, guarantees, legal opinions, professional advice, or representations regarding the accuracy, authenticity, safety, compatibility, or suitability of any User or profile.

The Company reserves the unrestricted right to alter recommendation methodologies, ranking criteria, filtering mechanisms, recommendation frequency, or recommendation models without prior notice.

6.5 Human Oversight

Although Artificial Intelligence may automate certain operational processes, the Company may implement appropriate human oversight over AI systems where reasonably necessary, technically feasible, commercially practicable, or legally required.

This comprehensive scope encompasses the review of high-risk decisions, the investigation of fraud alerts, and the management of moderation appeals. It also involves addressing customer complaints and grievance handling, alongside conducting legal compliance reviews and security incident investigations. Finally, the framework incorporates quality assurance assessments, algorithm validation, bias monitoring, and thorough internal audits.

The Company reserves absolute discretion to determine the level, timing, scope, and manner of human intervention based upon operational requirements, technological capabilities, legal obligations, security considerations, and business needs.

Nothing contained herein shall create any obligation requiring manual review of every AI-generated outcome.

6.6 AI Limitations

Users expressly acknowledge and agree that Artificial Intelligence technologies have inherent technical, statistical, computational, and operational limitations.

AI systems may generate inaccurate or incomplete outputs, misinterpret user inputs, and fail to recognize contextual nuances. They can also produce inconsistent recommendations, rely upon incomplete datasets, and generate false positives or false negatives. Furthermore, these systems contain probabilistic uncertainty, evolve through continuous learning, and may experience temporary technical failures. Finally, they can produce recommendations affected by data quality or otherwise generate outputs that differ from human judgment.

Accordingly, Users shall independently evaluate all AI-generated outputs before relying upon them for any personal, matrimonial, financial, legal, professional, or other decision.

The Company strongly discourages Users from relying exclusively upon AI-generated recommendations without exercising independent judgment.

6.7 No Guarantee Disclaimer

The Company expressly disclaims every representation, warranty, guarantee, assurance, undertaking, or promise regarding the performance, accuracy, completeness, reliability, suitability, availability, effectiveness, fairness, compatibility, predictability, or outcomes of any Artificial Intelligence system.

Without limiting the generality of the foregoing, the Company does not warrant that AI systems will identify suitable matrimonial partners, generate accurate compatibility scores, or correctly assess User behavior. Furthermore, the Company does not guarantee that these systems will prevent fraud in every instance, detect every fake profile, or eliminate human error. Users should also anticipate that the systems may not remain uninterrupted or error-free, operate without technical limitations, or produce identical results over time. Ultimately, there is no warranty that the AI systems will achieve any particular personal, matrimonial, commercial, or legal outcome.

AI-generated outputs are informational and assistive in nature only and shall not create any contractual warranty, fiduciary duty, professional obligation, or guarantee on the part of the Company.

To the fullest extent permitted by Applicable Law, the Company shall not be liable for any direct, indirect, incidental, consequential, special, exemplary, punitive, reputational, emotional, matrimonial, financial, or other losses arising from reliance upon AI-generated outputs or automated recommendations.

6.8 Bias Mitigation and Responsible AI Governance

The Company is committed to the responsible development and deployment of Artificial Intelligence technologies.

Subject to technological feasibility, operational practicality, commercial reasonableness, and Applicable Law, the Company may implement reasonable measures to identify, assess, monitor, reduce, and mitigate algorithmic bias, discriminatory outcomes, security vulnerabilities, model drift, adversarial attacks, data quality issues, and unintended consequences.

Such measures may include periodic model validation, security testing, and quality assurance reviews. They also involve representative data evaluation, fairness assessments, bias monitoring, and performance benchmarking. Where appropriate, explainability assessments are conducted alongside human review mechanisms and cybersecurity monitoring. Finally, these measures encompass continuous model improvement and the enforcement of internal governance controls.

The Company does not represent that every AI system will be entirely free from bias, error, or unintended outcomes, particularly where such outcomes arise from incomplete, inaccurate, misleading, outdated, manipulated, or insufficient information supplied by Users or third parties.

6.9 AI Transparency

The Company is committed to maintaining reasonable transparency regarding the use of Artificial Intelligence on the Platform.

Where reasonably appropriate, Users may be informed that specific Services, recommendations, automated communications, chatbots, moderation systems, customer support tools, fraud detection mechanisms, profile recommendations, or compatibility assessments involve Artificial Intelligence or automated Processing.

However, nothing contained in this Privacy Policy shall require the Company to disclose proprietary algorithms, source code, software architecture, or training datasets.

Furthermore, this restriction extends to model parameters, weighting methodologies, confidential technical documentation, trade secrets, and cybersecurity measures.

Ultimately, the Company is not required to reveal its intellectual property, commercially sensitive information, or any other information that could compromise Platform security, fraud prevention mechanisms, or the Company's legitimate business interests.

The Company reserves the right to improve, retrain, update, replace, or discontinue AI systems at any time without prior notice.

6.10 AI Security, Intellectual Property and Regulatory Compliance

The Company's Artificial Intelligence systems, algorithms, software, recommendation engines, model architectures, datasets (to the extent legally protectable), workflows, prompts, optimisation techniques, documentation, interfaces, outputs created by the

Company, trade secrets, confidential methodologies, and related technologies constitute valuable intellectual property and confidential information of the Company and are protected under applicable intellectual property, copyright, trade secret, and unfair competition laws.

Users shall not, directly or indirectly:

- reverse engineer, decompile, disassemble, copy, scrape, crawl, extract, benchmark, or replicate the Company's AI systems;
- use automated bots or tools to analyse or reproduce AI outputs for competitive purposes;
- attempt to discover confidential algorithms, prompts, weighting criteria, or model parameters;
- use the Company's AI systems to train competing artificial intelligence models without the

Company's prior written consent;

- interfere with, manipulate, or circumvent AI safety mechanisms or security controls; or
- exploit AI-generated outputs in violation of the Terms of Use or Applicable Law.

The Company reserves the right to implement AI governance frameworks, cybersecurity safeguards, audit mechanisms, model monitoring, and technical controls to ensure the secure, ethical, and lawful operation of its AI systems and to comply with evolving legal and regulatory requirements.

6.11 General Provisions Governing Artificial Intelligence

Artificial Intelligence shall be regarded as a technological tool intended to enhance, support, and improve the delivery of the Company's Services and not as a substitute for independent human judgment or due diligence by Users.

The Company may continue to develop, integrate, acquire, license, retire, or modify AI technologies in response to technological innovation, regulatory developments, operational requirements, cybersecurity considerations, industry standards, or legitimate business needs.

Nothing contained in this Chapter shall:

- create any guarantee regarding AI-generated outcomes;
- impose a fiduciary duty upon the Company in relation to AI recommendations;
- limit the Company's rights under the Terms of Use or Applicable Law;
- prevent the Company from using future AI technologies or automated systems consistent with this Privacy Policy; or
- restrict the Company's ability to implement security, compliance, fraud prevention, or operational measures involving Artificial Intelligence.

DISCLOSURE OF INFORMATION

7. DISCLOSURE OF INFORMATION

The Company recognises that the confidentiality and privacy of Personal Data are fundamental to the operation of the Platform. Accordingly, the Company shall not sell, lease, trade, or commercially exploit Personal Data except as expressly permitted under this Privacy Policy, the Terms of Use, User consent, or Applicable Law.

The Company may disclose Personal Data only where such disclosure is reasonably necessary for providing Services, protecting Users, complying with legal obligations, enforcing contractual rights, maintaining cybersecurity, preventing fraud, facilitating corporate operations, or pursuing other legitimate purposes described in this Privacy Policy.

All recipients receiving Personal Data from the Company shall be subject to appropriate confidentiality, contractual, technical, organisational, and security obligations proportionate to the nature of the information disclosed.

7.1 Disclosure to Affiliates and Group Companies

The Company may disclose Personal Data to its parent company, subsidiaries, holding companies, affiliates, associate companies, joint venture entities, group companies, successor entities, or entities under common ownership or control.

Such disclosure may be necessary for account administration, customer support, shared technology infrastructure, and cybersecurity. It also supports fraud prevention, internal administration, compliance management, and analytics. Additionally, this data sharing facilitates business continuity, research and development, Artificial Intelligence improvement, and marketing administration. Finally, it is utilized for financial reporting, corporate governance, and other legitimate business operations.

All affiliated entities receiving Personal Data shall Process such information only for authorised purposes and shall remain bound by confidentiality, privacy, cybersecurity, and data protection obligations substantially equivalent to those contained in this Privacy Policy.

7.2 Disclosure to Service Providers

The Company may engage independent third-party service providers, contractors, consultants, vendors, processors, sub-processors, technology partners, customer support providers, infrastructure providers, communication providers, verification agencies, software vendors, cybersecurity providers, and managed service providers to perform services on behalf of the Company.

Such service providers may receive access to Personal Data solely to the extent reasonably necessary for performing contracted services, including hosting services, customer support, and identity verification. This access also covers email and SMS delivery, fraud detection, cybersecurity monitoring, and software development. Additionally, it encompasses cloud infrastructure, database management, analytics, and marketing support. Finally, these providers may handle technical maintenance, quality assurance, payment administration, dispute management, and business continuity services.

The Company shall require such service providers to implement appropriate contractual, organisational, administrative, and technical safeguards to protect Personal Data and prohibit its unauthorised use, disclosure, sale, or Processing.

7.3 Disclosure to Payment Gateways and Financial Institutions

Where Users purchase subscriptions or make payments through the Platform, the Company may disclose necessary information to licensed payment gateways, banks, payment aggregators, card networks, Unified Payments Interface (UPI) providers, financial institutions, taxation authorities, recurring payment processors, fraud monitoring services, and settlement partners.

Information disclosed may include payment identifiers, billing information, invoice details, and transaction references. It also encompasses subscription status, refund information, taxation information, and merchant identifiers. Finally, this data extends to payment confirmations, fraud indicators, and other information reasonably necessary for processing financial transactions.

The Company shall not knowingly disclose complete payment authentication credentials except where required by Applicable Law or processed directly through authorised payment infrastructure.

7.4 Disclosure to Cloud Service Providers and Technology Infrastructure Providers

The Company may utilise domestic or international cloud infrastructure providers, managed hosting providers, content delivery networks, disaster recovery providers, database service providers, backup providers, cybersecurity vendors, Artificial Intelligence infrastructure providers, and other technology partners.

Such providers may Process Personal Data for purposes including secure hosting, database management, encrypted backups, and disaster recovery. This processing also covers redundancy, software deployment, cybersecurity monitoring, and infrastructure maintenance. Finally, it supports performance optimization, Artificial Intelligence processing, analytics, and business continuity.

The Company shall use commercially reasonable efforts to engage providers maintaining recognised information security standards and contractual confidentiality obligations.

7.5 Disclosure to Government Authorities and Regulatory Bodies

The Company may disclose Personal Data to Government authorities, statutory authorities, regulatory agencies, taxation authorities, data protection authorities, public authorities, cybersecurity agencies, sectoral regulators, consumer protection authorities, or any other competent governmental body where:

- required by Applicable Law;
- required for regulatory compliance;
- necessary for statutory reporting;

- directed by lawful governmental order;
- necessary to protect public interest;
- necessary for national security;
- required for tax administration;
- required for cybersecurity reporting; or
- otherwise lawfully authorised.

The Company shall disclose only such information as is reasonably necessary to comply with the relevant legal requirement unless broader disclosure is legally mandated.

7.6 Disclosure to Law Enforcement Agencies

The Company may disclose Personal Data, Electronic Records, Metadata, Communication Records, Digital Evidence, audit logs, security logs, verification records, transaction history, and other relevant information to law enforcement agencies where required or permitted under Applicable Law.

Such disclosure may occur for the investigation of criminal offenses, the prevention of fraud, and cybercrime investigations. It also covers identity theft investigations, financial crime investigations, and the protection of public safety. Additionally, this data may be shared for the enforcement of legal rights, the prevention of imminent harm, the execution of lawful warrants, or for compliance with lawful requests issued by competent authorities.

The Company reserves the right to preserve relevant Digital Evidence before, during, or after any such disclosure.

7.7 Disclosure Pursuant to Judicial Orders and Legal Proceedings

The Company may disclose Personal Data where required pursuant to orders of courts, tribunals, arbitrators, or judicial commissions. This disclosure may also occur during statutory authorities' reviews, regulatory proceedings, mediation proceedings, or arbitration proceedings. Finally, data may be shared to fulfill discovery obligations, or in response to subpoenas, summons, warrants, or any other legally enforceable process.

The Company may also disclose Personal Data where reasonably necessary to establish, exercise, defend, enforce, or protect its legal rights, contractual rights, intellectual property rights, or legitimate business interests.

7.8 Disclosure to Auditors, Accountants and Compliance Professionals

The Company may disclose Personal Data to internal auditors, statutory auditors, independent auditors, accountants, tax consultants, compliance professionals, risk consultants, cybersecurity auditors, forensic investigators, certification bodies, and other professional advisors engaged for

legitimate corporate purposes.

Such disclosure may be necessary for financial audits, statutory audits, and taxation compliance. It also supports corporate governance, internal investigations, cybersecurity assessments, and forensic examinations. Finally, this data sharing facilitates regulatory compliance, certification processes, risk management, and operational reviews.

Professional recipients shall remain subject to confidentiality obligations arising under law, professional ethics, contractual arrangements, or regulatory requirements.

7.9 Disclosure to Legal Advisors and Professional Representatives

The Company may disclose Personal Data to advocates, solicitors, legal consultants, external counsel, arbitrators, mediators, legal process managers, recovery agents, insurance counsel, intellectual property professionals, and other authorised legal representatives.

Such disclosure may be necessary for legal advice, litigation, arbitration, and mediation.

It also supports settlement negotiations, contract enforcement, debt recovery, and intellectual property protection. Finally, this data sharing facilitates regulatory proceedings, insurance claims, legal compliance, and overall dispute resolution.

The Company may also preserve privileged communications and legal work product to the fullest extent permitted by Applicable Law.

7.10 Corporate Transactions, Mergers and Business Transfers

The Company may disclose or transfer Personal Data in connection with mergers, acquisitions, amalgamations, or demergers. This sharing may also occur during restructurings, strategic investments, financing transactions, or insolvency proceedings.

Finally, data transfers may be necessary for asset sales, business transfers, joint ventures, succession planning, corporate reorganizations, or any other legitimate corporate transaction.

Any successor entity acquiring the Company's business shall be required to Process Personal Data in accordance with Applicable Law and substantially consistent privacy protections.

Where required by Applicable Law, Users shall be notified regarding material changes affecting the Processing of Personal Data following such transactions.

7.11 Emergency Disclosure

The Company may disclose Personal Data without prior notice to the User where the Company reasonably believes such disclosure is necessary to prevent imminent harm, protect life or physical safety, or respond to medical emergencies. It may also do so to address cybersecurity incidents, mitigate data breaches, prevent financial fraud, or investigate terrorism

and organized crime. Furthermore, this measure can be deployed to prevent child exploitation, respond to disaster situations, protect public health, preserve digital evidence, or prevent the destruction of evidence. Finally, such disclosures may occur to enforce emergency governmental directions or otherwise protect the rights, safety, security, or property of the Company, its Users, employees, business partners, or the public.

The Company shall make reasonable efforts to limit emergency disclosures to the minimum information necessary for the relevant purpose.

7.12 Cross-Border Disclosure and International Transfers

Where operationally necessary and permitted under Applicable Law, the Company may disclose or transfer Personal Data to recipients located outside India, including affiliates, cloud providers, technology vendors, verification agencies, customer support providers, or professional advisors.

Such transfers shall be undertaken only where:

- permitted by Applicable Law;
- appropriate contractual safeguards are implemented;
- reasonable security measures are maintained;
- confidentiality obligations are imposed; and
- the transfer is necessary for providing Services, maintaining infrastructure, or supporting legitimate business operations.

The Company shall take commercially reasonable steps to ensure that international recipients maintain an appropriate level of data protection consistent with this Privacy Policy and Applicable Law.

7.13 No Sale of Personal Data

Except where expressly authorised by the User or permitted under Applicable Law, the Company does not sell Personal Data as a commercial commodity.

The Company shall not disclose Personal Data to third parties for their independent marketing purposes unless the User has expressly consented or such disclosure is otherwise authorised under Applicable Law.

The Company may, however, disclose anonymised, aggregated, statistical, or de-identified information that does not identify any individual and no longer constitutes Personal Data under Applicable Law.

7.14 General Principles Governing Disclosure

Every disclosure of Personal Data shall be guided by the principles of lawfulness, necessity, proportionality, transparency, accountability, confidentiality, security, and purpose limitation.

Before disclosing Personal Data, the Company may implement appropriate safeguards including confidentiality agreements, data processing agreements, and non-disclosure agreements. It may also employ encryption, secure transmission protocols, and role-based access controls alongside audit logging and cybersecurity monitoring. Finally, these protective actions encompass contractual restrictions, periodic compliance reviews, and other organizational and technical security measures.

Nothing contained in this Chapter shall:

- require the Company to disclose confidential business information, trade secrets, proprietary algorithms, cybersecurity measures, legal privilege, or intellectual property;
- restrict the Company's right to preserve Electronic Records or Digital Evidence;
- prevent the Company from complying with statutory, judicial, or regulatory obligations;
- limit disclosures necessary to establish, exercise, or defend legal rights;
- prejudice the Company's rights under the Terms of Use, Applicable Law, or any contractual arrangement; or
- create any obligation to notify a User where such notification is prohibited by law, judicial order, regulatory direction, or would reasonably prejudice an investigation, cybersecurity operation, fraud prevention activity, or legal proceeding.

INTERNATIONAL DATA TRANSFERS

8. International Data Transfers

The Company operates through digital infrastructure that may utilise geographically distributed information systems, cloud computing environments, disaster recovery facilities, artificial intelligence infrastructure, communication networks, cybersecurity platforms, and third-party service providers located in different jurisdictions.

Accordingly, Personal Data collected by the Company may be transferred, accessed, processed, stored, hosted, transmitted, backed up, replicated, archived, or otherwise handled outside the territorial boundaries of India where such transfer is necessary for providing the Services, maintaining business continuity, enhancing cybersecurity, complying with Applicable Law, improving Platform functionality, or pursuing other legitimate business purposes.

The Company shall undertake such international transfers only where they are authorised under Applicable Law and shall implement commercially reasonable contractual, organisational, technical, and administrative safeguards designed to protect the confidentiality, integrity, availability, authenticity, and security of Personal Data throughout the transfer lifecycle.

8.1 Circumstances of International Transfer

The Company may transfer Personal Data internationally whenever such transfer is reasonably necessary for hosting the Platform, operating cloud infrastructure, maintaining secure backup systems, providing disaster recovery services, facilitating customer support, performing identity verification, processing payments, operating

Artificial Intelligence systems, conducting cybersecurity monitoring, preventing fraud, generating analytics, carrying out research and product development, complying with legal obligations, maintaining business continuity, administering corporate operations, or providing any other feature or functionality of the Platform.

Such transfers shall always be limited to the extent reasonably necessary for the relevant operational or legal purpose and shall not exceed what is proportionate under Applicable Law.

8.2 Countries and Jurisdictions

Personal Data may be transferred to, processed in, or accessed from jurisdictions where the Company, its Affiliates, subsidiaries, technology partners, cloud infrastructure providers, payment processors, verification agencies, cybersecurity vendors, communication service providers, customer support centres, or other authorised service providers maintain operational facilities.

The User acknowledges that privacy and data protection laws applicable in such jurisdictions may differ from those applicable in India. Nevertheless, the Company shall use reasonable efforts to ensure that recipients of Personal Data implement security measures and privacy protections substantially consistent with this Privacy Policy and Applicable Law.

8.3 Legal Basis for International Transfers

International transfers of Personal Data may be undertaken where such transfers are permitted under the Digital Personal Data Protection Act, 2023, authorised by any notification issued by the Government of India, necessary for the performance of a contract with the User, required for providing the requested Services, necessary for payment processing, fraud prevention, cybersecurity operations, legal compliance, dispute resolution, regulatory reporting, or otherwise permitted under Applicable Law.

Where Applicable Law requires separate User consent for specific categories of international transfers, the Company shall obtain such consent before undertaking the relevant transfer.

8.4 Safeguards Applicable to International Transfers

Before transferring Personal Data outside India, the Company may implement appropriate

technical, contractual, organisational, and administrative safeguards, including encryption of data during transmission and storage, secure communication protocols, role-based access controls, confidentiality agreements, Data Processing

Agreements, non-disclosure obligations, multi-factor authentication, security monitoring, audit mechanisms, cybersecurity controls, disaster recovery measures, vulnerability assessments, penetration testing, and periodic compliance reviews.

Notwithstanding these safeguards, the User acknowledges that no method of electronic transmission or international data transfer can be guaranteed to be entirely secure and that the Company cannot warrant absolute security against every technological risk.

8.5 Cloud Infrastructure and Distributed Processing

The Company may utilise cloud computing infrastructure, geographically distributed servers, content delivery networks, database replication technologies, redundancy mechanisms, disaster recovery environments, and Artificial Intelligence computing resources situated across multiple jurisdictions for improving service availability, operational resilience, cybersecurity, scalability, performance optimisation, and uninterrupted Platform operations.

Accordingly, Personal Data may be temporarily replicated, synchronised, cached, encrypted, archived, or backed up across multiple locations as part of normal technological operations.

8.6 International Service Providers

The Company may engage internationally located service providers, including cloud service providers, hosting providers, payment processors, Artificial Intelligence vendors, cybersecurity consultants, communication providers, customer support providers, analytics providers, verification agencies, auditors, legal advisors, disaster recovery providers, and technology partners.

Such recipients shall receive only the minimum amount of Personal Data reasonably necessary to perform the relevant services and shall remain subject to contractual confidentiality obligations, data protection commitments, cybersecurity standards, and other legal safeguards considered appropriate by the Company.

8.7 User Acknowledgement

By accessing, registering on, or continuing to use the Platform, the User expressly acknowledges and agrees that Personal Data may be transferred to, processed in, stored within, or accessed from jurisdictions outside India for the purposes described in this Privacy Policy.

The User further acknowledges that such international transfers are an essential component of

the Company's global technology infrastructure and may be necessary for ensuring uninterrupted Platform operations, enhanced cybersecurity, business continuity, customer support, Artificial Intelligence services, and other operational functions.

8.8 Government Restrictions

Where any governmental authority, regulatory body, or Applicable Law restricts, prohibits, regulates, or imposes conditions upon the transfer of Personal Data to specified jurisdictions, the Company shall comply with such restrictions to the extent legally required.

The Company reserves the right to modify, suspend, reroute, localise, or otherwise restructure its international data transfer mechanisms whenever necessary to comply with changing legal or regulatory requirements.

8.9 Emergency and Business Continuity Transfers

During cybersecurity incidents, infrastructure failures, force majeure events, natural disasters, public emergencies, legal proceedings, disaster recovery operations, or other exceptional circumstances, the Company may temporarily transfer Personal Data to alternate data centres, recovery environments, or emergency infrastructure located in other jurisdictions where reasonably necessary to restore Platform functionality, preserve Digital Evidence, protect Users, maintain business continuity, or comply with legal obligations.

8.10 General Provisions

Nothing contained in this Chapter shall be construed as requiring the Company to disclose the precise location of its servers, data centres, cybersecurity architecture, encryption methodologies, disaster recovery facilities, cloud configurations, network topology, Artificial Intelligence infrastructure, or any other confidential technical or security-related information. The Company reserves the right to modify, relocate, replace, expand, or discontinue any aspect of its international data processing infrastructure at any time in response to technological developments, operational requirements, cybersecurity considerations, regulatory changes, commercial necessities, or legitimate business interests.

9. DATA SECURITY

10. DATA SECURITY

The Company is committed to maintaining appropriate administrative, organisational, contractual, physical, and technical safeguards to protect the confidentiality, integrity, availability, authenticity, resilience, and security of Personal Data and the information systems used for providing the Services. Such safeguards are designed to prevent unauthorised access, accidental loss, misuse, unlawful disclosure, cyberattacks, system compromise, data corruption,

ransomware incidents, denial-of-service attacks, insider threats, and other security risks.

The Company shall continuously assess, review, enhance, and update its security framework having regard to technological developments, evolving cybersecurity threats, regulatory requirements, industry standards, operational needs, and the sensitivity of the information being Processed. However, no security measure, network, software application, hardware infrastructure, electronic communication, or method of internet transmission can be guaranteed to be completely secure, and the Company does not warrant absolute protection against every conceivable cyber threat or security incident.

10.1 Encryption

The Company may employ commercially reasonable cryptographic technologies and encryption mechanisms to safeguard Personal Data during transmission, storage, backup, replication, disaster recovery, and other Processing activities. Encryption may be applied to databases, communication channels, authentication credentials, backup media, cloud storage, application programming interfaces (APIs), and other technological components where appropriate.

The Company reserves the right to determine the nature, strength, configuration, and implementation of encryption technologies based upon prevailing industry standards, technological feasibility, operational requirements, cybersecurity risks, and Applicable Law. Nothing contained in this Privacy Policy shall require the Company to disclose its encryption architecture, cryptographic keys, key management procedures, security configurations, or other confidential technical information.

10.2 Access Controls

The Company shall implement reasonable access control mechanisms to ensure that Personal Data is accessible only to authorised personnel, service providers, contractors, or other persons having a legitimate business need and appropriate authority.

Such controls may include identity verification, role-based access control, least-privilege principles, multi-factor authentication, privileged access management, password policies, session management, network segmentation, device authentication, access logging, periodic access reviews, and other security measures considered appropriate by the Company.

Access rights may be modified, restricted, suspended, or revoked at any time where necessary to maintain Platform security, comply with Applicable Law, or protect the Company's legitimate interests.

10.3 Security Incident Response

The Company may establish and maintain an information security incident response framework

for detecting, analysing, investigating, containing, mitigating, documenting, recovering from, and responding to actual or suspected cybersecurity incidents affecting the Platform or Personal Data.

Security incidents may include unauthorised access, malware infections, ransomware attacks, phishing attempts, credential compromise, denial-of-service attacks, data breaches, insider misuse, infrastructure failures, software vulnerabilities, account takeovers, fraud, or any other event that may compromise the confidentiality, integrity, or availability of information.

Where required by Applicable Law, the Company may notify competent authorities, affected Users, regulators, or other stakeholders within the timelines prescribed by law.

The Company reserves the right to determine the nature, scope, timing, and content of any notification, subject to legal obligations and operational considerations.

10.4 Security Monitoring and Threat Detection

The Company may continuously monitor its information systems, networks, infrastructure, cloud environments, applications, databases, APIs, communication channels, and digital assets to identify, investigate, prevent, and respond to cybersecurity threats.

Such monitoring may include security logging, audit trails, intrusion detection systems, intrusion prevention systems, endpoint detection and response, behavioural analytics, Artificial Intelligence-assisted threat detection, anomaly detection, fraud monitoring, vulnerability scanning, penetration testing, threat intelligence, security information and event management (SIEM), digital forensics, and continuous risk assessments.

The Company reserves the right to collect, retain, analyse, and preserve system logs, metadata, access records, and other Digital Evidence for security, legal compliance, fraud prevention, and dispute resolution purposes.

10.5 CERT-In Compliance and Regulatory Obligations

The Company shall endeavour to comply with all cybersecurity obligations applicable under the Information Technology Act, 2000, the rules framed thereunder, directions issued by the Indian Computer Emergency Response Team (CERT-In), and other Applicable Laws.

Where legally required, the Company may maintain cybersecurity logs, preserve Digital Evidence, report specified cybersecurity incidents, cooperate with governmental authorities, provide information to competent agencies, implement incident reporting procedures, and retain relevant technical information for the duration prescribed under Applicable Law.

Nothing contained in this Privacy Policy shall limit the Company's right or obligation to cooperate with CERT-In, law enforcement agencies, regulatory authorities, or judicial bodies in connection with cybersecurity investigations or legal proceedings.

10.6 Cybersecurity Practices

The Company may implement a comprehensive cybersecurity programme comprising administrative, technical, contractual, and organisational safeguards designed to reduce cybersecurity risks and strengthen operational resilience.

Such safeguards may include secure software development practices, vulnerability management, periodic security assessments, penetration testing, source code reviews, security awareness programmes, employee training, endpoint protection, firewall management, anti-malware technologies, data loss prevention systems, network security controls, email security, patch management, privileged access management, Artificial

Intelligence-assisted cybersecurity tools, third-party security assessments, vendor risk management, and periodic policy reviews.

The Company reserves the right to revise, enhance, replace, or discontinue any cybersecurity measure whenever necessary to address evolving threats, regulatory requirements, technological developments, or operational needs.

10.7 Disaster Recovery

The Company may establish disaster recovery plans and technical recovery mechanisms intended to restore critical business operations following cyber incidents, infrastructure failures, natural disasters, hardware failures, software corruption, telecommunications outages, power disruptions, force majeure events, or other operational emergencies.

Disaster recovery measures may include encrypted backups, geographically distributed infrastructure, redundant systems, database replication, cloud-based recovery environments, emergency communication procedures, recovery testing, restoration protocols, and contingency planning.

The Company does not guarantee uninterrupted availability of the Platform during disaster recovery operations and reserves the right to suspend, restrict, or temporarily discontinue Services where necessary to protect Users, preserve data integrity, or restore secure operations.

10.8 Business Continuity

The Company may maintain a Business Continuity Management Framework designed to support the continued operation of essential business functions during emergencies, cybersecurity incidents, infrastructure failures, pandemics, public emergencies, labour disruptions,

governmental actions, force majeure events, or other unforeseen circumstances.

Business continuity measures may include operational redundancy, alternative communication channels, remote operational capabilities, emergency response procedures, succession planning, data backup strategies, infrastructure resilience, vendor continuity planning, crisis management protocols, and periodic continuity testing.

While the Company shall use commercially reasonable efforts to minimise operational disruption, uninterrupted availability of the Platform cannot be guaranteed under all circumstances.

10.9 User Security Responsibilities

Users are responsible for maintaining the confidentiality and security of their account credentials, passwords, authentication devices, one-time passwords (OTPs), recovery codes, and other security information associated with their Accounts.

Users shall immediately notify the Company upon becoming aware of any actual or suspected unauthorised access, credential compromise, phishing attempt, fraudulent activity, or other security incident affecting their Account.

The Company shall not be liable for any loss arising from the User's failure to maintain appropriate security practices, safeguard authentication credentials, or comply with the security obligations set forth in the Terms of Use.

10.10 Preservation of Digital Evidence

The Company may preserve Electronic Records, audit logs, system logs, access records, authentication records, metadata, communication records, forensic images, transaction histories, and other Digital Evidence where reasonably necessary for cybersecurity investigations, fraud prevention, legal proceedings, dispute resolution, regulatory compliance, internal investigations, insurance claims, or enforcement of the Company's legal rights.

Such Digital Evidence may be retained, analysed, disclosed, or produced before competent authorities, courts, arbitral tribunals, regulators, or law enforcement agencies in accordance with Applicable Law.

10.11 Limitation of Security Liability

Notwithstanding the implementation of reasonable security measures, the Company does not warrant that the Platform, its infrastructure, networks, databases, cloud environments, software applications, APIs, communication systems, or security controls shall be completely free from cyberattacks, malware, ransomware, hacking attempts, unauthorised access, security vulnerabilities, or other technological risks.

To the fullest extent permitted by Applicable Law, the Company shall not be liable for any loss, damage, interruption, corruption, disclosure, alteration, destruction, theft, delay, or unauthorised access resulting from events beyond its reasonable control, including sophisticated cyberattacks, zero-day vulnerabilities, failures of third-party infrastructure, internet outages, telecommunications failures, force majeure events, governmental actions, or acts or omissions of Users or third parties.

10.12 General Provisions

Nothing contained in this Chapter shall require the Company to disclose confidential security policies, network architecture, infrastructure topology, encryption methodologies, authentication mechanisms, vulnerability assessments, penetration testing reports, incident response procedures, Digital Forensics techniques, Artificial

Intelligence security models, trade secrets, or any other information that could reasonably compromise the security of the Platform or prejudice the Company's legitimate business interests.

The Company reserves the right to modify, enhance, replace, supplement, or discontinue any security measure, technology, policy, framework, or operational practice whenever necessary to address technological innovation, evolving cybersecurity threats, legal developments, regulatory requirements, operational needs, or recognised industry standards.

For a document of this size, it's best to draft one chapter at a time to maintain consistency, legal precision, and readability. Below is Chapter 11 in the same enterprise-grade, paragraph-style format.

DATA RETENTION & DELETION

11. DATA RETENTION & DELETION

The Company shall retain Personal Data only for such period as is reasonably necessary to fulfil the purposes described in this Privacy Policy, comply with Applicable Law, perform contractual obligations, resolve disputes, enforce legal rights, prevent fraud, maintain cybersecurity, preserve Digital Evidence, and support legitimate business operations.

Retention periods shall be determined having regard to the nature of the Personal Data, the purpose for which it was collected, statutory limitation periods, legal and regulatory obligations, contractual requirements, litigation risks, cybersecurity considerations, operational necessities, and recognised industry practices. The Company may periodically review, revise, or update its retention schedules to reflect changes in law, technology, business operations, or regulatory requirements.

11.1 Retention of Personal Data

The Company may retain Personal Data for the duration of the User's relationship with the Platform and thereafter for such additional period as may be reasonably necessary to fulfil legal, contractual, regulatory, accounting, taxation, audit, fraud prevention, cybersecurity, insurance, dispute resolution, business continuity, archival, or evidentiary purposes.

Where Personal Data is no longer required for the purpose for which it was collected, the Company may delete, anonymise, pseudonymise, archive, aggregate, or otherwise render such information incapable of identifying an individual, unless continued retention is required or permitted under Applicable Law.

11.2 Retention of Electronic Records and Digital Evidence

Notwithstanding any other provision of this Privacy Policy, the Company may preserve Electronic Records, system logs, audit trails, metadata, authentication records, communication records, transaction histories, verification records, security logs, forensic data, backups, and other Digital Evidence where such preservation is reasonably necessary for legal proceedings, arbitration, mediation, regulatory investigations, law enforcement requests, cybersecurity investigations, fraud prevention, insurance claims, internal investigations, contractual enforcement, or protection of the Company's legal rights.

The retention of such records shall not be construed as evidence that the underlying User Account remains active or that the relevant Services continue to be available.

11.3 Account Closure and Data Deletion

Where a User permanently closes an Account or requests deletion of Personal Data, the Company shall, subject to Applicable Law, take reasonable steps to delete or anonymise the Personal Data within a commercially reasonable period.

The Company shall, however, be entitled to retain information where retention is required for legal compliance, taxation, accounting, regulatory obligations, fraud prevention, cybersecurity, Digital Evidence preservation, dispute resolution, enforcement of contractual rights, protection of legitimate interests, or any other purpose authorised under Applicable Law.

Deletion of Personal Data from active systems does not necessarily require immediate removal from encrypted backup systems, disaster recovery environments, archival media, audit logs, or legally required records, which may continue to be retained until overwritten or deleted in accordance with the Company's internal retention schedules.

11.4 Anonymisation and Pseudonymisation

Where reasonably practicable, the Company may anonymise or pseudonymise Personal

Data to minimise privacy risks while enabling statistical analysis, research, Artificial Intelligence improvement, cybersecurity monitoring, business intelligence, service enhancement, product development, and other legitimate business activities.

Information that has been irreversibly anonymised so that it no longer identifies, or is reasonably capable of identifying, an individual shall cease to constitute Personal Data for the purposes of this Privacy Policy, subject to Applicable Law.

11.5 Secure Deletion and Disposal

The Company shall implement commercially reasonable administrative, technical, and organisational measures for the secure deletion, destruction, disposal, or overwriting of Personal Data when retention is no longer required.

Such measures may include secure erasure, cryptographic deletion, physical destruction of storage media, degaussing, certified disposal procedures, secure overwrite techniques, or other recognised methods appropriate to the nature of the information and the storage medium.

The Company reserves the right to determine the most appropriate deletion methodology based upon technological feasibility, operational requirements, cybersecurity considerations, and applicable legal obligations.

11.6 Suspension of Deletion

The Company may suspend, postpone, or refuse deletion of Personal Data where such information is subject to a litigation hold, judicial order, arbitral proceedings, regulatory investigation, governmental direction, law enforcement request, contractual dispute, fraud investigation, cybersecurity incident, insurance claim, audit requirement, or any other legal or operational necessity requiring continued preservation.

During such period, the Personal Data may continue to be retained, processed, and preserved solely for the purposes for which the retention is legally justified.

11.7 User Acknowledgement

The User acknowledges and agrees that deletion of Personal Data may result in the permanent loss of profile information, communications, preferences, subscription benefits, verification status, recommendations, transaction history, and other Platform functionalities. The Company shall not be responsible for restoring deleted information unless restoration is technically feasible and required under Applicable Law.

The User further acknowledges that certain copies of information may remain within encrypted backups, archival systems, security logs, or disaster recovery environments until the normal lifecycle of such systems permits their deletion.

11.8 General Provisions

Nothing contained in this Chapter shall require the Company to delete information that it is legally required or otherwise lawfully entitled to retain, nor shall it restrict the Company's right to preserve Electronic Records, Digital Evidence, audit logs, security records, or anonymised information for lawful purposes. The Company reserves the right to revise its retention and deletion practices in response to changes in Applicable Law, regulatory guidance, technological developments, cybersecurity requirements, operational needs, or recognised industry standards.

RIGHTS OF USERS / DATA PRINCIPALS

12. RIGHTS OF USERS / DATA PRINCIPALS

The Company recognises that Users and Data Principals possess certain statutory rights concerning their Personal Data. The Company shall implement reasonable administrative and technical mechanisms to facilitate the exercise of such rights in accordance with Applicable Law.

The exercise of any right under this Chapter shall be subject to appropriate identity verification, authentication procedures, fraud prevention measures, cybersecurity safeguards, contractual obligations, and legal restrictions. The Company reserves the right to refuse, defer, partially comply with, or impose reasonable conditions upon any request where permitted under Applicable Law or where necessary to protect the rights, freedoms, safety, security, confidentiality, intellectual property, or legitimate interests of the Company, other Users, or third parties.

12.1 Right to Information

Subject to Applicable Law, a User or Data Principal may request information regarding the Personal Data Processed by the Company, including the categories of Personal Data collected, the purposes of Processing, the categories of recipients with whom such Personal Data has been shared, the lawful basis of Processing, the retention practices adopted by the Company, and such other information as may be required to be disclosed under Applicable Law.

The Company may decline to disclose information where such disclosure would reveal trade secrets, confidential commercial information, cybersecurity measures, proprietary algorithms, intellectual property, privileged communications, information relating to other Users, or any information exempt from disclosure under Applicable Law.

12.2 Right to Access

Subject to verification of identity and compliance with Applicable Law, the User may request access to Personal Data maintained by the Company.

The Company may provide access through electronic means, user dashboards, account interfaces, downloadable reports, secure communications, or any other method considered appropriate by the Company.

The Company may refuse or limit access where disclosure would adversely affect the rights of another person, compromise cybersecurity, prejudice ongoing investigations, interfere with legal proceedings, reveal confidential business information, or otherwise fall within any statutory exemption recognised under Applicable Law.

The Company may prescribe reasonable procedures, authentication requirements, and response timelines for processing access requests.

12.3 Right to Correction and Updating of Personal Data

A User may request correction, completion, updating, or rectification of inaccurate, incomplete, misleading, outdated, or incorrect Personal Data maintained by the Company.

The Company may require documentary evidence or other reasonable verification before implementing any requested correction where accuracy cannot reasonably be established.

The Company shall not be responsible for inaccuracies arising from information supplied by the User, third parties, governmental databases, verification agencies, or circumstances beyond the Company's reasonable control.

The Company reserves the right to retain historical versions of corrected information where necessary for legal compliance, fraud prevention, cybersecurity, Digital Evidence preservation, audit purposes, dispute resolution, contractual enforcement, or regulatory obligations.

12.4 Right to Erasure

Subject to Applicable Law, a User may request deletion or erasure of Personal Data that is no longer required for the purposes for which it was collected or where such deletion is otherwise required by law.

The Company may decline or postpone deletion where continued retention is necessary for compliance with Applicable Law, contractual obligations, taxation, accounting, fraud prevention, cybersecurity, legal proceedings, insurance claims, audit requirements, dispute resolution, Digital Evidence preservation, protection of legal rights, or any other lawful purpose.

Deletion from active systems does not necessarily require immediate deletion from backup systems, disaster recovery environments, archival storage, audit logs, security logs, or other

legally retained records.

Where deletion is not reasonably practicable, the Company may instead anonymise or pseudonymise the relevant information in accordance with Applicable Law.

12.5 Right to Withdraw Consent

Where the Processing of Personal Data is based upon the User's Consent, the User may withdraw such Consent at any time using the mechanisms provided by the Company or by contacting the designated Grievance Officer.

Withdrawal of Consent shall operate prospectively and shall not affect the lawfulness of any Processing undertaken before such withdrawal or Processing undertaken on any other lawful basis recognised under Applicable Law.

The User acknowledges that withdrawal of Consent may result in suspension, restriction, reduction, or termination of certain Services, Platform functionalities, subscription benefits, verification services, AI-powered features, personalised recommendations, communications, or other features that depend upon such Consent.

The Company shall not be liable for any loss of functionality or inability to provide Services resulting solely from the withdrawal of Consent.

12.6 Right to Grievance Redressal

A User who has any concern regarding the collection, Processing, disclosure, retention, security, or use of Personal Data may submit a grievance to the Company's designated Grievance Officer or such other authority as may be notified by the Company.

The Company shall endeavour to acknowledge, investigate, and resolve grievances within the timelines prescribed under Applicable Law or within a commercially reasonable period where no statutory timeline exists.

The Company may require the User to provide sufficient information to verify identity, understand the grievance, and enable an appropriate investigation before taking corrective action.

Submission of a grievance shall not prejudice the Company's legal rights or prevent the Company from taking appropriate action to protect its legitimate interests, other Users, or the integrity of the Platform.

12.7 Right to Nominate

Where recognised under Applicable Law, a User may nominate one or more individuals to exercise specified privacy-related rights on the User's behalf in the event of death, incapacity, or such other circumstances as may be recognised under law.

The Company may require documentary evidence establishing the authority, identity, legal status, or entitlement of the nominee before acting upon any such request.

The Company reserves the right to decline any nomination request where the authenticity of the nomination cannot reasonably be verified, where conflicting claims exist, where legal proceedings are pending, or where compliance would otherwise violate

Applicable Law.

12.8 Right to Complaint

Where a User believes that the Company has failed to comply with Applicable Law or has not satisfactorily addressed a grievance, the User may exercise the right to approach the competent statutory authority, regulatory body, or other authority having jurisdiction under Applicable Law.

Nothing contained in this Privacy Policy shall restrict or waive any statutory right available to a User under the Digital Personal Data Protection Act, 2023, or any other

Applicable Law.

However, the Company encourages Users to first utilise the Company's internal grievance redressal mechanism to facilitate prompt, efficient, and amicable resolution of concerns wherever reasonably practicable.

12.9 Verification of Requests

Before acting upon any request under this Chapter, the Company may require the User to complete reasonable identity verification procedures, provide supporting documentation, authenticate account ownership, answer security questions, or comply with any other authentication measures considered necessary to prevent fraud, identity theft, unauthorised disclosures, or misuse of privacy rights.

The Company may refuse to process any request that cannot be reasonably authenticated or that appears fraudulent, malicious, repetitive, excessive, abusive, or otherwise inconsistent with Applicable Law.

12.10 Limitations on the Exercise of Rights

The rights described in this Chapter shall not be absolute and shall remain subject to statutory exemptions, legal restrictions, judicial orders, regulatory directions, contractual obligations, protection of third-party rights, confidentiality obligations, legal privilege, cybersecurity requirements, fraud prevention measures, preservation of Electronic

Records, Digital Evidence retention, intellectual property protection, national security considerations, and other lawful limitations recognised under Applicable Law.

The Company reserves the right to refuse, restrict, defer, or condition any request where

necessary to comply with such limitations.

12.11 No Waiver of Legal Rights

Nothing contained in this Chapter shall:

- require the Company to disclose confidential business information, proprietary algorithms, trade secrets, security architecture, or privileged communications;
- require deletion of information that the Company is legally required or lawfully entitled to retain;
- prejudice the Company's rights to preserve Electronic Records or Digital Evidence;
- limit the Company's rights relating to fraud prevention, cybersecurity, dispute resolution, regulatory compliance, or contractual enforcement; or
- create any obligation beyond those imposed under Applicable Law.

CHILDREN'S PRIVACY

13. CHILDREN'S PRIVACY

The Company is committed to protecting the privacy, safety, and Personal Data of children. The Platform is designed exclusively for individuals who are legally competent to enter into binding contracts and who satisfy the eligibility requirements prescribed under the Terms of Use and Applicable Law.

Accordingly, the Platform is not intended for use by children, and the Company does not knowingly permit children to register Accounts, access the Services, create Profiles, subscribe to memberships, or otherwise use the Platform except where expressly permitted under Applicable Law and supported by legally valid parental or guardian authorisation.

13.1 Age Eligibility

Users shall access and use the Platform only if they have attained the minimum age prescribed under Applicable Law and possess the legal capacity to enter into binding agreements.

The Company reserves the right to prescribe higher minimum age requirements for specific Services, Premium Services, verification programmes, promotional activities, or other Platform features where considered appropriate for legal, operational, safety, or business reasons.

Any registration or use of the Platform by a person who does not satisfy the prescribed eligibility requirements shall constitute a material violation of the Terms of Use.

13.2 No Knowing Collection of Children's Personal Data

The Company does not knowingly solicit, collect, Process, store, disclose, or otherwise handle Personal Data relating to a child except where such Processing is expressly authorised or required under Applicable Law.

If the Company becomes aware, through any means, that Personal Data belonging to a child has been collected without the legally required authorisation, the Company may immediately suspend the relevant Account, restrict access to the Services, seek additional verification, delete or anonymise the relevant Personal Data, or take such other action as the Company considers appropriate or as may be required under Applicable Law.

Nothing contained in this Privacy Policy shall require the Company to independently investigate the age of every User unless circumstances reasonably indicate that such verification is necessary.

13.3 Age Verification

The Company reserves the right, at any time and without prior notice, to require Users to provide reasonable proof of age, identity, legal capacity, or eligibility before permitting access to all or any part of the Platform.

Age verification may be conducted through documentary verification, government- issued identification, digital identity verification services, Artificial Intelligence-assisted verification technologies, third-party verification agencies, biometric comparison where legally permissible, or any other lawful verification mechanism considered appropriate by the Company.

Failure to satisfactorily complete any verification process may result in suspension, restriction, or permanent termination of the relevant Account without liability to the Company.

13.4 Parental or Lawful Guardian Consent

Where Applicable Law permits the Processing of Personal Data relating to a child subject to verifiable parental or lawful guardian consent, the Company may implement reasonable mechanisms to verify the identity and authority of the parent or lawful guardian before commencing such Processing.

The Company may require documentary evidence establishing parental authority, guardianship, identity, legal relationship, age, or any other information reasonably necessary to comply with Applicable Law.

The Company reserves the right to refuse or discontinue Processing where satisfactory verification cannot be completed.

13.5 Restricted Processing of Children's Data

Where Personal Data relating to a child is lawfully Processed, the Company shall limit such Processing to the minimum extent reasonably necessary for the lawful purpose for which it is collected.

The Company shall endeavour to implement appropriate administrative, organisational, contractual, and technical safeguards designed to protect such Personal Data against unauthorised access, disclosure, misuse, alteration, destruction, profiling, behavioural tracking, cyber threats, or unlawful Processing.

The Company shall not knowingly Process children's Personal Data for purposes prohibited under Applicable Law, including unlawful behavioural monitoring, targeted advertising directed specifically at children where prohibited, or any activity likely to cause material harm to a child.

13.6 AI Systems and Children's Data

The Company does not knowingly use Artificial Intelligence systems, automated profiling, recommendation engines, behavioural analytics, or automated decision-making technologies in relation to a child's Personal Data except where expressly permitted under Applicable Law and subject to appropriate safeguards.

Where legally required, any AI-assisted Processing involving children's Personal Data shall remain subject to enhanced governance measures, additional security controls, human oversight, and other protections considered appropriate by the Company.

13.7 Removal of Children's Personal Data

Where the Company becomes aware that Personal Data relating to a child has been collected contrary to this Privacy Policy or Applicable Law, the Company may take reasonable steps to delete, anonymise, restrict, or otherwise cease Processing such information within a commercially reasonable period, subject to any legal obligation requiring its continued retention. Nothing contained herein shall require immediate deletion of information that is required to be retained for legal compliance, fraud prevention, cybersecurity, preservation of Digital Evidence, judicial proceedings, regulatory investigations, or protection of the Company's legal rights.

13.8 Responsibility of Parents and Guardians

Parents and lawful guardians are responsible for supervising children's online activities and ensuring that children do not provide Personal Data to the Company in violation of this Privacy Policy or Applicable Law.

If a parent or lawful guardian reasonably believes that a child has submitted Personal Data through the Platform without appropriate authorisation, the parent or lawful guardian may contact the Company's designated Grievance Officer or Privacy Contact to request review, verification, restriction, correction, or deletion of such information, subject to identity verification and Applicable Law.

The Company may require reasonable documentary evidence before acting upon any such request.

13.9 Educational, Research and Public Interest Exceptions

Nothing contained in this Chapter shall prevent the Company from Processing information relating to children where such Processing is expressly authorised, mandated, or exempted under Applicable Law, judicial orders, governmental directions, regulatory notifications, or any recognised statutory exception.

Any such Processing shall remain subject to appropriate legal safeguards and the principles of necessity, proportionality, transparency, security, and accountability.

13.10 Limitation of Liability

The Company shall not be responsible for any inaccurate declaration of age, forged identity documents, false representations, misstatements, unauthorised use of another person's identity, or any other fraudulent act committed by a User or third party for the purpose of obtaining access to the Platform.

To the fullest extent permitted under Applicable Law, the Company shall not be liable for any consequences arising solely from reliance upon information, declarations, documents, or representations provided by Users regarding their age or legal capacity, provided that the Company has acted in good faith and exercised reasonable diligence consistent with Applicable Law.

13.11 General Provisions

Nothing contained in this Chapter shall:

- require the Company to independently verify the age of every User in the absence of circumstances reasonably warranting such verification;

- prejudice the Company's rights to suspend, restrict, terminate, or investigate

Accounts suspected of being operated by children or persons lacking legal capacity;

- affect the Company's rights relating to fraud prevention, cybersecurity, preservation of Electronic Records, Digital Evidence, or legal compliance;

- limit the Company's statutory rights or obligations under Applicable Law; or

- create any representation or warranty that every individual accessing the

Platform has been independently age verified by the Company.

The Company reserves the right to amend, strengthen, or supplement its child privacy practices at any time to reflect changes in legislation, regulatory guidance, technological developments, recognised industry standards, or operational requirements.

THIRD-PARTY LINKS & SERVICES

14. THIRD-PARTY LINKS & SERVICES

The Platform may contain hyperlinks, embedded content, application programming interfaces (APIs), software integrations, payment gateways, social media integrations, cloud services, Artificial Intelligence services, verification services, communication tools, advertising technologies, plugins, widgets, or other features that enable Users to interact with websites, applications, products, or services operated by third parties.

The inclusion, availability, integration, advertisement, or accessibility of any third-party service through the Platform shall not constitute or imply any endorsement, certification, sponsorship, recommendation, guarantee, representation, partnership, agency, employment, joint venture, or approval by the Company unless expressly stated in writing.

Users acknowledge that they access and use third-party services entirely at their own discretion and risk.

14.1 Independent Third-Party Services

Various features available through the Platform may be provided, operated, maintained, hosted, or supported by independent third parties over whom the Company has no ownership, management, operational control, or supervisory authority.

Such third-party services may include payment gateways, cloud hosting providers, communication platforms, identity verification agencies, Artificial Intelligence providers, mapping services, analytics providers, advertising networks, customer support platforms, authentication services, social media platforms, video conferencing services, cybersecurity vendors, logistics providers, or other technology partners.

The Company neither controls nor assumes responsibility for the availability, functionality, security, legality, quality, accuracy, reliability, or continuity of any third-party service.

14.2 Third-Party Websites and External Links

The Platform may provide hyperlinks, banners, advertisements, QR codes, embedded pages, redirect links, referral links, or other electronic references directing Users to external websites or digital platforms operated by third parties.

Once a User leaves the Platform or accesses a third-party resource, the Company shall have no control over the content, policies, security practices, availability, or operation of such external website or service.

Users are encouraged to independently review the applicable terms of use, privacy policies, cookie policies, security practices, and other legal documents of every third-party website

before providing Personal Data, making payments, downloading software, or engaging in any transaction.

14.3 Third-Party Privacy Practices

The Company shall not be responsible for the manner in which third parties collect, Process, store, disclose, retain, transfer, monetise, analyse, or otherwise use Personal Data after a User voluntarily accesses or interacts with such third-party services. Any Personal Data collected directly by a third party shall be governed exclusively by the applicable privacy policy and contractual terms of that third party.

The Company does not guarantee that third parties maintain privacy, cybersecurity, or data protection standards equivalent to those adopted by the Company or required under Indian law.

14.4 Third-Party Payment Services

Payments made through the Platform may be processed by independent banks, payment aggregators, payment gateways, Unified Payments Interface (UPI) providers, card networks, financial institutions, digital wallet providers, recurring payment processors, or other licensed payment service providers.

The Company shall not be responsible for delays, transaction failures, payment reversals, banking interruptions, settlement errors, chargebacks, payment fraud, unauthorised transactions, processing failures, currency conversion issues, network downtime, or technical malfunctions occurring within the systems or infrastructure of such third-party payment providers. Users shall comply with the contractual terms and policies of the relevant payment service provider while completing financial transactions.

14.5 Social Media Platforms

The Platform may permit Users to interact with, connect, authenticate through, or share content using third-party social media platforms or social login services.

Where a User voluntarily links a social media account with the Platform, the Company may receive limited information from such third-party platform in accordance with the permissions granted by the User and the privacy settings selected on that platform.

The Company shall not be responsible for any collection, disclosure, publication, profiling, tracking, or other Processing activities undertaken independently by social media providers.

14.6 Artificial Intelligence and Technology Providers

The Company may utilise third-party Artificial Intelligence systems, cloud computing services, machine learning infrastructure, language models, automated moderation systems, fraud

detection technologies, cybersecurity platforms, identity verification solutions, analytics engines, or recommendation technologies for improving the Services.

The Company does not warrant that outputs generated by any third-party Artificial Intelligence service shall be accurate, complete, unbiased, uninterrupted, suitable for any specific purpose, or free from technical errors.

Users acknowledge that certain Platform functionalities may depend upon third-party AI technologies that remain subject to independent technical limitations and operational constraints.

14.7 Third-Party Content

Content displayed through the Platform may include information, advertisements, profiles, reviews, ratings, testimonials, promotional material, publications, media, videos, photographs, articles, blogs, or other material supplied by independent third parties.

The Company neither verifies nor guarantees the authenticity, legality, completeness, reliability, accuracy, or suitability of such third-party content and expressly disclaims responsibility for any reliance placed upon it.

Users shall independently evaluate all third-party information before making personal, financial, matrimonial, legal, commercial, or other decisions.

14.8 Third-Party Advertisements

The Platform may display advertisements, sponsored listings, promotional campaigns, affiliate links, or marketing content supplied by advertisers or advertising networks.

The appearance of any advertisement shall not constitute an endorsement, certification, recommendation, warranty, or guarantee by the Company regarding the advertiser, its products, or its services.

All transactions, communications, warranties, representations, complaints, refunds, or disputes arising from interactions between a User and any advertiser shall be solely between the User and the relevant third party.

14.9 APIs and Technology Integrations

The Platform may communicate with external software, APIs, cloud infrastructure, databases, authentication systems, payment processors, verification services, messaging platforms, government databases where legally permitted, cybersecurity systems, or other technology providers for operational purposes.

The Company reserves the right to modify, replace, suspend, discontinue, or introduce any third-party integration without prior notice where reasonably necessary for legal compliance,

technological advancement, cybersecurity, operational efficiency, or business continuity.

The Company shall not be liable for interruptions, incompatibility, service degradation, data delays, API failures, software defects, or technological limitations attributable to third-party systems.

14.10 Limitation of Liability

To the fullest extent permitted under Applicable Law, the Company shall not be liable for any direct, indirect, incidental, consequential, exemplary, punitive, special, economic, reputational, or other loss arising from or relating to:

- the availability or unavailability of third-party services;
- acts or omissions of third-party providers;
- third-party cybersecurity incidents or data breaches;
- payment failures or banking interruptions;
- third-party software defects or vulnerabilities;
- inaccurate information supplied by third parties;
- third-party Artificial Intelligence outputs;
- unauthorised disclosures by external platforms;
- contractual disputes between Users and third parties;
- advertisements, sponsored content, or promotional offers; or
- any transaction or relationship established independently between a User and a third party.

Nothing in this Chapter shall exclude or limit liability where such exclusion or limitation is prohibited under Applicable Law.

14.11 User Responsibility

Users are solely responsible for exercising appropriate caution before interacting with any third-party website, service, software, advertiser, payment provider, social media platform, Artificial Intelligence tool, or other external resource accessible through the Platform.

Users shall independently verify the authenticity, legality, security, and suitability of any third-party service before providing Personal Data, making payments, downloading software, sharing confidential information, or entering into contractual relationships.

The Company shall not be responsible for any loss arising from the User's voluntary engagement with third-party services.

14.12 General Provisions

Nothing contained in this Chapter shall:

- create any partnership, agency, joint venture, fiduciary relationship, employment relationship, or representation between the Company and any third party;
- require the Company to monitor, supervise, verify, audit, or guarantee third-party services;
- restrict the Company's right to add, remove, replace, suspend, or modify third-party integrations at any time;
- prejudice the Company's rights relating to fraud prevention, cybersecurity, Digital Evidence preservation, legal compliance, or protection of its legitimate business interests; or
- limit the applicability of the Terms of Use, Privacy Policy, Cookie Policy, AI Governance Policy, Data Security Policy, or any other policy forming part of the Company's integrated legal and governance framework.

ADVERTISEMENTS & ANALYTICS

15. ADVERTISEMENTS & ANALYTICS

The Company may display advertisements, sponsored content, promotional campaigns, recommendations, featured listings, affiliate promotions, marketing communications, or other commercial content through the Platform to improve User experience, promote Services, support Platform operations, generate revenue, measure marketing effectiveness, and facilitate business growth.

The Company may also utilise analytics technologies, Artificial Intelligence systems, statistical models, behavioural analysis tools, and performance measurement technologies to understand User interactions, optimise Platform functionality, improve security, detect fraud, enhance customer experience, evaluate business performance, and support research and development.

15.1 Advertisements

The Platform may display advertisements relating to the Company's own products and services or those of third-party advertisers, business partners, affiliates, sponsors, marketing agencies, or authorised promotional partners.

Advertisements may appear in various forms, including banners, featured profiles, sponsored search results, promotional emails, in-application notifications, push notifications, recommendations, videos, interactive content, affiliate links, or other marketing formats.

The display of any advertisement shall not constitute an endorsement, recommendation, certification, warranty, or representation by the Company regarding the advertiser or the advertised products or services unless expressly stated otherwise.

15.2 Personalised Advertising

Subject to Applicable Law and any Consent requirements, the Company may use Personal

Data, usage information, preferences, subscription history, profile information, demographic information, device information, approximate location, behavioural patterns, and engagement metrics to personalise advertisements, recommendations, promotional offers, and marketing communications.

Personalisation is intended to improve the relevance of advertisements and enhance the overall User experience. However, the Company does not guarantee that personalised advertisements or recommendations will always correspond with the User's interests, preferences, or expectations.

Where Applicable Law requires prior Consent for personalised advertising or targeted marketing, the Company shall obtain such Consent before undertaking the relevant Processing.

15.3 Promotional Communications

The Company may send newsletters, promotional messages, service announcements, product updates, event invitations, surveys, educational content, subscription reminders, discount offers, loyalty programme information, referral programme communications, and other marketing communications through email, SMS, telephone calls, instant messaging services, push notifications, or other legally permissible communication channels.

Users may opt out of receiving non-essential promotional communications by following the unsubscribe instructions provided in such communications or by updating their communication preferences through the Platform. Withdrawal of marketing preferences shall not affect transactional communications, legal notices, security alerts, account-related notifications, billing information, or other communications necessary for providing the Services or complying with Applicable Law.

15.4 Analytics

The Company may collect and analyse information relating to User behaviour, Platform usage, navigation patterns, device characteristics, feature utilisation, session duration, traffic sources, search activity, interaction history, error reports, crash logs, performance metrics, subscription trends, conversion rates, and other operational information for analytical purposes.

Such analytics may assist the Company in improving Platform performance, enhancing user experience, strengthening cybersecurity, preventing fraud, developing new products and services, monitoring operational efficiency, conducting business planning, and fulfilling legitimate business interests.

Analytics information may be processed in aggregated, pseudonymised, anonymised, or

identifiable form depending upon the relevant purpose and Applicable Law.

15.5 Artificial Intelligence and Predictive Analytics

The Company may utilise Artificial Intelligence systems, machine learning technologies, predictive analytics, recommendation engines, statistical models, natural language processing technologies, automated classification systems, and behavioural analysis tools to analyse User interactions, improve matchmaking, personalise Platform features, optimise advertisements, detect fraudulent activities, identify security threats, improve customer support, and enhance operational efficiency.

Outputs generated by Artificial Intelligence systems are based upon available information, statistical probabilities, algorithmic processing, and machine learning models and may not always be complete, accurate, current, or free from bias. Users should exercise independent judgment and should not rely exclusively upon AI-generated recommendations when making personal, matrimonial, financial, legal, or other important decisions.

15.6 Third-Party Analytics Providers

The Company may engage independent analytics providers, advertising technology partners, marketing platforms, customer engagement providers, cloud service providers, Artificial Intelligence vendors, data measurement providers, social media platforms, and similar technology partners to assist in measuring Platform performance and marketing effectiveness. Such third parties may utilise Cookies, SDKs, APIs, web beacons, pixels, device identifiers, log files, or similar technologies in accordance with their own contractual obligations and Applicable Law.

The Company shall use commercially reasonable efforts to engage reputable service providers; however, it does not control the independent privacy practices, security measures, or operational policies of such third parties.

15.7 Advertising Measurement and Performance

The Company may measure the effectiveness of advertisements, promotional campaigns, referral programmes, sponsored content, affiliate marketing initiatives, and customer acquisition activities by analysing impressions, clicks, conversions, engagement rates, subscription activity, campaign performance, return on investment, customer retention, and other relevant metrics. Such measurements may be conducted using first-party technologies, third-party analytics tools, Artificial Intelligence systems, or statistical methodologies considered appropriate by the Company.

15.8 Cookies and Advertising Technologies

Advertisements and analytics may rely upon Cookies, tracking pixels, local storage technologies, software development kits (SDKs), advertising identifiers, browser technologies, device identifiers, APIs, and other technical mechanisms described in the Company's Cookies & Tracking Technologies Chapter.

Users may manage their Cookie preferences through browser settings, consent management tools, or Platform controls where available. Disabling certain Cookies may affect the availability, relevance, accuracy, or functionality of advertisements, recommendations, analytics, or other Platform features.

15.9 Data Sharing for Advertising and Analytics

Where permitted under Applicable Law, the Company may disclose limited information to authorised advertising partners, analytics providers, Affiliates, technology vendors, marketing agencies, cloud service providers, measurement partners, or other authorised service providers solely for purposes relating to advertising, campaign management, analytics, fraud prevention, service improvement, business intelligence, or operational support.

The Company shall not sell Personal Data as a commercial commodity unless expressly authorised by the User or otherwise permitted under Applicable Law. Any disclosure of Personal Data shall remain subject to contractual confidentiality obligations, appropriate security safeguards, and the provisions of this Privacy Policy.

15.10 User Choices

Users may exercise available choices regarding marketing communications, Cookies, personalised advertisements, communication preferences, and other advertising-related settings through the mechanisms provided by the Platform or by contacting the Company.

The Company may require reasonable verification of identity before implementing certain requests. Users acknowledge that opting out of personalised advertising does not necessarily eliminate advertisements altogether, and they may continue to receive contextual, generic, service-related, or legally required communications.

15.11 Limitation of Liability

The Company does not warrant that advertisements, promotional offers, recommendations, sponsored listings, analytics reports, behavioural insights, Artificial Intelligence outputs, or marketing communications will always be accurate, complete, current, uninterrupted, suitable, error-free, or relevant to every User.

To the fullest extent permitted under Applicable Law, the Company shall not be liable for any

loss, damage, expense, claim, or liability arising from reliance upon advertisements, promotional content, third-party marketing materials, analytics outputs, Artificial Intelligence recommendations, measurement technologies, or interactions between Users and advertisers or other third parties.

Nothing contained herein shall exclude or limit liability where such exclusion or limitation is prohibited by Applicable Law.

15.12 General Provisions

Nothing contained in this Chapter shall:

- require the Company to disclose confidential advertising strategies, proprietary algorithms, audience segmentation methodologies, analytics models, Artificial Intelligence systems, trade secrets, marketing strategies, pricing methodologies, or commercially sensitive information;
- create any obligation upon the Company to display or continue displaying any advertisement, promotional campaign, affiliate programme, sponsored content, or marketing initiative;
- prevent the Company from introducing, modifying, suspending, restricting, replacing, or discontinuing advertising technologies, analytics platforms, Artificial Intelligence tools, or marketing practices in response to technological developments, legal requirements, regulatory directions, operational needs, cybersecurity considerations, or legitimate business interests; or
- prejudice the Company's rights relating to fraud prevention, cybersecurity, preservation of Electronic Records, Digital Evidence, legal compliance, or enforcement of contractual rights.

DIGITAL EVIDENCE & LEGAL COMPLIANCE

16. DIGITAL EVIDENCE & LEGAL COMPLIANCE

The Company maintains various categories of Electronic Records and Digital Evidence generated through the operation of the Platform. Such records may include Personal Data, authentication records, account activity, communication logs, audit trails, payment records, security logs, metadata, IP addresses, device identifiers, verification records, AI-generated system logs, access histories, transactional records, and other electronically stored information required for operational, legal, regulatory, cybersecurity, evidentiary, or business purposes.

The Company may create, collect, Process, preserve, analyse, archive, reproduce, certify, disclose, or otherwise use such Electronic Records whenever reasonably necessary to operate the Platform, protect Users, enforce contractual rights, investigate misconduct, prevent fraud,

comply with Applicable Law, or defend the Company's legitimate interests.

16.1 Recognition of Electronic Records

The User acknowledges and agrees that Electronic Records maintained by the Company constitute legally recognised records capable of being relied upon, produced, authenticated, and admitted in judicial, arbitral, regulatory, administrative, investigative, or quasi-judicial proceedings in accordance with Applicable Law.

The mere existence of Electronic Records shall not, by itself, create any presumption against the Company regarding liability, negligence, contractual obligations, or factual admissions.

16.2 Categories of Digital Evidence

The Company may preserve and maintain Digital Evidence including, but not limited to, account registration records, login histories, authentication logs, IP addresses, device identifiers, browser information, metadata, timestamps, payment records, invoices, subscription histories, communication records, customer support interactions, chat records, AI-generated moderation records, verification records, audit logs, server logs, security alerts, fraud detection reports, system events, Cookies, tracking identifiers, location information where lawfully collected, API requests, backup records, encrypted archives, and any other Electronic Records generated through the operation of the Platform.

Such Digital Evidence may be retained in original, encrypted, archived, replicated, or backup formats as determined by the Company.

16.3 Preservation of Digital Evidence

The Company reserves the right to preserve Electronic Records and Digital Evidence whenever reasonably necessary for legal proceedings, arbitration, mediation, regulatory investigations, law enforcement requests, cybersecurity incidents, fraud investigations, internal disciplinary proceedings, insurance claims, contractual enforcement, intellectual property protection, audit requirements, or any other lawful purpose.

The preservation of Digital Evidence may continue notwithstanding account deletion requests, withdrawal of Consent, closure of Accounts, expiry of subscriptions, or termination of Services where continued retention is required or permitted under Applicable Law.

16.4 Audit Logs and System Records

The Company may generate and maintain audit trails, access logs, authentication logs, administrative logs, infrastructure logs, database records, API logs, system activity records,

security monitoring records, AI operational logs, transaction histories, and other system-generated information for maintaining operational integrity, ensuring cybersecurity, investigating incidents, resolving disputes, detecting fraud, monitoring compliance, and improving Platform security.

Such records may be automatically generated without individual notice to the User and may be retained for periods determined by the Company's internal governance framework or Applicable Law.

16.5 Legal Disclosure and Cooperation

The Company may disclose Electronic Records or Digital Evidence to courts, tribunals, arbitral tribunals, governmental authorities, law enforcement agencies, regulators, statutory bodies, auditors, investigators, legal advisors, insurance providers, cybersecurity agencies, or any other competent authority where such disclosure is required or permitted under Applicable Law, judicial order, regulatory direction, lawful request, or where necessary to establish, exercise, or defend the Company's legal rights.

The Company may also voluntarily cooperate with competent authorities in matters involving cybersecurity incidents, financial fraud, identity theft, money laundering, organised crime, child protection, national security, public safety, or other matters recognised under Applicable Law.

16.6 Internal Investigations

The Company reserves the right to investigate any suspected violation of the Terms of Use, Privacy Policy, Applicable Law, cybersecurity incident, fraudulent activity, abuse of the Platform, intellectual property infringement, impersonation, unauthorised access, or other misconduct affecting the Platform or its Users.

For such purposes, the Company may review, analyse, preserve, correlate, and rely upon relevant Electronic Records, Digital Evidence, metadata, audit logs, communications, payment information, device information, AI-generated reports, and other lawfully available information.

Nothing contained herein shall require the Company to disclose confidential investigative methodologies, forensic techniques, threat intelligence, or internal security procedures.

16.7 Regulatory Compliance

The Company shall endeavour to comply with all statutory obligations relating to record maintenance, regulatory reporting, data preservation, cybersecurity incident reporting, taxation, anti-money laundering requirements where applicable, consumer protection obligations, judicial directions, and other legal responsibilities imposed under Applicable Law.

The Company reserves the right to modify its compliance framework, governance practices, record retention procedures, internal controls, and documentation standards in response to legislative amendments, judicial decisions, regulatory guidance, technological developments, or recognised industry standards.

16.8 User Cooperation

Users shall cooperate with the Company during any lawful investigation relating to fraud, cybersecurity incidents, misuse of the Platform, contractual disputes, regulatory proceedings, judicial proceedings, or other lawful inquiries.

Where reasonably required, Users may be requested to provide additional information, identity verification, supporting documents, transaction details, communication records, or other relevant evidence necessary for resolving disputes or complying with Applicable Law.

Failure to cooperate may result in suspension, restriction, or termination of the User's Account, subject to Applicable Law.

16.9 Evidentiary Value of Electronic Communications

The User acknowledges that communications exchanged through the Platform, including emails, electronic notices, system notifications, in-application messages, digital acknowledgements, electronic consents, OTP verifications, digital signatures where applicable, electronic confirmations, and other electronic communications may constitute legally valid evidence and may be relied upon by the Company in legal, regulatory, contractual, or dispute resolution proceedings.

Electronic communications shall not be denied legal effect solely because they exist in electronic form.

16.10 Preservation During Disputes

Where any litigation, arbitration, mediation, regulatory inquiry, governmental investigation, internal investigation, or legal dispute is pending or reasonably anticipated, the Company may implement a litigation hold or legal preservation process to prevent alteration, deletion, destruction, or disposal of relevant Electronic Records and Digital

Evidence until such proceedings have concluded or the Company determines that preservation is no longer legally required.

Such preservation obligations shall prevail over ordinary retention or deletion schedules.

16.11 Limitation of Liability

The Company shall not be liable for any inability to produce Electronic Records where such

records have been lawfully deleted, anonymised, overwritten, corrupted, destroyed by force majeure events, affected by third-party infrastructure failures, lost due to technological limitations, or otherwise become unavailable despite the implementation of commercially reasonable record management and cybersecurity practices.

Nothing contained in this Chapter shall create any obligation upon the Company to preserve every Electronic Record indefinitely or beyond the period required under

Applicable Law or the Company's lawful retention policies.

16.12 General Provisions

Nothing contained in this Chapter shall:

- require the Company to disclose confidential forensic methodologies, cybersecurity architecture, encryption mechanisms, internal investigation procedures, legal strategies, proprietary algorithms, trade secrets, or privileged communications;
- prejudice the Company's rights to preserve, authenticate, certify, analyse, disclose, or rely upon Electronic Records and Digital Evidence in accordance with Applicable Law;
- restrict the Company's right to cooperate with governmental authorities, regulators, law enforcement agencies, courts, tribunals, arbitrators, or other competent authorities;
- limit the Company's rights relating to fraud prevention, cybersecurity, contractual enforcement, intellectual property protection, business continuity, or legal compliance; or
- affect any statutory privilege, immunity, exemption, defence, or legal protection available to the Company under Applicable Law.

The Company reserves the right to amend, supplement, strengthen, or replace its Digital Evidence and legal compliance practices at any time to reflect changes in legislation, judicial precedents, regulatory directions, technological advancements, cybersecurity risks, operational requirements, or recognised industry standards.

DATA BREACH MANAGEMENT

17. DATA BREACH MANAGEMENT

The Company maintains a comprehensive Data Breach Management Framework designed to identify, assess, contain, investigate, mitigate, document, recover from, and respond to actual, suspected, or reasonably anticipated Personal Data Breaches and cybersecurity incidents affecting the Platform, its Users, business operations, or information assets.

The Company's incident response procedures are intended to minimise harm, preserve Digital Evidence, maintain business continuity, protect affected Users, comply with

Applicable Law, and strengthen the Company's overall cybersecurity posture. Nothing contained in this Chapter shall be construed as guaranteeing that every cybersecurity incident can be prevented, detected, or eliminated.

17.1 Definition of a Personal Data Breach

For the purposes of this Privacy Policy, a Personal Data Breach includes any accidental, unlawful, unauthorised, malicious, or unintended access, acquisition, disclosure, exposure, alteration, destruction, corruption, encryption, deletion, loss, misuse, theft, exfiltration, unavailability, compromise, or other Processing of Personal Data or

Electronic Records that affects, or is reasonably likely to affect, the confidentiality, integrity, availability, authenticity, or security of such information.

A cybersecurity incident shall not automatically constitute a Personal Data Breach merely because it affects the Company's infrastructure. The Company shall determine, acting reasonably and in accordance with Applicable Law, whether a particular incident constitutes a reportable Personal Data Breach.

17.2 Detection and Identification

The Company may employ administrative, organisational, contractual, physical, and technical safeguards to identify actual or suspected Personal Data Breaches at the earliest reasonably practicable opportunity.

Such safeguards may include security monitoring systems, Artificial Intelligence-assisted threat detection, intrusion detection systems, endpoint protection technologies, security information and event management platforms, audit logs, anomaly detection systems, vulnerability monitoring, penetration testing, fraud detection mechanisms, employee reporting procedures, third-party notifications, customer reports, and other security technologies or operational controls considered appropriate by the Company.

17.3 Assessment and Classification

Upon becoming aware of an actual or suspected Personal Data Breach, the Company may conduct an internal assessment to determine the nature, scope, origin, severity, duration, potential impact, categories of information affected, number of affected Users, legal implications, cybersecurity risks, operational consequences, and other relevant circumstances.

The Company may classify incidents according to their severity, urgency, business impact, regulatory significance, and risk to affected individuals, and shall determine the appropriate response measures based upon such assessment.

17.4 Containment and Mitigation

Following the identification of a Personal Data Breach, the Company may take such immediate and reasonable measures as it considers necessary to contain, isolate, restrict, suspend, remediate, or otherwise mitigate the incident.

Such measures may include disabling affected systems, restricting account access, resetting authentication credentials, isolating compromised infrastructure, blocking malicious network traffic, restoring secure backups, applying emergency security patches, enhancing monitoring activities, preserving Digital Evidence, notifying service providers, activating disaster recovery procedures, or implementing any other technical or organisational measures reasonably necessary to minimise further harm.

The specific containment measures adopted shall remain within the Company's reasonable discretion having regard to the circumstances of each incident.

17.5 Investigation

The Company reserves the right to investigate every actual or suspected Personal Data Breach using internal personnel, external cybersecurity consultants, digital forensic specialists, legal advisors, auditors, Artificial Intelligence-assisted forensic tools, managed security service providers, or other qualified professionals.

During the course of such investigation, the Company may examine Electronic Records, audit logs, metadata, authentication records, communication records, transaction histories, system logs, Digital Evidence, cloud infrastructure, backup systems, endpoint devices, user activity, third-party systems, and any other information reasonably relevant to determining the cause, extent, impact, and consequences of the incident.

Nothing contained herein shall require the Company to disclose confidential forensic methodologies, investigation strategies, threat intelligence, security architecture, or privileged legal communications.

17.6 Notification of Personal Data Breaches

Where Applicable Law requires notification of a Personal Data Breach, the Company shall endeavour to notify the competent regulatory authority, affected Users, governmental authorities, CERT-In, law enforcement agencies, or any other competent authority within the timelines prescribed by Applicable Law.

The timing, manner, content, and recipients of any notification shall be determined by the Company having regard to the applicable legal requirements, the nature of the incident, operational considerations, ongoing investigations, and cybersecurity risks.

The Company reserves the right to delay, limit, or withhold notifications where permitted under

Applicable Law or where immediate notification could reasonably prejudice an investigation, compromise cybersecurity operations, facilitate criminal activity, or otherwise cause additional harm.

17.7 User Responsibilities During a Data Breach

Users shall promptly notify the Company if they become aware of any unauthorised access to their Account, credential compromise, phishing attempt, suspicious activity, fraudulent transaction, identity theft, malware infection, or any other incident that may affect the security of their Personal Data or the Platform.

Users shall cooperate with the Company during any investigation by providing accurate information, completing identity verification procedures, changing passwords where requested, enabling additional security controls, and complying with reasonable security instructions issued by the Company.

Failure to cooperate may delay remediation efforts and may affect the Company's ability to investigate or resolve the incident.

17.8 Preservation of Digital Evidence

The Company may preserve all relevant Electronic Records, audit logs, metadata, communication records, forensic images, authentication logs, transaction histories, system logs, server records, AI-generated security reports, and other Digital Evidence relating to a Personal Data Breach.

Such Digital Evidence may be retained, analysed, certified, disclosed, or produced before courts, tribunals, arbitral authorities, regulators, governmental agencies, insurers, auditors, cybersecurity experts, or law enforcement authorities in accordance with Applicable Law.

The preservation of Digital Evidence shall take precedence over ordinary deletion schedules where reasonably necessary to protect legal rights or comply with legal obligations.

17.9 Recovery and Business Continuity

Following containment of a Personal Data Breach, the Company may initiate recovery procedures designed to restore Platform functionality, recover affected information systems, verify data integrity, strengthen cybersecurity controls, monitor for recurring threats, and resume normal business operations.

Recovery activities may include restoration from secure backups, system validation, infrastructure replacement, software updates, enhanced monitoring, user communication, security testing, penetration testing, vulnerability remediation, employee training, vendor

reviews, and improvements to the Company's information security programme.

The Company does not guarantee uninterrupted availability of the Platform during breach response or recovery activities.

17.10 Post-Incident Review

After resolution of a Personal Data Breach, the Company may conduct an internal review to evaluate the effectiveness of its response, identify root causes, assess lessons learned, strengthen security controls, improve policies and procedures, update incident response plans, review vendor performance, and implement corrective or preventive measures.

The Company may revise its security practices, governance framework, contractual arrangements, employee training programmes, Artificial Intelligence systems, technical controls, or operational procedures whenever reasonably necessary to reduce the likelihood of similar incidents occurring in the future.

17.11 Limitation of Liability

The Company shall implement commercially reasonable administrative, technical, organisational, and contractual safeguards to protect Personal Data. However, the User acknowledges that no information system, network, software application, cloud infrastructure, electronic communication, or internet-based service can be guaranteed to be completely secure or immune from cyber threats.

To the fullest extent permitted under Applicable Law, the Company shall not be liable for any loss, damage, interruption, unauthorised access, disclosure, corruption, alteration, deletion, ransomware attack, phishing attack, malware infection, denial-of-service attack, advanced persistent threat, zero-day exploit, infrastructure failure, telecommunications failure, force majeure event, criminal activity, or other cybersecurity incident arising from circumstances beyond the Company's reasonable control, provided that the Company has implemented reasonable security measures consistent with

Applicable Law.

Nothing contained herein shall exclude or limit liability where such exclusion or limitation is prohibited by Applicable Law.

17.12 General Provisions

Nothing contained in this Chapter shall:

- require the Company to disclose confidential cybersecurity architecture, forensic methodologies, vulnerability assessments, incident response playbooks, security configurations, encryption mechanisms, threat intelligence, penetration testing reports, proprietary algorithms,

trade secrets, or privileged legal advice;

- prejudice the Company's rights to preserve Electronic Records, Digital Evidence, audit logs, or security records for legal, regulatory, evidentiary, cybersecurity, insurance, or dispute resolution purposes;

- restrict the Company's right to cooperate with governmental authorities, CERT-

In, law enforcement agencies, regulators, courts, tribunals, arbitral authorities, insurers, cybersecurity experts, or other competent authorities;

- create any guarantee that the Platform will be immune from cybersecurity incidents or Personal Data Breaches; or

- limit any statutory defence, immunity, exemption, contractual right, or legal protection available to the Company under Applicable Law.

The Company reserves the right to amend, strengthen, supplement, or replace its Data Breach Management Framework at any time to reflect changes in legislation, regulatory guidance, judicial decisions, cybersecurity risks, technological developments, recognised industry standards, operational requirements, or legitimate business interests.

GRIEVANCE OFFICER & CONTACT DETAILS

18. GRIEVANCE OFFICER & CONTACT DETAILS

Renu Sharma : Grievance Officer Mobile No. 7428110309

The Company is committed to maintaining an effective, transparent, fair, and accessible grievance redressal mechanism for addressing complaints, concerns, requests, and queries relating to the Platform, the Services, Personal Data, privacy, cybersecurity, subscriptions, payments, intellectual property, contractual matters, and other issues arising under the Terms of Use, this Privacy Policy, or Applicable Law.

The Company shall designate a Grievance Officer or such other authorised representative as may be required under Applicable Law. The Grievance Officer shall act as the primary point of contact for receiving, coordinating, reviewing, and facilitating the resolution of grievances submitted by Users, Data Principals, regulatory authorities, or other authorised persons.

18.1 Appointment of Grievance Officer

The Company shall appoint a Grievance Officer in accordance with Applicable Law and may appoint one or more deputy grievance officers, compliance officers, privacy officers, data protection personnel, customer support representatives, or authorised officers to assist in the discharge of grievance-related functions.

The Company reserves the right to change the identity, designation, responsibilities, contact

details, reporting structure, or jurisdiction of the Grievance Officer at any time without prior notice, provided that updated contact information is made available through the Platform or other appropriate communication channels.

18.2 Scope of Grievances

Users may submit grievances relating to matters including, but not limited to, the collection, Processing, disclosure, retention, correction, deletion, security, or transfer of Personal Data; account access; identity verification; subscription services; billing disputes; payment issues; refunds; AI-generated recommendations; profile verification; cybersecurity concerns; intellectual property infringement; misuse of the Platform; impersonation; fraudulent activities; policy violations; advertisements; third-party integrations; accessibility issues; service quality; contractual disputes; or any other matter arising from the Company's Services.

Submission of a grievance shall not prevent the Company from exercising its contractual or statutory rights, nor shall it operate as an admission of liability

18.3 Submission of Grievances

Grievances may be submitted through the communication channels notified by the Company from time to time, including electronic mail, online grievance forms, customer support portals, in-application support systems, postal correspondence, or any other communication mechanism designated by the Company.

A grievance should, to the extent reasonably practicable, contain sufficient particulars to enable proper investigation, including the complainant's name, registered contact details, account information, description of the grievance, supporting documents, transaction references, screenshots, correspondence, dates of relevant events, and any other information reasonably necessary for evaluating the complaint.

The Company may decline to process anonymous, incomplete, illegible, repetitive, abusive, malicious, fraudulent, or manifestly unfounded grievances where permitted under Applicable Law.

18.4 Verification of Identity

Before acting upon any grievance involving Personal Data, account access, financial transactions, or confidential information, the Company may require reasonable identity verification, authentication, documentary evidence, or additional information to confirm the identity and authority of the complainant.

The Company may refuse to disclose confidential information or implement requested actions

until such verification has been satisfactorily completed.

Such verification measures are intended to protect Users against fraud, identity theft, unauthorised disclosures, and other security risks.

18.5 Investigation and Resolution

Upon receipt of a grievance, the Company may acknowledge its receipt, conduct such enquiries or investigations as it considers appropriate, obtain additional information from the complainant or third parties, examine relevant Electronic Records, Digital

Evidence, audit logs, communication records, payment records, AI-generated logs, or other relevant information, and determine an appropriate course of action.

The Company shall endeavour to resolve grievances within the timelines prescribed under Applicable Law or, where no statutory timeline exists, within a commercially reasonable period having regard to the complexity, nature, and circumstances of the grievance.

The Company may close a grievance where it is satisfactorily resolved, withdrawn, abandoned, duplicated, rendered infructuous, or otherwise disposed of in accordance with Applicable Law.

18.6 Escalation Mechanism

Where a complainant is dissatisfied with the outcome of a grievance or where the grievance cannot reasonably be resolved at the initial level, the Company may provide an internal escalation mechanism to an authorised senior officer, compliance function, legal department, management representative, or such other authority as may be designated by the Company.

Nothing contained herein shall prejudice the complainant's statutory right to approach any competent regulatory authority, court, tribunal, or other forum having jurisdiction under Applicable Law.

18.7 Regulatory Cooperation

The Company reserves the right to cooperate with governmental authorities, regulatory bodies, courts, tribunals, arbitrators, law enforcement agencies, data protection authorities, consumer authorities, CERT-In, auditors, or other competent authorities in relation to grievances, complaints, investigations, inspections, legal proceedings, or regulatory inquiries.

The Company may disclose relevant Personal Data, Electronic Records, Digital Evidence, audit logs, communication records, or other information where required or permitted under Applicable Law.

18.8 No Guarantee of Specific Outcome

While the Company shall make commercially reasonable efforts to investigate and address grievances fairly, efficiently, and in good faith, the Company does not warrant or guarantee that

every grievance shall be resolved in the manner desired by the complainant.

The Company reserves the right to reject, partially allow, defer, or otherwise dispose of any grievance where the requested relief is contrary to Applicable Law, contractual obligations, technical feasibility, cybersecurity requirements, third-party rights, judicial orders, regulatory directions, or the Company's legitimate business interests.

18.9 Communication

The Company may communicate with the complainant through electronic mail, telephone, SMS, in-application notifications, registered account communications, courier, postal correspondence, or any other communication channel reasonably considered appropriate.

Communications transmitted to the registered email address, mobile number, or other contact details provided by the User shall be deemed to have been duly delivered in accordance with the Terms of Use unless proven otherwise.

18.10 Contact Details

Users may contact the Company's designated Grievance Officer using the contact details published on the Platform or communicated by the Company from time to time.

Grievance Officer

Name: Renu Sharma_____

Designation: Grievance Officer

Company: Ramisht Kripa Private Limited

Registered Office: _ Flat No. 9188, 1st Floor, LIG Flat,B-9 Vasant Kunj New Delhi- 110070

Email: _support@sarkarihumsafar.com_____

Telephone: _7428110309_____

Working Days: Monday to Friday (excluding public holidays)

Business Hours: _9AM to 5 PM_____

The Company reserves the right to update or replace the above contact details at any time. Updated contact information shall become effective immediately upon publication on the Platform unless otherwise required by Applicable Law.

18.11 Limitation of Liability

The Company shall not be liable for any delay in responding to or resolving a grievance arising from circumstances beyond its reasonable control, including force majeure events, failures of communication networks, cyberattacks, technical outages, incomplete information supplied by the complainant, delays attributable to third parties, judicial or governmental restrictions, or any

other event preventing timely resolution.

Nothing contained in this Chapter shall require the Company to disclose privileged legal advice, confidential commercial information, proprietary algorithms, cybersecurity measures, internal investigation reports, trade secrets, or other information protected under Applicable Law.

18.12 General Provisions

Nothing contained in this Chapter shall:

- limit the Company's statutory rights, contractual rights, or legal remedies under Applicable Law;
- prejudice the Company's right to preserve Electronic Records, Digital Evidence, audit logs, or security records;
- restrict the Company's right to investigate fraud, cybersecurity incidents, contractual breaches, or unlawful activities;
- create any contractual obligation beyond those expressly imposed under Applicable Law or this Privacy Policy; or
- affect the applicability of the dispute resolution, governing law, limitation of liability, indemnity, or jurisdiction provisions contained in the Terms of Use.

The Company reserves the right to amend, supplement, or replace its grievance redressal procedures, contact details, escalation mechanisms, or operational framework at any time to reflect changes in legislation, regulatory guidance, judicial decisions, organisational restructuring, technological developments, or legitimate business requirements.

AMENDMENTS TO THE PRIVACY POLICY

19. AMENDMENTS TO THE PRIVACY POLICY

The Company reserves the absolute and continuing right, at its sole discretion, to amend, modify, revise, replace, update, supplement, consolidate, or discontinue this Privacy Policy, in whole or in part, at any time and without prior notice, except where prior notice is expressly required under Applicable Law.

Such amendments may be made to ensure continued compliance with legislative developments, regulatory directions, judicial decisions, technological advancements, cybersecurity requirements, operational improvements, business restructuring, changes in the Services, Artificial Intelligence systems, data processing activities, international best practices, or any other lawful business or compliance requirement.

Nothing contained herein shall be construed as creating any obligation upon the Company to maintain any particular version of this Privacy Policy indefinitely.

19.1 Right to Amend

The Company may amend this Privacy Policy whenever it considers such amendment necessary or appropriate, including but not limited to circumstances involving:

- changes in Applicable Law, governmental policies, judicial precedents, or regulatory guidance;
- modifications to the Platform, Services, subscriptions, Artificial Intelligence systems, analytics technologies, or business operations;
- implementation of new cybersecurity measures, fraud prevention mechanisms, or technical safeguards;
- introduction of new products, features, technologies, payment methods, verification procedures, or third-party integrations;
- mergers, acquisitions, restructuring, business transfers, or corporate reorganisations;
- changes in industry standards, recognised security frameworks, or privacy best practices; or
- any other circumstance requiring revision to protect the legitimate interests of the Company, its Users, or third parties.

19.2 Publication of Updated Policy

Any amendment to this Privacy Policy may be published on the Platform, mobile application, official website, customer portal, or through any other communication channel determined appropriate by the Company.

The Company may also notify Users by email, SMS, in-application notification, push notification, dashboard notice, account message, or any other electronic communication where considered appropriate or where required under Applicable Law.

The absence of an individual notification shall not invalidate any amendment where publication on the Platform is legally sufficient.

19.3 Effective Date of Amendments

Unless otherwise expressly stated, every amendment to this Privacy Policy shall become effective immediately upon its publication on the Platform or on such later date as may be specified by the Company.

Where Applicable Law requires prior notice or renewed Consent before implementing particular amendments, the Company shall comply with such legal requirements before the relevant amendment becomes effective.

19.4 Continued Use Constitutes Acceptance

The User acknowledges and agrees that continued access to, registration on, or use of the Platform or Services after the effective date of any amendment shall constitute the User's

acceptance of the revised Privacy Policy.

If a User does not agree with any amendment, the User must immediately discontinue use of the Platform and may request closure of the Account in accordance with the Company's applicable policies, subject to the Company's legal rights to retain information under Applicable Law.

19.5 Material Changes

Where the Company determines, or where Applicable Law requires, that an amendment materially affects Users' privacy rights, data processing activities, or legal obligations, the Company may provide additional notice through one or more communication channels before such amendment becomes effective.

The method, timing, and content of such notice shall be determined by the Company in accordance with Applicable Law and operational feasibility.

Nothing contained herein shall require the Company to provide individual notice for editorial, administrative, formatting, grammatical, technical, or other non-material changes.

19.6 User Responsibility

Users are responsible for periodically reviewing the latest version of this Privacy Policy available on the Platform.

Failure by a User to review any amendment shall not affect the enforceability or validity of the amended Privacy Policy.

The Company shall not be liable for any loss arising solely from a User's failure to review updated versions of this Privacy Policy.

19.7 No Waiver

The Company's failure to exercise, enforce, or immediately implement any amendment, right, provision, or remedy under this Privacy Policy shall not constitute a waiver of such right or prevent its subsequent enforcement.

No amendment, waiver, representation, or modification shall be binding upon the Company unless made in accordance with this Chapter or otherwise required under Applicable Law.

19.8 Preservation of Existing Rights

Any amendment to this Privacy Policy shall not adversely affect:

- the Company's accrued legal rights;
- obligations already incurred by Users;
- rights relating to previously collected Personal Data where Processing remains lawful;

- preservation of Electronic Records and Digital Evidence;
- cybersecurity investigations;
- ongoing legal proceedings, regulatory investigations, or dispute resolution processes; or
- any statutory rights, remedies, immunities, exemptions, or defences available to the Company under Applicable Law.

The Company may continue to Process and retain Personal Data collected before any amendment where such Processing remains lawful under Applicable Law.

19.9 Version Control

The Company may maintain historical versions, archived copies, internal revisions, audit records, and version histories of this Privacy Policy for legal compliance, audit purposes, Digital Evidence preservation, regulatory inspections, dispute resolution, internal governance, cybersecurity, or business continuity.

The Company reserves the right to determine which version of the Privacy Policy applies to a particular event, transaction, dispute, or Processing activity, having regard to the relevant effective date and Applicable Law.

19.10 Limitation of Liability

To the fullest extent permitted under Applicable Law, the Company shall not be liable for any direct, indirect, incidental, consequential, special, exemplary, or punitive loss arising solely from amendments made to this Privacy Policy in accordance with Applicable Law or this Chapter.

Nothing contained herein shall exclude or limit liability where such exclusion or limitation is prohibited under Applicable Law.

19.11 General Provisions

Nothing contained in this Chapter shall:

- restrict the Company's right to revise its privacy, cybersecurity, Artificial Intelligence, compliance, governance, or operational practices;
- require the Company to obtain Consent for amendments where such Consent is not required under Applicable Law;
- affect the validity of any Processing lawfully undertaken before the effective date of an amendment;
- prejudice the Company's rights relating to fraud prevention, cybersecurity, preservation of Electronic Records, Digital Evidence, legal compliance, contractual enforcement, or business continuity; or
- limit any statutory right, defence, immunity, exemption, or contractual protection available to

the Company.

The Company reserves the right to issue supplemental privacy notices, product-specific privacy disclosures, regional privacy notices, regulatory notices, or operational guidelines, which shall form an integral part of this Privacy Policy to the extent applicable.

GOVERNING LAW, DISPUTE RESOLUTION & JURISDICTION

20. GOVERNING LAW, DISPUTE RESOLUTION & JURISDICTION

The Company is committed to resolving disputes fairly, efficiently, confidentially, and in accordance with Applicable Law. This Chapter governs all disputes, controversies, claims, proceedings, complaints, investigations, and causes of action arising out of or relating to this Privacy Policy, the Platform, the Services, the collection or Processing of Personal Data, Electronic Records, Digital Evidence, contractual obligations, statutory rights, or any relationship between the Company and a User.

The Parties acknowledge that alternative dispute resolution mechanisms are intended to reduce unnecessary litigation, facilitate efficient resolution of disputes, preserve business relationships, and minimise legal costs.

20.1 Governing Law

This Privacy Policy, together with all rights, obligations, liabilities, disputes, claims, controversies, and matters arising directly or indirectly out of or in connection with the Platform, the Services, or the Processing of Personal Data, shall be governed by and construed exclusively in accordance with the laws of the Republic of India, without regard to any conflict of laws principles.

All statutory rights, obligations, and remedies available under Applicable Law shall continue to apply to the extent they cannot lawfully be excluded by contract.

20.2 Good Faith Resolution

Before initiating arbitration or judicial proceedings, the User shall make reasonable efforts to resolve the dispute by submitting a written grievance to the Company's designated Grievance Officer in accordance with the grievance redressal mechanism provided under this Privacy Policy.

The Parties shall endeavour to resolve the dispute amicably through discussions, negotiations, exchange of information, or other mutually acceptable methods within thirty (30) days, or such other period as may be mutually agreed in writing.

Nothing contained herein shall prevent either Party from seeking urgent interim, conservatory, or statutory relief where immediate action is reasonably necessary.

20.3 Mandatory Arbitration

If any dispute is not resolved through amicable discussions within the period specified above, such dispute shall, to the fullest extent permitted under Applicable Law, be referred to and finally resolved by arbitration in accordance with the provisions of the Arbitration and Conciliation Act, 1996, including all statutory amendments, modifications, or re-enactments thereof.

The arbitration shall be the exclusive dispute resolution mechanism for all contractual disputes arising from or relating to this Privacy Policy, except where Applicable Law expressly provides otherwise or confers exclusive jurisdiction upon a statutory authority or court.

20.4 Appointment of Arbitrator

Unless otherwise mutually agreed, the arbitration shall be conducted by a sole arbitrator mutually appointed by the Parties.

If the Parties fail to agree upon the appointment of the arbitrator within thirty (30) days, the arbitrator shall be appointed in accordance with the provisions of the Arbitration and Conciliation Act, 1996 by the competent court having jurisdiction.

The arbitrator shall possess appropriate legal qualifications, independence, impartiality, and expertise relevant to commercial, technology, privacy, or information technology disputes.

20.5 Seat, Venue and Language of Arbitration

The seat and legal place of arbitration shall be New Delhi, India, unless the Company expressly agrees otherwise in writing.

The hearings may be conducted physically, virtually, or through hybrid electronic means as determined by the arbitral tribunal.

The arbitration proceedings shall be conducted in the English language, unless otherwise agreed by the Parties.

20.6 Confidentiality of Proceedings

All negotiations, mediation discussions, arbitration proceedings, pleadings, witness statements, documentary evidence, Electronic Records, Digital Evidence, arbitral awards, and settlement discussions shall remain strictly confidential except where disclosure is required:

- under Applicable Law;
- pursuant to a judicial or governmental order;
- for enforcement or challenge of an arbitral award;
- for insurance purposes;
- for obtaining legal, accounting, or professional advice; or

- for protecting the Company's legal rights.

The Parties shall take reasonable measures to preserve confidentiality throughout the dispute resolution process.

20.7 Electronic Records and Digital Evidence

The User expressly acknowledges and agrees that Electronic Records, Digital Evidence, metadata, audit logs, IP addresses, authentication records, communication records, AI-generated system logs, payment records, server logs, timestamps, account activity, electronic acknowledgements, digital consents, electronically generated reports, and other electronically stored information maintained by the Company may be relied upon as evidence in any judicial, arbitral, regulatory, or administrative proceeding, subject to

Applicable Law.

The admissibility, evidentiary value, authenticity, and reliability of such Electronic Records shall be determined in accordance with the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, and other Applicable Laws

20.8 Interim and Emergency Relief

Nothing contained in this Chapter shall prevent the Company from approaching any competent court, tribunal, statutory authority, or arbitral tribunal for obtaining interim, emergency, conservatory, injunctive, equitable, protective, or other urgent relief relating to:

- protection of confidential information;
- preservation of Digital Evidence;
- cybersecurity incidents;
- intellectual property rights;
- fraud prevention;
- unauthorised access;
- data security;
- recovery of outstanding dues;
- enforcement of contractual obligations; or
- any matter where immediate relief is reasonably necessary.

The exercise of such rights shall not constitute a waiver of arbitration.

20.9 Exclusive Jurisdiction

Subject to the arbitration provisions contained herein, the courts situated at New Delhi, India, shall have exclusive jurisdiction over:

- applications relating to arbitration;

- interim measures;
- enforcement of arbitral awards;
- challenges to arbitral awards;
- matters requiring judicial intervention under Applicable Law;
- proceedings where arbitration is not legally permissible; and
- any matter over which statutory authorities or courts possess exclusive jurisdiction.

The User irrevocably submits to the exclusive jurisdiction of such courts.

20.10 Limitation Period

Any claim arising out of or relating to this Privacy Policy, the Platform, or the Services shall be initiated within the limitation period prescribed under Applicable Law.

To the extent permitted by Applicable Law, failure to initiate proceedings within the applicable limitation period shall constitute a complete bar to such claim.

20.11 Waiver of Class or Representative Proceedings

To the fullest extent permitted under Applicable Law, all disputes shall be pursued solely in an individual capacity.

The User agrees not to participate in any class action, representative action, collective proceeding, public interest litigation, mass arbitration, consolidated arbitration, or similar proceeding against the Company where such waiver is legally enforceable.

Nothing contained herein shall restrict statutory proceedings that cannot lawfully be waived.

20.12 Costs and Expenses

Unless otherwise directed by the arbitral tribunal, competent court, or required under Applicable Law, each Party shall bear its own legal fees, professional expenses, and costs incurred in connection with the dispute.

The arbitral tribunal shall have the authority to award costs, interest, legal fees, arbitration expenses, and other relief in accordance with Applicable Law.

20.13 Survival

The provisions contained in this Chapter shall survive:

- termination or suspension of the User's Account;
- deletion of Personal Data where lawfully retained;
- expiry of subscriptions;
- termination of Services;
- withdrawal of Consent;
- closure of the Platform; and

- termination of the contractual relationship between the Company and the User, to the extent necessary for resolving disputes, preserving legal rights, enforcing obligations, or complying with Applicable Law.

20.14 Severability

If any provision of this Chapter is held to be invalid, illegal, unenforceable, or contrary to Applicable Law by a competent court or arbitral tribunal, the remaining provisions shall continue in full force and effect to the maximum extent permitted by law.

The invalid provision shall, where possible, be interpreted or modified so as to most closely reflect the original commercial intent of the Parties while remaining legally enforceable.

20.15 Limitation of Liability

Nothing contained in this Chapter shall:

- limit or prejudice any statutory rights that cannot lawfully be excluded;
- restrict the Company's rights to preserve Electronic Records, Digital Evidence, audit logs, or cybersecurity records;
- affect the Company's rights to cooperate with regulators, law enforcement agencies, courts, tribunals, or governmental authorities;
- constitute a waiver of sovereign, statutory, contractual, or equitable remedies available to the Company; or
- require the Company to disclose privileged legal advice, confidential settlement discussions, proprietary algorithms, trade secrets, cybersecurity architecture, or confidential commercial information.

20.16 General Provisions

The Company reserves the right to revise or supplement this dispute resolution framework to reflect amendments in legislation, judicial precedents, regulatory guidance, recognised arbitration practices, technological developments, or legitimate business requirements.

No delay or omission by the Company in exercising any right or remedy under this Chapter shall constitute a waiver of such right.

Certainly. Since your Privacy Policy has now reached an enterprise/legal compliance standard, it should conclude with a Miscellaneous Provisions chapter. This chapter consolidates all residual legal protections that are commonly found in privacy policies of multinational corporations, technology companies, financial institutions, SaaS providers, marketplaces, matrimonial platforms, and regulated digital businesses.

Below is a comprehensive drafting.

MISCELLANEOUS PROVISIONS

21. MISCELLANEOUS PROVISIONS

This Chapter governs all matters relating to the interpretation, validity, enforceability, continuity, administration, and legal effect of this Privacy Policy. These provisions shall supplement every other provision contained herein and shall continue to apply notwithstanding suspension, termination, deletion of an Account, expiry of a subscription, withdrawal of Consent, or discontinuance of the Platform, to the extent permitted under Applicable Law.

21.1 Entire Agreement

This Privacy Policy, together with the Company's Terms of Use, Cookie Policy, Consent Management Framework, AI Governance Policy, Refund Policy, Community Guidelines, and all other policies, notices, disclosures, or agreements published by the Company from time to time, constitutes the complete and entire understanding between the Company and the User concerning the collection, Processing, storage, disclosure, protection, retention, and use of Personal Data.

This Privacy Policy supersedes all previous privacy notices, representations, understandings, negotiations, communications, or agreements relating to the same subject matter unless expressly preserved by the Company in writing.

21.2 Severability

If any provision, clause, paragraph, or part of this Privacy Policy is declared invalid, illegal, unenforceable, or contrary to Applicable Law by a court, tribunal, arbitral tribunal, or competent authority, such provision shall be severed only to the minimum extent necessary.

The remaining provisions shall continue in full force and effect and shall remain valid, binding, and enforceable.

Where reasonably possible, the invalid provision shall be interpreted or modified so as to achieve substantially the same commercial, legal, and regulatory purpose originally intended.

21.3 No Waiver

No delay, omission, failure, or partial exercise by the Company in enforcing any right, remedy, protection, discretion, or provision contained in this Privacy Policy shall constitute a waiver thereof.

Any waiver shall be valid only if made expressly in writing by an authorised representative of the Company and shall apply only to the specific matter expressly identified therein.

No waiver of one breach shall constitute a waiver of any subsequent or continuing breach.

21.4 Survival

The provisions relating to confidentiality, data retention, Digital Evidence, cybersecurity, limitation of liability, indemnification, dispute resolution, governing law, intellectual property, legal compliance, audit rights, fraud prevention, Electronic Records, arbitration, jurisdiction, and any other provision which by its nature is intended to survive shall continue to remain effective notwithstanding:

- suspension or termination of a User Account;
- deletion of Personal Data where legally retained;
- withdrawal of Consent;
- cancellation of subscriptions;
- discontinuation of Services;
- expiry of contractual relationships; or
- cessation of business interactions between the Company and the User.

21.5 Assignment

The Company may assign, transfer, novate, delegate, subcontract, or otherwise dispose of its rights, obligations, assets, business operations, contracts, databases, intellectual property, or this Privacy Policy, in whole or in part, to any Affiliate, successor entity, purchaser, investor, acquirer, transferee, or other lawful person in connection with a merger, amalgamation, demerger, restructuring, acquisition, financing, business transfer, insolvency process, or other corporate transaction, subject to Applicable Law.

The User shall not assign, transfer, delegate, sublicense, or otherwise dispose of any rights or obligations under this Privacy Policy without the Company's prior written consent.

21.6 Force Majeure

The Company shall not be liable for any delay, interruption, failure, degradation of Services, inability to Process Personal Data, or non-performance resulting directly or indirectly from events beyond its reasonable control, including but not limited to:

- natural disasters;
- floods, earthquakes, fires, pandemics, epidemics, or public health emergencies;
- acts of war, terrorism, civil unrest, riots, strikes, labour disputes, or governmental actions;
- cyberattacks, ransomware, distributed denial-of-service attacks, malware, zero-day vulnerabilities, internet failures, telecommunications outages, cloud infrastructure failures, or power disruptions;
- failures of third-party service providers;
- changes in Applicable Law;

- judicial or regulatory restrictions; or
- any other event constituting force majeure under Applicable Law.

During such events, the Company's obligations shall remain suspended to the extent affected.

21.7 Relationship of Parties

Nothing contained in this Privacy Policy shall be construed as creating any partnership, joint venture, agency, fiduciary relationship, employment relationship, franchise, association, representative relationship, or legal partnership between the Company and any User.

The User accesses the Platform solely as an independent contracting party.

21.8 No Third-Party Rights

Except where expressly required under Applicable Law, nothing contained in this Privacy Policy shall confer any right, remedy, benefit, claim, or cause of action upon any person who is not a party to this Privacy Policy.

No third party shall have any right to enforce any provision contained herein merely because such provision may incidentally benefit that third party.

21.9 Notices

The Company may provide notices, disclosures, legal communications, regulatory updates, security alerts, amendments, policy revisions, account notifications, invoices, payment reminders, verification requests, or any other communication through email;

SMS; registered mobile number; in-application notifications; dashboard messages; push notifications; courier; postal correspondence; publication on the Platform; or any other legally recognised electronic communication method.

Any notice transmitted using the contact details provided by the User shall be deemed duly served in accordance with Applicable Law unless the User proves otherwise.

Users are responsible for ensuring that their contact details remain accurate and up to date.

21.10 Electronic Communications

The User expressly consents to receive communications electronically and agrees that all electronic notices, acknowledgements, disclosures, invoices, receipts, policies, amendments, contracts, records, OTP verifications, confirmations, digital signatures

(where applicable), and Electronic Records shall satisfy any legal requirement that such communications be in writing.

Electronic communications shall have the same legal validity and enforceability as physical written communications to the fullest extent permitted by Applicable Law.

21.11 Compliance with Future Laws

If any future legislation, statutory amendment, governmental notification, judicial decision, regulatory guideline, industry standard, code of practice, or technological development requires modification of this Privacy Policy, the Company may implement such modifications without affecting the validity of the remaining provisions.

Users acknowledge that continued legal compliance may require periodic amendments to this Privacy Policy.

21.12 Reservation of Rights

The Company expressly reserves all legal rights, contractual rights, statutory rights, equitable remedies, intellectual property rights, proprietary interests, privileges, immunities, defences, and protections not expressly waived under this Privacy Policy.

Nothing contained herein shall be interpreted as limiting any remedy otherwise available to the Company under Applicable Law.

21.13 Interpretation

The headings, titles, numbering, and formatting used in this Privacy Policy are inserted solely for convenience and shall not affect interpretation.

Words importing the singular shall include the plural and vice versa. References to one gender shall include every gender. References to statutes shall include all amendments, re-enactments, subordinate legislation, and successor enactments.

Where any conflict arises between this Privacy Policy and any mandatory provision of Applicable Law, the mandatory legal provision shall prevail only to the extent of such inconsistency, and the remaining provisions shall continue in full force and effect.

21.14 Language

This Privacy Policy is executed and published in the English language.

Where translations are provided for convenience, the English version shall prevail in the event of any inconsistency, ambiguity, conflict, or dispute, unless otherwise required under Applicable Law.

21.15 Counterparts and Electronic Acceptance

Where this Privacy Policy is executed, acknowledged, or accepted electronically, such electronic acceptance, click-wrap acceptance, browse-wrap acceptance, digital confirmation, OTP verification, electronic signature, or other legally recognised electronic method shall constitute valid, binding, and enforceable acceptance under Applicable Law.

Electronic copies, digitally stored versions, and Electronic Records maintained by the Company shall be admissible and enforceable in accordance with Applicable Law.

21.16 Contact for Legal Notices

Any legal notice, statutory notice, regulatory communication, court process, arbitration notice, or other formal legal correspondence intended for the Company shall be addressed to:

Ramisht Kripa Private Limited

Registered Office: Flat No. 9188, 1st Floor, LIG Flat,B-9 Vasant Kunj New Delhi- 110070

Email: _support@sarkarihumssafar.com

Attention: Legal Department / Compliance Officer

Service of notices through the above contact details shall be subject to Applicable Law and any additional procedures prescribed by the Company from time to time.

21.17 Final Acknowledgement

By accessing, registering with, browsing, subscribing to, or otherwise using the Platform or any of the Company's Services, the User acknowledges that they have carefully read, understood, and agreed to be bound by this Privacy Policy, including all amendments made from time to time.

The User further acknowledges that they have had an adequate opportunity to review this Privacy Policy, obtain independent legal advice if considered necessary, and make an informed decision before using the Platform.

This Privacy Policy shall be binding upon the User, the Company, their respective successors, permitted assigns, legal representatives, administrators, and other persons entitled under Applicable Law.

21.18 General Saving Clause

Nothing contained in this Privacy Policy shall:

- waive or limit any statutory obligation or protection available under Applicable Law;
- prejudice the Company's rights relating to cybersecurity, fraud prevention, Digital Evidence preservation, regulatory compliance, contractual enforcement, business continuity, or protection of intellectual property;
- require the disclosure of privileged legal advice, confidential commercial information, trade secrets, proprietary algorithms, internal security procedures, or protected information;
- create any representation, warranty, fiduciary obligation, or guarantee beyond those expressly

provided by Applicable Law; or

- affect any rights, remedies, immunities, exemptions, or defences available to the Company under any present or future law.

WEBSITE DISCLAIMER

The information, services, content, software, mobile application, Artificial Intelligence (“AI”) features, recommendations, profiles, communications, and all other materials made available on this Platform are provided by Ramisht Kripa Private Limited (“Company”) on an “AS IS”, “AS AVAILABLE”, and “WITH ALL FAULTS” basis. The Company makes no representations, warranties, guarantees, or assurances of any kind, whether express or implied, except to the extent expressly required under Applicable Law.

The Platform is intended solely to facilitate matrimonial introductions and related services. The Company functions only as an intermediary technology platform and does not act as a marriage bureau, marriage broker, marriage counsellor, matchmaker, or guarantor of matrimonial outcomes. Users are solely responsible for exercising their independent judgment, discretion, and due diligence before relying upon or interacting with any profile, information, or content available on the Platform.

The Company does not guarantee or warrant any marriage, engagement, compatibility between Users, successful matchmaking, relationship success, authenticity or accuracy of User profiles, continued availability of any User, response from any User, profile visibility, or uninterrupted or error-free functioning of the Services. All such outcomes are uncertain and entirely dependent on User interactions and external factors beyond the Company’s control.

All profile information available on the Platform is provided directly by Users. The Company does not independently verify each profile or the accuracy of information relating to photographs, qualifications, employment, income, family background, caste, religion, horoscope, health status, or other personal details unless expressly stated. Users are strongly advised to independently verify all such information before making any personal, financial, or matrimonial decisions.

AI-generated recommendations and outputs provided on the Platform are automated suggestions only and may be inaccurate, incomplete, outdated, or inappropriate. Such AI outputs do not constitute legal, matrimonial, financial, medical, psychological, or any other form of professional advice and must not be relied upon as such. All final decisions remain solely with the User.

Nothing contained on the Platform shall be construed as legal, financial, investment, medical, psychological, matrimonial counselling, tax, or any other professional advice.

Users are advised to consult qualified professionals before taking any action based on information available on the Platform.

The Company is not responsible or liable for any third-party websites, external links, payment gateways, advertisers, cloud service providers, social media platforms, verification agencies, APIs, or any other third-party services integrated with or accessible through the Platform. Use of such third-party services is entirely at the User's own risk.

While the Company adopts commercially reasonable security practices, it does not guarantee that the Platform or any server, system, software, or transmission is completely secure. The Company shall not be liable for any cyberattacks, hacking, phishing, malware, ransomware, data breaches, or any other security incidents or failures beyond its reasonable control.

The Company does not guarantee uninterrupted or error-free availability of the Platform and reserves the right to modify, suspend, restrict, or discontinue any feature or service at any time without prior notice for maintenance, security, legal compliance, or operational requirements.

All intellectual property rights in the Platform, including but not limited to software, source code, databases, trademarks, logos, AI models, text, graphics, designs, and content, are owned by or licensed to the Company and are protected under Applicable Law. No rights or licences are granted except as expressly permitted.

Electronic records, system logs, audit trails, metadata, digital signatures, AI logs, OTP records, and other electronic communications maintained by the Company may be relied upon as legally valid and admissible evidence in accordance with Applicable Law.

To the fullest extent permitted by Applicable Law, the Company shall not be liable for any direct, indirect, incidental, consequential, special, or punitive damages, including but not limited to emotional distress, matrimonial disputes, failed relationships or marriages, financial loss, reputational harm, loss of opportunity, data loss, business interruption, or any acts or omissions of Users or third parties.

The Company shall also not be liable for any delay or failure in performance caused by events beyond its reasonable control, including but not limited to natural disasters, pandemics, governmental actions, internet outages, cyber incidents, power failures, labour disputes, civil unrest, war, terrorism, or similar force majeure events.

The Company reserves the right to amend, modify, update, or replace this Disclaimer at any time without prior notice. Continued use of the Platform shall constitute acceptance of such

revised terms.

This Disclaimer shall be governed by the laws of India, and any disputes shall be subject to the dispute resolution mechanism set out in the Company's Terms of Use.

All rights not expressly granted or waived under this Disclaimer are expressly reserved by the Company.

For any legal or compliance-related queries regarding this Disclaimer, Users may contact the Company through the contact details provided in the Terms of Use or as available on the Platform.

COMMUNITY GUIDELINES & SAFETY POLICY

1. Purpose and Applicability

1.1. This Community Guidelines & Safety Policy ("Policy") establishes the standards of conduct, safety expectations and responsible-use requirements applicable to all Users, Members, subscribers, visitors and other persons accessing or using the website, mobile application, software, digital interfaces and related services operated under the name SarkariHumsafar.com ("Platform") by Ramisht Kripa Private Limited ("Company").

1.2. The purpose of this Policy is to maintain a safe, respectful, authentic and trustworthy matrimonial environment and to protect Users, the Company, its personnel, service providers and the Platform from fraud, abuse, harassment, impersonation, exploitation, unlawful conduct, cybersecurity threats and other misuse.

1.3. This Policy shall be read together with the Company's Terms of Use, Privacy Policy, Website Disclaimer, Content Moderation & User Reporting Policy, Child Safety Policy, Anti-Dowry Policy, AI Policy, Grievance Redressal Policy, Intellectual Property Policy and such other policies as may be published or notified by the Company from time to time.

1.4. In the event of any inconsistency between this Policy and the Terms of Use, the Terms of Use shall prevail to the extent of such inconsistency, subject always to Applicable Law.

2. Acceptance and Binding Effect

2.1. By accessing, browsing, registering on, creating a Profile on, communicating through, subscribing to, or otherwise using the Platform, the User acknowledges that the User has read, understood and agreed to comply with this Policy.

2.2. Compliance with this Policy is a condition of continued access to and use of the Platform. A violation of this Policy may constitute a violation of the Terms of Use and may result in appropriate enforcement action by the Company.

2.3. Depending upon the nature, seriousness, frequency and circumstances of a violation, the Company may issue a warning, remove or restrict Content, restrict Profile visibility, suspend or terminate an Account, restrict access to particular Services, block technical identifiers or take any other action available under the Terms of Use and Applicable Law.

3. General Community Standards

3.1. Every User shall use the Platform honestly, responsibly, respectfully and solely for lawful matrimonial purposes and shall conduct all interactions in a manner that does not cause unlawful harm, harassment, intimidation, deception or undue distress to another person.

3.2. Users are expected to exercise reasonable judgment, maintain appropriate personal boundaries, respect the decisions and preferences of other Users and refrain from conduct that is abusive, deceptive, threatening, exploitative or otherwise inconsistent with the purpose of the Platform.

3.3. Users shall not use the Platform to circumvent Applicable Law, contractual restrictions, Platform safeguards, moderation mechanisms or other technical or legal controls implemented by the Company.

4. Authenticity and Truthful Representation

4.1. Every User shall provide information that is accurate and not materially misleading and shall make reasonable efforts to keep Profile information current during the period in which the Profile remains active.

4.2. No User shall create or maintain a Profile containing a false identity, materially false personal information, fabricated qualifications, misleading employment information, false income details, fabricated family information, false marital status or any other representation intended or reasonably likely to deceive another User.

4.3. Users shall not impersonate another person, use another person's identity or credentials, falsely claim affiliation with any government department, public authority, employer, institution or organisation, or otherwise create a misleading impression concerning their identity, status, occupation or background.

4.4. The Company may require additional information or verification where it reasonably considers such verification necessary for safety, fraud prevention, Platform integrity, regulatory compliance or investigation of suspected misuse.

5. Government Employment and Official Representation

5.1. A User claiming to be employed by a Central Government department, State Government, public sector undertaking, statutory authority, armed force, police organisation or

other governmental or public institution shall not make any false, fabricated or misleading representation concerning such employment or affiliation.

5.2. No User shall falsely represent that the User holds any government designation, rank, authority, office or entitlement, or use government insignia, logos, documents or identification material for the purpose of creating a false impression of official status.

5.3. The Platform is privately operated and is not itself a Government of India platform or a governmental matrimonial service. No User shall represent otherwise.

6. Respectful Communication and Behaviour

6.1. Users shall communicate with other Users in a respectful and lawful manner and shall not engage in harassment, bullying, intimidation, stalking, threats, abusive conduct, humiliation, coercion, blackmail, extortion or targeted personal attacks.

6.2. Repeatedly contacting a User after the User has clearly requested that communication cease may constitute harassment and may result in enforcement action.

6.3. A disagreement, rejection of a matrimonial proposal or discontinuation of communication shall not justify threats, retaliation, abusive conduct or publication of another person's private information.

7. Consent and Personal Boundaries

7.1. Users shall respect the physical, emotional, matrimonial, digital and personal boundaries of other Users and shall not attempt to obtain compliance through intimidation, manipulation, coercion or persistent unwanted communication.

7.2. No User shall pressure another User to disclose intimate information, photographs, videos, passwords, OTPs, financial credentials, government identification documents or other confidential information.

7.3. Consent to communicate through the Platform shall not be construed as consent to meet physically, enter into a relationship, marry, share Personal Data, participate in financial transactions or undertake any other activity.

8. Fraud and Financial Safety

8.1. Users shall exercise appropriate caution before sending money, transferring property, making investments, providing loans, purchasing goods or services, making payments or entering into any financial arrangement with another User introduced through the Platform.

8.2. The Platform shall not be used for romance scams, matrimonial fraud, investment fraud, advance-fee fraud, fraudulent fundraising, cryptocurrency scams, loan scams, fake employment schemes, payment diversion, money laundering or obtaining money or property through

deception.

8.3. Users shall not request, obtain, use or misuse another person's banking credentials, passwords, OTPs, UPI PINs, card information, CVV, authentication codes or other confidential financial security information.

8.4. The Company does not undertake or guarantee the financial credibility, solvency, income, assets, investment claims or financial intentions of any User. Every User shall independently verify such information before relying upon it.

9. Anti-Dowry and Unlawful Matrimonial Demands

9.1. The Platform shall not be used to demand, solicit, negotiate, facilitate, promote or communicate any dowry or unlawful matrimonial consideration.

9.2. Users shall not make marriage conditional upon payment or transfer of money, property, assets, vehicles, valuables or any other unlawful consideration.

9.3. Any User who encounters conduct reasonably suspected to involve dowry demands or related unlawful matrimonial financial demands is encouraged to report the matter to the Company through the available reporting mechanism.

9.4. The Company's separate Anti-Dowry Policy shall apply to such conduct in addition to this Policy.

10. Sexual Harassment and Sexual Misconduct

10.1. Users shall not use the Platform to engage in sexual harassment, unwanted sexual advances, sexual solicitation, coercive sexual communication or any other sexually abusive or exploitative conduct.

10.2. Users shall not request, obtain, circulate, publish or threaten to publish intimate photographs, videos or other sexually sensitive material without lawful authority and appropriate consent.

10.3. Any attempt to use intimate material for blackmail, extortion, intimidation or coercion shall be treated as a serious safety violation and may result in immediate enforcement action and reporting to competent authorities where appropriate.

11. Child Safety

11.1. The Platform shall not be used for grooming, sexual exploitation, inappropriate contact with minors, sexual solicitation of minors or any other conduct involving the exploitation or abuse of children.

11.2. Users shall not upload, transmit, request, distribute, store or facilitate any Child Sexual Abuse Material or other unlawful material involving children.

11.3. Where the Company becomes aware of conduct presenting a serious child-safety concern, it may take immediate protective measures, preserve relevant Digital Evidence and cooperate with competent authorities in accordance with Applicable Law.

11.4. The Company's separate Child Safety Policy shall govern detailed child-safety requirements and procedures.

12. Photographs, Videos and Other Media

12.1. Users shall upload, publish or transmit only photographs, videos and other media that they are lawfully entitled to use.

12.2. Users shall not use another person's photograph or media to create a false Profile, impersonate another person, mislead Users or facilitate fraud.

12.3. Users shall not manipulate, morph, alter, sexualise, deepfake or otherwise digitally modify another person's image for the purpose of deception, harassment, exploitation, blackmail or reputational harm.

12.4. The Company may remove or restrict media reasonably suspected to be fraudulent, unlawful, infringing, manipulated or harmful and may preserve relevant records where necessary for investigation or legal compliance.

13. Privacy and Personal Information

13.1. Users shall respect the privacy and confidentiality of information received from other Users.

13.2. No User shall publish, disclose, distribute, sell, misuse or otherwise process another person's Personal Data without lawful authority.

13.3. Users shall not engage in doxxing, unauthorised disclosure of residential addresses, private telephone numbers, government identification documents, financial information, private communications or other confidential information.

13.4. The Company's collection and Processing of Personal Data shall be governed by the Privacy Policy and Applicable Law.

14. Off-Platform Communication and Meetings

14.1. Users may independently choose to communicate or interact outside the Platform; however, any such interaction is undertaken at the User's own discretion and subject to the User's independent assessment of the associated risks.

14.2. Before moving communication outside the Platform or meeting another User, Users are advised to independently verify identity and material representations and to avoid prematurely disclosing sensitive Personal Data or entering into financial arrangements.

14.3. For initial physical meetings, Users are advised to meet in public locations, inform a trusted person, maintain independent transportation arrangements and take such other reasonable precautions as may be appropriate.

14.4. The Company does not arrange, supervise or guarantee the safety, conduct or outcome of meetings or interactions occurring outside its reasonable control.

15. Commercial Solicitation and Unauthorised Use

15.1. Unless expressly authorised by the Company, the Platform shall not be used for advertising, commercial solicitation, recruitment, lead generation, sale of goods or services, fundraising, investment solicitation, political campaigning or other unrelated commercial activity.

15.2. Users shall not use matrimonial communication as a means to promote businesses, schemes, investments, employment opportunities or other commercial interests without lawful authority and express permission of the Company.

16. Spam, Bots and Automated Misuse

16.1. Users shall not send bulk unsolicited messages, operate bots, create fraudulent Accounts, use automated scripts, scrape User information, harvest contact details or otherwise engage in automated activity designed to circumvent Platform restrictions or interfere with normal Platform operations.

16.2. Users shall not manipulate search results, Profile visibility, engagement metrics, recommendations or other Platform functionality through artificial or deceptive means.

17. Cybersecurity and Platform Security

17.1. Users shall not attempt to obtain unauthorised access to the Platform, another User's Account, Company systems, databases, servers, APIs or other infrastructure.

17.2. Users shall not introduce malware, malicious code, viruses or other harmful technology, conduct denial-of-service attacks, circumvent security mechanisms, exploit vulnerabilities without authorisation or otherwise interfere with Platform security.

17.3. Any suspected compromise of an Account or security vulnerability should be reported promptly through the Company's designated security or support channel.

18. User Account Security

18.1. Users are responsible for maintaining the confidentiality and security of their Account credentials and shall take reasonable precautions to prevent unauthorised access.

18.2. Users shall immediately notify the Company upon becoming aware of suspected unauthorised access, compromised credentials, suspicious Account activity or loss or theft of

relevant authentication information.

18.3. The Company may temporarily restrict an Account where it reasonably believes that such action is necessary to protect the Account, User, Platform or other persons from security risks.

19. User Content

19.1. Users remain responsible for the Profile information, photographs, videos, documents, messages, reviews, comments and other Content submitted or transmitted by them through the Platform.

19.2. User Content shall not be unlawful, fraudulent, materially misleading, defamatory, infringing, abusive, malicious, harmful or otherwise inconsistent with this Policy or the Terms of Use.

19.3. The Company may moderate, restrict, remove, disable or preserve User Content in accordance with the Terms of Use, Content Moderation & User Reporting Policy and Applicable Law.

20. Reporting of Safety Concerns

20.1. Users are encouraged to promptly report suspected fraud, impersonation, harassment, threats, stalking, sexual misconduct, child-safety concerns, dowry demands, privacy violations, fake Profiles, financial scams, cybersecurity incidents or other serious violations.

20.2. A report should, where reasonably available, contain sufficient information to enable the Company to identify the relevant Account, Content or incident and may include screenshots, messages, dates, times, Profile information or other supporting material.

20.3. The Company may request additional information where reasonably necessary to assess or investigate a report.

21. False or Malicious Reports

21.1. Users shall not knowingly submit false, fabricated, malicious, retaliatory or materially misleading complaints or reports.

21.2. Submission of a genuine complaint in good faith shall not constitute a violation merely because the Company is unable to substantiate the allegation.

21.3. Where the Company reasonably determines that the reporting mechanism has been deliberately abused, it may take appropriate action against the reporting Account.

22. Safety Investigation and Content Moderation

22.1. The Company may investigate reports and suspected violations through automated systems, AI-assisted tools, human review, verification procedures, User-provided evidence, technical records and other reasonable means.

22.2. The Company may temporarily restrict Content, Profiles, messaging functionality or Accounts while an investigation is pending where reasonably necessary for safety, security, fraud prevention, legal compliance or protection of evidence.

22.3. Detailed procedures concerning moderation, review and reporting shall be governed by the Company's Content Moderation & User Reporting Policy.

23. AI-Assisted Safety Measures

23.1. The Company may use Artificial Intelligence, Machine Learning and automated technologies for fraud detection, Profile analysis, spam detection, Content moderation, cybersecurity, suspicious-activity detection and other safety-related purposes.

23.2. Automated systems may generate false positives or false negatives and shall not be regarded as infallible.

23.3. Where appropriate, automated safety measures may be supplemented by human review in accordance with the Company's AI Policy and Applicable Law.

24. Enforcement Measures

24.1. Where the Company reasonably believes that a User has violated this Policy, the Terms of Use, Applicable Law or Platform safety requirements, it may take one or more appropriate measures.

24.2. Such measures may include warning, Content removal, Content restriction, Profile restriction, reduced visibility, messaging restrictions, withdrawal of verification, temporary suspension, permanent termination, technical blocking, evidence preservation or reporting to competent authorities.

24.3. The nature and extent of enforcement may depend upon the seriousness, frequency, intent, impact, available evidence and circumstances of the conduct.

25. Immediate Protective Measures

25.1. Where conduct presents a serious or immediate risk to personal safety, child safety, financial security, cybersecurity, Platform integrity or legal compliance, the Company may take immediate action without prior notice.

25.2. Such action may include removal of Content, restriction of communication, suspension or termination of an Account, preservation of Digital Evidence and notification to competent authorities where appropriate or required by Applicable Law.

26. Digital Evidence and Record Preservation

26.1. For purposes of safety, fraud prevention, cybersecurity, investigation, dispute resolution and legal compliance, the Company may preserve relevant Electronic Records and Digital

Evidence, including Account activity, communications, reports, timestamps, IP information, device information, moderation records, audit logs, security records and metadata, subject to Applicable Law and the Privacy Policy.

26.2. Such records may be used for legitimate operational, investigative, regulatory or legal purposes and may be disclosed where authorised or required by Applicable Law or lawful process.

27. Law Enforcement Cooperation

27.1. The Company may cooperate with courts, police authorities, cybercrime authorities, regulatory bodies, governmental authorities, CERT-In and other competent authorities in accordance with Applicable Law.

27.2. Where legally permissible and appropriate, the Company may preserve or disclose relevant information in response to lawful requests, court orders, statutory requirements, emergency circumstances or investigations involving suspected unlawful conduct.

28. No Guarantee of Complete Safety

28.1. Although the Company may implement verification, moderation, cybersecurity, fraud-detection, reporting and other reasonable safety measures, the Company does not represent or warrant that every User will be genuine, every Profile will be accurate, every violation will be detected or every harmful interaction can be prevented.

28.2. Users acknowledge that online matrimonial interactions involve inherent risks and that independent verification, reasonable caution and personal judgment remain essential.

29. Matrimonial Disclaimer

29.1. The Platform facilitates matrimonial introductions and related digital services but does not guarantee compatibility, engagement, marriage, relationship success, family acceptance, financial compatibility, emotional compatibility or any particular matrimonial outcome.

29.2. A Profile, recommendation, verification badge, ranking, match or AI-generated suggestion shall not be interpreted as an endorsement, certification or guarantee by the Company.

30. Appeals and Review

30.1. Where an appeal or review mechanism is made available, a User may request review of an enforcement decision through the prescribed channel and within the applicable period.

30.2. The Company may request additional information or evidence and may uphold, modify or reverse an enforcement decision based upon its review.

30.3. Nothing in this Policy shall create an unconditional right to reinstatement or restoration of

an Account except where required by Applicable Law.

31. Anti-Retaliation

31.1. The Company does not permit retaliation against a person who makes a genuine safety complaint or participates in an investigation in good faith.

31.2. Threatening, intimidating, harassing or otherwise retaliating against a reporting User, complainant or witness may constitute an independent violation of this Policy.

32. Emergency Situations

32.1. The Platform is not an emergency-response or law-enforcement service.

32.2. A User facing an immediate threat to life, physical safety, health or property should immediately contact the appropriate emergency services or competent authorities and should not rely solely upon the Company's reporting mechanism.

33. User Responsibility

33.1. Each User acknowledges that the Company cannot control the conduct of other Users and that the User remains responsible for exercising reasonable judgment and conducting appropriate due diligence before relying upon information, communicating privately, entering into financial arrangements or meeting another person.

33.2. Nothing in this Policy shall be interpreted as transferring the User's personal responsibility for decisions or conduct undertaken by the User.

34. Relationship with the Terms of Use and Other Policies

34.1. This Policy supplements and forms part of the Company's Terms of Use and does not replace the contractual provisions contained therein.

34.2. The Privacy Policy governs the Company's Processing of Personal Data, the Content Moderation & User Reporting Policy governs moderation procedures, the Child Safety Policy governs child-protection matters, the Anti-Dowry Policy governs dowry-related conduct, and the AI Policy governs the Company's use of AI and automated technologies.

34.3. The Company may enforce this Policy together with any other applicable policy or contractual provision.

35. Amendment and Updating of Policy

35.1. The Company may modify, amend, update, supplement or replace this Policy from time to time to reflect changes in Applicable Law, judicial or regulatory requirements, Platform functionality, technology, cybersecurity risks, AI systems, operational requirements or emerging safety concerns.

35.2. The updated version shall become effective from the date specified by the Company or

upon publication on the Platform, as applicable.

36. Severability

36.1. If any provision of this Policy is held to be invalid, unlawful or unenforceable, such provision shall, to the extent legally permissible, be modified or severed without affecting the validity and enforceability of the remaining provisions.

37. No Waiver

37.1. Any failure or delay by the Company in exercising or enforcing any right or provision under this Policy shall not constitute a waiver of that right or provision, nor prevent the Company from enforcing the same or any other provision subsequently.

38. Governing Law and Dispute Resolution

38.1. This Policy shall be governed by and construed in accordance with the laws of India.

38.2. Any dispute arising in connection with this Policy shall be dealt with in accordance with the dispute-resolution provisions contained in the Terms of Use, subject to mandatory rights and remedies available under Applicable Law.

39. Reporting and Contact Details

39.1. Safety complaints, suspected violations and other concerns may be reported through the reporting mechanism provided on the Platform or through the Company's designated support or grievance channels.

Safety / Policy Reporting:

Email: support@sarkarihumsafar.com _____

Grievance Officer:

Name: __Renu Sharma_____

Email: support@sarkarihumsafar.com _____

Child Safety Contact:

Name: __Renu Sharma_____

Email: support@sarkarihumsafar.com _____

Registered Office:

Ramisht Kripa Private Limited

40. Final Acknowledgement

40.1. By accessing or using the Platform, every User acknowledges that online matrimonial interactions involve inherent risks; that no verification or moderation system can eliminate every such risk; that Users must exercise independent judgment and reasonable due diligence; and that fraudulent, abusive, unlawful, deceptive, exploitative or unsafe conduct may result in

restriction or termination of access and, where appropriate, preservation of evidence and reporting to competent authorities.

40.2. The Company seeks to maintain a safe, respectful and trustworthy matrimonial environment; however, safety is a shared responsibility and every User is expected to act honestly, respectfully, cautiously and in accordance with this Policy, the Terms of Use and Applicable Law.