Privacy Policy

Navyor Technologies Private Limited (“Navyor”, “we”, “us”, or “our”) operates the Navyor mobile application, website, and related services (collectively, the “Services”).

Navyor is an advanced AI-powered platform for interior design and project management. Our Services empower users to conceptualize and manage interior projects, upload and analyse room and product imagery, generate AI-assisted design concepts, discover curated products, maintain project documentation, and process or oversee applicable orders.

This Privacy Policy outlines our data collection practices, the methods by which we utilize and safeguard your information, the circumstances under which we may share data, and the privacy choices available to you.

By accessing or utilizing our Services, you acknowledge and agree to the data practices established in this Privacy Policy.

1. Information We Collect

1.1 **Account and Profile Information**

When establishing or utilizing a Navyor account, the Company may collect the following categories of information:

- Full legal name, electronic mail address, and telephone number.
- Account credentials, security tokens, and associated authentication data.
- Information transmitted through authorized third-party authentication services, including Google Sign-In, subject to the user's applicable account privacy configurations and explicit user consent.

Limitation of Authentication Methods: Navyor exclusively supports authorized third-party authentication via Google Sign-In where integrated. Navyor does not currently support, offer, or maintain integration for Sign in with Apple.

1.2 **Project and User-Generated Content**

The Services enable Users to initiate, configure, and administer interior design projects. In connection therewith, the Company may collect, process, and store the following categories of data:

- Project identifiers, titles, and descriptive summaries;
- Spatial and architectural parameters, including room specifications;
- Design preferences, styling choices, and product selections;
- Financial and procurement data, including bills of quantities and related project documentation;
- User-generated annotations, memoranda, and operational inputs; and
- Any supplementary content, materials, or media uploaded, transmitted, or otherwise generated by the User in furtherance of a project.

Purpose of Collection: All data collected pursuant to this Section 1.2 shall be utilized strictly for the provision, maintenance, security, and enhancement of the Services, and to facilitate the specific functionalities requested or authorized by the User.

1.3 **Photographs, Files, and Media**

Users may upload, transmit, or otherwise make available photographs, digital files, and media through the Services, which may include, without limitation:

- Photographic representations of interior spaces and rooms;
- Architectural drawings, schematics, and floor-plan images;
- Product photographs and design catalogs; and
- Supplementary interior-related imagery and digital documentation.

Device Access and Permissions: Users may capture and submit such media via their device camera or photo library, strictly contingent upon the permissions granted by the User within the operating system of the applicable device.

Processing and Sub processing: Uploaded photographs and files may be processed, analysed, and stored by the Company and its vetted third-party technology providers solely to deliver core application functionality, including but not limited to:

- Interior design generation and spatial rendering;

- Computer vision analysis and image evaluation;
- Product identification, Stock Keeping Unit (SKU) analysis, and catalog matching;
- Automated image classification and labeling;
- Content moderation and safety enforcement; and
- Any other features or functionalities explicitly requested or authorized by the User.

Use of Photographs and Digital Files: The Company may process photographs and digital files uploaded by Users to provide the Services requested by them, including AI-powered design features and the publication of project images on public Interior Designer profiles, where requested by the User. Users who submit content for public display are responsible for ensuring that they have the necessary rights and permissions for such publication. The Company will use such content for its own advertising, marketing, or commercial promotional purposes only where the User has provided the necessary consent or other lawful authorisation, as applicable.

.

1.4 **Orders and Transactional Data**

To the extent a registered Business User (including interior design firms, independent interior designers, trade contractors, suppliers, and vendor partners) conducts commercial procurement, trade purchasing, or project-fulfillment activities through the NAVYOR marketplace platform, the Company collects, processes, and retains data strictly necessary to execute, settle, and audit business-to-business transactions. Such information shall comprise:

- Commercial Billing & Logistics Addresses: Corporate headquarters, registered billing offices, active project job-site delivery locations, and commercial warehouse receiving coordinates;
- Designee & Site Contacts: Identity, professional designation, and direct contact details of authorized corporate purchasing agents, project managers, or on-site receiving supervisors;

- Commercial Purchase Specifications: Project codes, enterprise purchase orders (POs), bulk itemized manifests, commercial tier pricing, custom finish specifications, and volumetric or freight requirements;
- Trade Sourcing & Material Identifiers: Trade vendor credentials, manufacturer designations, architectural-grade materials specifications, and product Stock Keeping Units (SKUs);
- Corporate Settlement & Invoicing Records: Tax exemption certificates, corporate credit terms, GST/tax identification credentials, transaction settlement confirmations, credit notes, and commercial pro-forma or tax invoices.

1.5 **Payment Processing and Financial Data**

All monetary transactions and commercial settlements conducted through the Services shall be facilitated via Cashfree, acting as the authorized third-party payment gateway and processing merchant.

- **Exclusion of Sensitive Data Retention:** The Company explicitly disclaims the physical or digital retention, storage, or processing of sensitive financial credentials upon its proprietary servers or infrastructure. This exclusion encompasses, without limitation, complete primary account numbers (PAN), card verification values (CVV/CVC), personal identification numbers (PINs), and confidential banking authentication particulars handled directly by Cashfree.
- **Governing Terms of Third-Party Processors:** The collection, transmission, safeguarding, and disposition of all financial and payment-related data shall be governed exclusively by the terms of service, security architectures, and privacy policies enforced by the designated payment service provider, entirely independent of the Company's direct operational control.

1.6 **Device Telemetry and Authentication Data**

The Company reserves the right to collect, process, and retain technical metadata strictly necessary to authenticate Users, validate access credentials, and maintain secure operational sessions across the Services.

- **Local Execution of Biometric Verification:** In the event a User elects to utilize Face ID, fingerprint recognition, or any equivalent native biometric authentication protocol integrated within the underlying hardware, all biometric verification procedures shall be executed exclusively and locally by the operating system of the User's device.
- **Absolute Exclusion of Biometric Acquisition:** The Company expressly covenants and warrants that it shall neither receive, access, collect, process, nor store raw biometric data, templates, facial geometry models, or cryptographic representations derived from a User's Face ID or associated biometric authentication credentials.

1.7 **Camera and Photo Library Permissions**

The Company reserves the right to request system-level access to the User's device camera and photo library strictly conditioned upon the User's affirmative election to capture, upload, or transmit photographic materials in furtherance of the Services.

- **User Configuration and Revocation:** Users retain full sovereignty over their hardware permissions, maintaining the unconditional right to modify, grant, or revoke access to the device camera and photo library at any time via their device's native operating system settings.
- **Purpose-Bound Access:** Access granted to the aforementioned device resources shall be strictly bounded, utilized, and maintained exclusively for the provisioning of core features, operational tasks, and functionalities explicitly initiated or authorized by the User requiring such media processing.

2. **Scope and Purposes of Data Processing**

The Company processes, collects, analyses, and retains personal data and user content exclusively to the extent necessary to perform its contractual obligations,

provide the Services, comply with applicable legal frameworks, and pursue legitimate business interests. Subject to applicable data protection legislation, information processed under this Policy is strictly limited to the following operational, commercial, and legal purposes:

- **Account Administration and Authentication:** Establishing, configuring, maintaining, and administering User credentials; verifying identity; managing access privileges; and preserving structural account integrity.

- **Service Delivery and Platform Capabilities:** Rendering the core features of the platform, including digital interior design generation, architectural spatial planning, and comprehensive project management workflows.

- **Project Archival and Digital Asset Management:** Organizing, cataloging, storing, and maintaining active and archived design assets, metadata, user files, and associated project documentation.

- **Spatial and Media Processing:** Processing digital media, architectural floor plans, spatial dimensions, room photography, and furnishing product imagery.

- **Generative AI and Computer Vision Operations:** Deploying machine learning models, artificial intelligence algorithms, and automated computer vision frameworks to analyze spatial layouts, detect architectural elements, extract spatial metadata, and synthesize interior design visualizations.

- **Content Governance and Platform Safety:** Moderating, auditing, and reviewing user-uploaded assets and system-generated outputs to enforce acceptable use standards and prevent misuse.

- **Inventory, SKU, and Catalog Administration:** Facilitating the tracking, categorization, indexing, and commercial management of furniture, fixtures, materials, and distinct Stock Keeping Units (SKUs).

- **Order Processing and Fulfillment:** Administering, processing, and coordinating the procurement, routing, logistics, and delivery of commercial goods and specified merchandise.

- **Financial and Transactional Processing:** Facilitating payment processing, settlement, and billing transactions through PCI-DSS-compliant third-party payment gateways.

- **Operational and Administrative Communications:** Transmitting non-marketing service notifications, operational alerts, billing notices, security advisories, and status updates concerning ongoing projects or active orders.

- **Customer Care and Technical Diagnostics:** Investigating system errors, diagnosing technical anomalies, troubleshooting software defects, and delivering responsive customer support.

- **Information Security and Fraud Prevention:** Proactively detecting, investigating, mitigating, and remediating security incidents, fraud, unauthorized intrusion, denial of service, and technical vulnerabilities.

- **Legal and Regulatory Compliance:** Satisfying binding statutory obligations, tax reporting standards, judicial processes, subpoenas, and enforceable governmental or regulatory demands.

- **Protection of Rights and Enforcement:** Protecting and defending the legal rights, intellectual property, operational security, and contractual

remedies of the Company, its personnel, its users, and relevant third parties.

- **System Maintenance and Performance Optimization:** Monitoring infrastructure reliability, load balancing, capacity planning, and optimizing service performance, latency, and system availability.

Exclusion of Third-Party Analytics Trackers: Notwithstanding any standard industry practice or provision to the contrary, the Company expressly covenants that it does not embed, deploy, license, or execute third-party analytics trackers, behavioural telemetry monitors, advertising identifiers, or external crash-reporting Software Development Kits (SDKs) within the core architecture of the Navyor application infrastructure.

3. Artificial Intelligence and Automated Data Processing

The Services utilize proprietary and third-party artificial intelligence, deep learning, computer vision, and automated data-processing technologies to deliver generative rendering, spatial analysis, and core platform functionality.

3.1 **Algorithmic Training, Testing, and Optimization**

To the extent permissible under applicable data protection laws, the Company reserves the right to process, analyse, evaluate, and utilize User Content-including text prompts, uploaded source media, structural parameters, and resulting AI-generated outputs-for the purposes of training, fine-tuning, validating, and optimizing its machine learning models, neural networks, and underlying software algorithms. Where technically practicable and commercially feasible, the Company employs data-minimization, pseudonymization, or aggregation techniques prior to utilizing any datasets for model development and platform enhancement.

3.2 **Integrated Third-Party Infrastructure and Sub processors**

Certain AI-driven workflows and analytical tasks rely on specialized third-party infrastructure and model service providers. Depending on the specific tool or feature executed by the User, inputs, metadata, and media may be transmitted to, processed by, or stored across the following infrastructure partners (and their affiliated data hosting environments):

- **Fal.ai:** Deployed for high-throughput image synthesis, diffusion modeling, latent space transformations, and automated visual moderation pipelines.
- **Google Cloud (Gemini):** Deployed for multimodal semantic comprehension, structural image analysis, Stock Keeping Unit (SKU) detection, and content governance workflows.
- **Amazon Web Services (AWS) Recognition:** Deployed for automated computer vision, structural feature extraction, object identification, and spatial labelling.
- **Amazon Web Services (AWS) S3:** Deployed as the underlying encrypted cloud infrastructure for persistent object storage, media caching, and asset archival.

The allocation of tasks across these sub processors varies dynamically based on operational demand, system latency, and functional requirements. All such sub processors are bound by commercially reasonable data protection agreements, confidentiality obligations, and data processing terms compliant with applicable statutory standards.

3.3 **Express Disclaimer of Generative Outputs and Professional Standards**

All visualizations, 2D/3D spatial renderings, material estimations, layout proposals, and automated product mappings generated by the Services are produced algorithmically and provided strictly “as is” and “with all faults” for conceptual, preliminary, and illustrative purposes only.

The Company makes no representations, warranties, or covenants, whether express, implied, or statutory, regarding the geometric precision, physical feasibility, or dimensional fidelity of any AI-generated output. Under no circumstances shall any system output be construed, marketed, or relied upon

as stamped architectural plans, licensed structural or civil engineering drawings, building-code compliance assessments, or professional interior construction documentation. The Services do not replace or substitute for the oversight, inspection, and certification of licensed architects, structural engineers, or credentialed construction professionals.

3.4 **Allocation of Risk and Independent Verification Mandate**

The User acknowledges and agrees that the technical nature of generative artificial intelligence and neural rendering models involves inherent probabilistic risks, including algorithmic hallucinations, non-viable load calculations, scale distortions, and inaccurate product metadata or inventory correlations.

The User bears the exclusive legal and financial duty to independently audit, measure, field-verify, and validate all AI-generated outputs-including dimensional clearances, load requirements, local code conformity, and product procurement schedules-prior to executing any commercial agreements, purchasing materials or furniture, issuing construction bids, or undertaking physical demolition, fabrication, or installation. The Company disclaims all liability for physical damages, financial losses, procurement errors, or regulatory non-compliance arising directly or indirectly from reliance upon generative outputs.

4. Disclosure and Transfer of Personal Data to Third Parties

4.1 **Authorized Third-Party Service Providers**

The Company may disclose, transfer, or otherwise make available user personal data to vetted third-party service providers, contractors, and sub-processors strictly on a need-to-know basis and solely to the extent necessary to perform, support, secure, and optimize the Services. These authorized recipients are limited to the following operational categories and designated providers:

- **Google LLC:** For single sign-on (SSO) authentication services (Google Sign-In) and machine learning/generative artificial intelligence capabilities (Google Gemini);

- **Fal.ai, Inc.:** For artificial intelligence image generation, computer vision workflows, image rendering, and automated content moderation;

- **Amazon Web Services, Inc. (AWS):** For foundational cloud hosting, managed relational/object storage (including Amazon S3), and automated media analysis (including Amazon Recognition); and

- **Cashfree Payments India Private Limited:** For encrypted transaction processing, payment gateway management, and merchant settlement services.

4.2 **Data Minimization and Purpose Limitation**

Any disclosure of personal data to the third parties identified in Section 4.1 shall be strictly governed by the principle of data minimization, restricted solely to the data points reasonably necessary to discharge the contracted technical or operational functions.

4.3 **Independent Processing and Governance**

While the Company executes data processing agreements with its vendors to require commercially reasonable safeguards, the receipt, retention, and processing of personal data by designated third parties shall also be subject to the terms of service, security standards, and privacy disclosures independently maintained by each respective provider.

4.4 **Absolute Prohibition on the Sale of Data**

Notwithstanding anything to the contrary contained herein, the Company affirmatively covenants and warrants that it does not sell, lease, rent, trade, or otherwise monetize or transfer users' personal information or data to any third

party for monetary or other valuable consideration under applicable data protection laws.

5. Data Storage, Security, and Retention

The Company implements and maintains commercially reasonable administrative, technical, and physical safeguards designed to protect collected information against unauthorized access, alteration, disclosure, loss, or destruction.

- **Cloud Infrastructure and Storage:** User data, digital files, and media uploads are hosted and stored via secure third-party cloud infrastructure, including Amazon Web Services (AWS).
- **Limitation of Security Guarantee**: While the Company employs industry-standard security protocols, no method of electronic transmission over the internet or method of digital storage is completely secure. Consequently, the Company expressly disclaims an absolute guarantee of data security.
- **User Security Obligations:** Users assume sole responsibility for maintaining the strict confidentiality of their account credentials, security tokens, and access mechanisms. Users shall immediately notify the Company in writing upon discovering or suspecting any unauthorized access to their account or any other breach of security.

6. Data Retention, Archival, and Secure Disposition

6.1 **Purpose-Limitation and Category-Specific Retention Schedules:** Pursuant to the principles of purpose limitation and data minimization, NAVYOR retains business entity records, trade project assets, commercial communications, and transactional documentation strictly for the operational duration required to execute marketplace agreements, fulfill vendor and buyer covenants, satisfy statutory fiscal mandates, and protect legitimate business interests. Retention schedules for registered Business Users (including interior

design firms, independent design professionals, trade suppliers, and commercial vendors) are administered as follows:

a. **Business Entity Accounts, Designer Profiles, and Trade Credentials:** Enterprise account identifiers, business registration details, trade license filings, team access permissions, and corporate authentication credentials are maintained throughout the active tenure of the Business User's NAVYOR account. Following the validated receipt and processing of an account closure, dissolution, or contractual termination request, all associated personal and representative identifiers shall be permanently deleted or irreversibly anonymized within ninety (90) calendar days, contingent upon the final discharge of outstanding corporate credit terms, invoices, or open commercial trade disputes.

b. **Design Project Media, Architectural Plans, and Specification Assets:** Project-linked design documentation—including CAD drawings, BIM models, site layouts, architectural blue-prints, mood boards, trade schedules, material finish specifications, and algorithmic rendering outputs—are stored to maintain continuity across long-cycle interior construction projects. In the event of uninterrupted enterprise account inactivity exceeding twelve (12) consecutive calendar months, or documented platform abandonment, NAVYOR reserves the contractual right to archive or permanently purge unassigned project assets, without prejudice to the firm's administrative right to manually export or purge project repositories prior to that milestone.

c. **Trade Orders, Freight Manifests, and Fulfillment Records:** Documentation concerning commercial purchase orders (POs), bulk procurement manifests, job-site delivery confirmations, bills of lading (BOL), custom millwork/material inspection sign-offs, and trade return/defect claims is retained for a period of three (3) calendar years following complete project-site delivery. This retention governs trade defect remediation, commercial warranty enforcement, contractual indemnity reviews, and inter-firm dispute resolutions

(excluding statutory consumer-protection frameworks, as transactions on NAVYOR are strictly business-to-business).

d. **Statutory Tax, Corporate, and Fiscal Books of Account:**

Commercial tax invoices, pro-forma estimates, debit/credit notes, payment settlement ledgers, tax exemption documentation, and statutory business identifiers (including Goods and Services Tax Identification Numbers ("GSTIN") or equivalent regional enterprise tax IDs) shall be retained for a mandatory minimum period of eight (8) consecutive fiscal years following the close of the corresponding financial year, or such extended statutory prescriptive term required under applicable corporate governance, commercial trade acts, and direct/indirect taxation enactments.

e. **Commercial Support Logs, Account Escalations, and Trade Dispute Records:**

Correspondence records between business entities and NAVYOR trade support—including technical escalation logs, vendor SLA breach notices, damaged-in-transit trade tickets, and merchant coordination communications—are preserved for twenty-four (24) months following formal matter closure, exclusively for merchant governance, vendor SLA evaluation, and evidentiary substantiation during commercial arbitration or contract claims.

f. **Disaster Recovery Snapshots and System Backups:**

Encrypted database archives, server parity images, and enterprise platform recovery backups operate on automated, rotating lifecycle protocols. These redundant system copies are cryptographically purged or systematically overwritten within a rolling retention period not to exceed sixty (60) calendar days from generation.

6.2 **Legal Holds and Mandatory Statutory Preservation**

Notwithstanding the standard schedules articulated in Section 6.1, the Company reserves the express authority to extend the retention period of relevant records beyond customary disposition thresholds where reasonably deemed necessary to:

- Discharge obligations arising from a binding judicial decree, subpoena, statutory mandate, regulatory audit, or valid administrative process served by an authorized governmental authority; or
- Investigate, establish, pursue, or defend against actual, pending, or reasonably anticipated civil litigation, administrative investigations, or arbitral proceedings, in which circumstance records subject to legal hold shall be maintained until the conclusive, non-appealable determination or formal compromise of the underlying matter.

6.3 **Secure Disposition, Sanitization, and Irreversible De-Identification**

Upon the expiration of the applicable retention schedule, or upon the definitive exhaustion of the legal and operational bases underpinning continued processing, the Company shall effect secure disposal via one of the following methods:

Cryptographic Erasure and Overwriting: Digital assets and associated production records shall be purged using technical sanitization methods aligned with recognized industry standards (such as secure multi-pass overwriting or physical/cryptographic key destruction), rendering the underlying data permanently unrecoverable across all active server environments and logical storage volumes; or

Irreversible Anonymization: Data payloads shall be scrubbed, decoupled, aggregated, or pseudonymize in such a manner that the residual information cannot, through any technological means, be attributed to or reconciled with an identifiable natural person. Resultant anonymized metrics may be retained indefinitely solely for structural optimization, platform telemetry, and macroeconomic analytical reporting.

7. Account Termination, De-Registration, and Permanent Deletion Protocols

7.1 **User-Initiated Account Deletion**

Users maintain the affirmative right to terminate their commercial relationship with the Company and request the permanent de-registration and deletion of their Navyor account at any time. Such requests may be initiated through the native self-service administrative settings within the application interface, or by transmitting a verified deletion petition to the Company's designated Data Protection Officer/Grievance Officer.

7.2 **Operational Scope of Erasure and Sub-Processor Cascading**

Upon receipt, authentication, and execution of a bona fide account deletion request:

- **Primary Logical Erasure:** The Company shall execute automated protocols to permanently de-index, purge, cryptographically erase, or irreversibly anonymize all direct identifiers, registered profile data, and proprietary User-generated content (including uploaded spatial imagery, architectural blueprints, textual input prompts, and generative rendering outputs) across its production databases and logical storage systems.
- **Downstream Sub-Processor Notification:** The Company shall transmit programmatic deletion signals to its integrated third-party infrastructure providers, cloud-hosting vendors, and sub-processors (including AI rendering engines and object storage partners) to ensure the commensurate sanitization of transient caches and associated payload copies, subject to their respective enterprise retention windows.

7.3 **Lawful Grounds for Retention and Statutory Exclusions**

Notwithstanding the receipt of a verified deletion petition, the Company expressly reserves the statutory authority and contractual right to retain segregated subsets of user data and transaction records where continued preservation is mandatory or legally justifiable under applicable law, strictly limited to:

- **Statutory and Fiscal Compliance:** Maintaining commercial books of accounts, tax invoices, transactional metadata, billing party details, and GSTIN-associated records for the mandatory statutory period prescribed under corporate, accounting, and direct/indirect taxation statutes;

- **Regulatory Inquiries and Law Enforcement Mandates:** Satisfying enforceable judicial subpoenas, valid court orders, statutory preservation directives, or formal regulatory investigations issued by competent governmental authorities;

- **Dispute Adjudication and Claim Preservation:** Preserving evidentiary records strictly necessary to initiate, substantiate, enforce, or defend against active, pending, or reasonably anticipated civil litigation, commercial arbitration, chargeback claims, or consumer grievances; and

- **Fraud Prevention and Platform Integrity:** Retaining de-identified telemetry, risk flags, and technical identifiers exclusively to investigate or deter fraudulent activity, severe terms-of-service violations, malicious access attempts, or critical platform security incidents.

7.4 **Technical Quarantine, Purpose Limitation, and Security of Residual Records**

Any personal data or transactional documentation preserved pursuant to the exceptions set forth in Section 7.3 shall be:

- **Functionally Quarantined:** Segregated, logically decoupled, and rendered inaccessible from standard operational and user-facing production workflows;

- **Subject to Strict Purpose Limitation:** Processed solely and exclusively for the specific statutory, fiscal, forensic, or legal purpose for which it was preserved, with all commercial, analytic, and marketing processing immediately and permanently terminated; and

- **Securely Disposed:** Subjected to permanent cryptographic erasure or irreversible sanitization immediately upon the final expiration of the

underlying statutory preservation threshold or the conclusive resolution of the applicable legal proceeding or tax audit.

8. Data Subject Statutory Rights, Grievance Redressal Architecture, and Procedural Protocol

8.1 Recognition and Scope of Statutory Rights

In accordance with prevailing data protection enactments—including the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and cognate data protection regulations across applicable jurisdictions—the Company acknowledges and accords to each User (designated as a "Data Principal") the following enforceable rights, subject to statutory exceptions, lawful reservations, and technical feasibility:

a. Right to Confirmation, Access, and Summary of Processing:

The Data Principal is entitled to obtain formal, written confirmation from the Company as to whether personal data concerning them is undergoing active processing, alongside an intelligible summary of such personal data, an accounting of processing activities undertaken, and the specific corporate identities of all third-party entities, sub-processors, or infrastructure vendors with whom such data has been shared.

b. Right to Correction, Completion, and Updating:

The Data Principal maintains the right to mandate the rectification, formal updating, or supplementation of any inaccurate, misleading, incomplete, or out-of-date personal data, spatial asset metadata, billing coordinates, or commercial account records maintained across the Company's active production environments and logical databases.

c. Right to Erasure and Cryptographic Purging:

The Data Principal may petition for the permanent erasure, de-indexing, and irreversible destruction of their personal data where continued retention is no longer necessary to fulfill the primary commercial or technical purposes for which it was ingested. This entitlement remains subject to the Company's

affirmative right to retain requisite data categories strictly necessary to preserve fiscal, corporate, and statutory records, satisfy anti-money laundering and tax mandates, maintain audit readiness, or assert or defend active or reasonably anticipated legal claims.

d. Right to Revocation of Consent:

Where processing operations are grounded exclusively upon the Data Principal's prior affirmative consent, such consent may be formally revoked at any juncture. Revocation of consent shall operate prospectively and shall not impair the lawful validity or enforceability of processing operations executed prior to the date of formalized receipt of such revocation.

e. Right of Nomination:

Pursuant to applicable statutory governance, the Data Principal maintains the affirmative right to designate, through formal written nomination, an individual authorized to exercise data subject rights or seek administrative redress on the Data Principal's behalf in the event of the Data Principal's death or physical or mental incapacitation.

f. Right to Redressal of Grievance:

The Data Principal retains the right to submit grievances regarding any purported non-compliance, unauthorized processing, or breach of data processing commitments directly to the Company's institutional grievance apparatus, with recourse to competent supervisory tribunals upon exhaustion of internal remedies.

8.2 Procedural Protocol for Invocations and Substantive Determinations

a. **Formal Requisites for Intake:**

To initiate an actionable data subject request pursuant to Section 8.1, the Data Principal must transmit a signed, written application to the designated Grievance Officer set forth in Section 8.3. The submission must satisfy the following formal thresholds:

1. Provide the applicant’s verified legal name, registered user identification handle, and primary email address affiliated with the active or former account;
2. Categorically identify the specific statutory right or remedy being invoked; and

3. Provide a clear and precise statement setting forth the specific project files, spatial media, billing artifacts, or transactional data categories forming the scope of the request.

b. **Verification and Identity Authentication Safeguards:**

The Company reserves the contractual and statutory right to condition any disclosure, rectification, or deletion upon the satisfactory verification of the applicant's bona fides. The Company may deploy multi-factor cryptographic challenges, out-of-band verification tokens via the registered communication interface, or demand statutory identification documentation strictly necessary to forestall fraudulent exfiltration, social engineering, or identity usurpation.

c. **Timelines, Disposition, and Exceptions:**

- The Company shall transmit an electronic acknowledgment of receipt within seventy-two (72) business hours of formal transmission.

- Validated requests shall be substantively reviewed, determined, and executed within thirty (30) calendar days from the date of conclusive identity authentication, or within such prescriptive statutory window as applicable law mandates.

- In the event that archival retrieval complexity, volume of distributed sub-processor assets, or technical infeasibility precludes completion within the initial thirty (30) calendar days, the Company shall furnish written notice setting forth the operational impediments and designating the definitive

fulfillment timeline, which extension shall not exceed statutory allowances.

d. **Functional Consequences of Deletion and Consent Revocation:**

The Data Principal expressly acknowledges that the operational execution of an erasure request or the formal withdrawal of consent regarding core, non-discretionary data payloads (including spatial room imagery, dimensional parameters, architectural floor plans, or primary account credentials) shall render the continuation of automated algorithmic synthesis, rendering engines, and associated platform features technically impossible, effecting immediate and permanent termination of the corresponding active projects without liability to the Company.

8.3 Institutional Grievance Officer and Regulatory Recourse

Pursuant to Section 5(2) and Section 13 of the Digital Personal Data Protection Act, 2023, and Rule 3(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Company has appointed a designated statutory officer to oversee the adjudication of data subject requests, remediate complaints, and interface with regulatory bodies:

- **Official Designation:** Data Protection Lead & Grievance Officer
- **Corporate Entity:** Navyor Technologies Private Limited
- **Registered Corporate Address:** B-2201, Lake Verandah, Hiranandani, Akshaynagar, Near Hulimavu Lake, Bangalore – 560076, Karnataka, India
- **Designated Electronic Grievance Ingestion Channel:** grievance@navyor.com
- **Telephonic Contact Helpline:** +91 8618637591

- **Operating Hours:** Monday through Friday, 10:00 AM to 6:00 PM IST (excluding statutory, national, and gazetted banking holidays)

Regulatory Escalation: If the Data Principal does not receive a substantive disposition within thirty (30) calendar days of acknowledged receipt of the grievance, or if the Data Principal remains aggrieved by the formal determination rendered by the Grievance Officer, the Data Principal is statutorily entitled to escalate the grievance by lodging a formal complaint with the **Data Protection Board of India** or the relevant statutory supervisory authority exercising competent jurisdiction.

9. Authentication via Third-Party Identity Provider (Google Sign-In)

a) **Integration of Federated Authentication Protocols**

Where a User elects to register, access, or authenticate their account via the Google Sign-In single sign-on ("SSO") mechanism or OpenID Connect ("OIDC") protocol, the handshake, cryptographic verification, and credential authentication processes are administered directly and exclusively across infrastructure maintained by Google LLC and its affiliates ("Google").

b) **Scope of Ingested Profile Attributes and Authorization Tokens**

Pursuant to the standardized OAuth permissions framework invoked upon User authorization, the Company ingests and processes only the non-sensitive, core identity parameters transmitted by Google, strictly limited to:

- The User's primary legal or display name;
- Verified primary electronic mail address;
- Google-assigned unique subject identifier (sub ID / alphanumeric user token); and

- Profile photograph URL (where designated as publicly accessible by the User's privacy configurations).

The Company utilizes such ingested data elements solely to generate the User's internal platform account, associate transactional workflows, and maintain session continuity.

c) **Absolute Exclusion of Authentication Secrets**

The Company covenants that it does not intercept, access, capture, decrypt, or retain the User's Google account password, passkeys, multi-factor authentication (MFA) tokens, security challenge responses, or underlying master security credentials. Verification is executed exclusively via cryptographically signed JSON Web Tokens ("JWTs") and short-lived authorization grants issued by Google.

d) **Independent Third-Party Governance and Disclaimers**

The transmission of account data, session lifecycle administration, and identity verification managed by Google are subject independently to Google's respective Terms of Service, the Google APIs Terms of Service, and the Google Privacy Policy. The Company disclaims all liability for unauthorized credential disclosures, session hijacking, or outages originating within Google's identity management systems or arising from compromises of the User's primary Google account.

10. Commercial Eligibility, Business Representative Capacity, and Exclusion of Minors

a. Enterprise Qualification and Strict Prohibition of Minors

The NAVYOR platform is exclusively an enterprise-facing, Business-to-Business trade marketplace designed, operated, and intended solely for legally constituted business entities, professional interior design firms, sole proprietorships, trade contractors, and independent design practitioners. The Services are strictly restricted to natural persons who act solely as duly authorized commercial

representatives, procurement managers, or key personnel of such qualifying business entities, and who have attained the statutory age of majority with full legal capacity to execute enforceable commercial contracts (under the Indian Contract Act, 1872, the Digital Personal Data Protection Act, 2023, and equivalent foreign trade and privacy statutes). Natural persons who have not attained the age of majority ("Minors" or "Children") are strictly disqualified from registering, administering enterprise profiles, or engaging in procurement activities on the platform.

a. **Prohibition on the Ingestion of Minor Data** Because the platform's workflows are strictly restricted to enterprise vendor onboarding, architectural specification, and commercial bulk procurement, NAVYOR does not solicit, register, process, or knowingly retain data pertaining to minors. Authorized Business Users are expressly prohibited from provisioning platform seats, design portal access, or trade communication credentials to any individual under the statutory age of majority. NAVYOR does not deploy consumer-facing tracking, youth-oriented behavioral profiling, or retail advertising mechanisms across its systems.

b. **Remediation and Account Revocation for Unauthorized Ingestion**

   If NAVYOR receives notice, discovers during enterprise KYC verification, or develops reasonable operational suspicion that an account representative, credentialed user, or data payload linked to a trade account pertains to an individual under the legal age of majority

   - NAVYOR shall initiate an immediate forensic audit to isolate the affected credentials, session tokens, corporate sub-

accounts, and associated data payloads across its production environments;

- The individual user seat or, where necessary, the associated business onboarding access shall be immediately quarantined, revoked, or suspended from initiating commercial purchase orders, trade negotiations, and platform interactions; and
- NAVYOR shall deploy secure data sanitization procedures to permanently delete, overwrite, or de-link such records from its production repositories, except for the narrow, legally segregated retention strictly required to demonstrate compliance with statutory regulatory audits or enforce professional trade terms.

c. Enterprise Inquiries and Representation Notices

Any parent, legal guardian, or enterprise officer who discovers that an individual under the age of majority has been improperly registered, listed as an enterprise liaison, or submitted data through a firm's business portal may direct a formal notice to the Company's designated Grievance Officer / Data Protection Officer at grievance@navyor.com. Upon verification of the request, NAVYOR shall immediately execute the deletion, credential invalidation, and permanent cessation of processing concerning the individual's records.

11. Cross-Border Data Transmission and Extraterritorial Processing Regimes

11.1 **Engagement of Global Infrastructure and Extraterritorial Dissemination:**

To effectuate the advanced computational workflows, computer-vision indexing, generative diffusion renderings, and distributed cloud-hosting architecture comprising the Services, the Company interfaces with enterprise infrastructure

providers and specialized application programming interface ("API") sub-processors, including Amazon Web Services, Inc., Fal, Inc., and Google LLC. In consequence thereof, User personal data, uploaded photographic media, architectural floor plans, textual prompts, and system metadata are routinely transmitted across sovereign boundaries to, ingested by, and hosted upon server infrastructures situated outside the Republic of India, primarily within the United States of America and other designated overseas jurisdictions hosting such enterprise data centres.

11.2 **Statutory Harmonization with Indian Data Protection Jurisprudence:**

All cross-border flows of personal data and extraterritorial computational operations are undertaken in rigorous compliance with the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the Information Technology Act, 2000 read with the applicable rules, gazetted regulations, and notifications issued thereunder by the Central Government of India:

d. Adherence to the Negative List Regime:

Pursuant to Section 16(1) of the DPDP Act, the Company covenants that it does not transfer, route, or disclose personal data to any foreign jurisdiction, territory, or state that has been expressly placed on the restricted list, embargoed, or otherwise blacklisted by the Central Government via official statutory notification.

e. Mandatory Contractual Governance and Technical Equivalency:

The Company subjects every foreign recipient, cloud host, and third-party sub-processor to enforceable, bilateral Data Processing Addenda ("DPAs"), enterprise compliance terms, or equivalent cross-border data protection instruments that contractually obligate the foreign entity to:

- Ingest, process, and retain the transmitted data strictly upon the verified, documented operational instructions of the Company and solely within the scope of the disclosed functional capabilities;
- Institute and maintain administrative, operational, and cryptographic safeguards-including TLS 1.3 encryption in

transit and AES-256 cryptographic standards at rest-that provide a level of security and integrity no less stringent than that mandated under the DPDP Act and relevant statutory frameworks; and

- Abide by strict non-disclosure obligations, prompt statutory breach notification protocols, and mandatory data sanitization, cryptographic erasure, or repatriation upon the expiration or fulfillment of the contracted computational task.

f. Paramountcy of Sectorial and Financial Localization Directives:

Notwithstanding the extraterritorial computational processing authorized herein, the Company ensures that all core financial instruments, card tokenization databases, and payment aggregation flows administered via Cashfree Payments India Private Limited remain strictly compliant with the relevant data localization mandates and storage directives promulgated by the Reserve Bank of India ("RBI").

11.3 **User Consent, Extraterritorial Processing Mandate, and Jurisdictional Remedies:**

By accessing the platform and uploading spatial imagery, project data, or personal details for processing, the User provides express, informed, and unequivocal authorization for the cross-border transit, extraterritorial processing, and enterprise cloud hosting of such data in accordance with the safeguards set forth in this Section. Extraterritorial processing shall not prejudice, impair, or diminish the User's substantive statutory rights under the laws of India, including the right to enforce compliance or pursue remedial.

12. Business User Content, Trade Intellectual Property Covenants, and Marketplace Governance

a. Continuing Representations and Warranties of Professional Title:

The Business User (including interior design firms, independent interior designers, trade contractors, and commercial specifiers) represents and warrants on a continuing basis that it holds all requisite corporate authority,

commercial licenses, statutory authorizations, and intellectual property clearances necessary to lawfully upload, submit, transmit, or configure architectural drawings, BIM models, CAD technical drafts, spatial elevations, site surveys, room photography, dimensional schedules, trade finish prompts, and commercial procurement specifications (collectively, "Business User Content") across the NAVYOR platform.

b. Covenants Against Prohibited and Infringing Trade Submissions:

The Business User strictly covenants that no Business User Content submitted through the platform shall infringe, misappropriate, or violate any patent, registered design right, copyright, trademark, trade dress, trade secret, or proprietary intellectual property entitlement of any third party (including architectural firms, commercial brand licensors, or product manufacturers), nor shall it breach applicable trade confidentiality, commercial nondisclosure agreements, or statutory privacy frameworks.

c. Project Site and Real Property Authorizations:

The Business User expressly represents and warrants that all job-site photography, structural survey scans, commercial blueprints, and spatial layouts ingested into the platform are submitted with the verifiable authorization and consent of the underlying commercial property owner, corporate client, real estate developer, principal architect, or structural rights holder.

d. Prohibition of Illicit Payloads and Enterprise System Abuse:

The Business User shall not ingest or distribute any content that is unlawful, defamatory, deceptive, or trade-libelous, nor shall it deploy malicious code, automated scraping mechanisms, vulnerability-scanning routines, executable exploits, or unauthorized API integrations designed to compromise NAVYOR's marketplace architecture, trade pricing structures, or cloud infrastructure.

e. **Harmonized Grant of Global Operational and Computational License:**

To ensure seamless enterprise service execution across the marketplace, the Business User grants to NAVYOR, its corporate affiliates, assigns, and contracted technical sub-processors a worldwide, non-exclusive, royalty-free, fully paid-up, transferable, and sublicensable license to host, store, cache,

reproduce, reformat, translate, analyze, index, and computationally process Business User Content solely for the purpose of operating, maintaining, and delivering the marketplace services.

f. Permitted Scope of Processing and Service Execution:

The license granted above is exercisable strictly to execute core platform operations invoked by the Business User, including automated material take-offs, computer-vision spatial tagging, algorithmic finish matching, dynamic Bill of Quantities (BOQ) compilation, trade catalog indexing, and enterprise design-to-procurement rendering workflows, including routing essential payload data across authorized technical API sub-processors.

g. Permitted Algorithmic Optimization and System Calibration:

NAVYOR is licensed to utilize submitted project data, trade prompts, and system configurations to train, evaluate, test, and calibrate its proprietary architectural-search engines, automated estimation models, and visual-spatial algorithms, subject strictly to enterprise anonymization, commercial de-identification, and data minimization protocols that strip corporate identities and client project references.

h. Reservation of Underlying Ownership and Proprietary Rights:

Except for the operational, computational, and indexing licenses expressly conferred herein, the Business User retains full proprietary copyright, trade ownership, and title in and to its original Business User Content, design documents, and project deliverables.

i. Statutory Marketplace Intermediary Classification:

Pursuant to Section 79 of the Information Technology Act, 2000, and applicable electronic marketplace governance rules, NAVYOR functions strictly as a digital technology intermediary. NAVYOR provides a neutral commercial trading platform and enterprise specification ecosystem through which registered business buyers discover, configure, negotiate, and procure trade fixtures, structural furnishings, and architectural-grade materials supplied by independent third-party manufacturers, industrial suppliers, millwork

fabricators, or wholesale trade vendors (collectively, "Third-Party Trade Vendors").

j. Disclaimer of Seller-of-Record Status:

Unless expressly and contractually designated as the legal "Seller-of-Record" on a specific transaction manifest, enterprise purchase order (PO), or commercial tax invoice, NAVYOR is not the legal seller, manufacturer, merchant-of-record, or titleholder with respect to commercial physical goods, raw materials, or trade Stock Keeping Units (SKUs) cataloged or procured across the marketplace.

k. Direct Vendor-to-Business Contract and Commercial Accountability:

The legal contract for the sale, transfer of commercial title, freight risk, merchantability, and structural performance of physical materials is formed strictly and directly between the purchasing Business User and the respective Third-Party Trade Vendor. The Third-Party Trade Vendor bears sole, non-delegable responsibility for commercial product specifications, regulatory compliance, commercial labeling, bills of lading (BOL), factory transit insurance, trade defect claims, commercial restocking terms, and formal manufacturer warranties.

l. Disclaimer of Product Liability and Limitation of Commercial Remedies:

To the fullest extent permitted under applicable law, NAVYOR disclaims all express, statutory, or implied warranties regarding physical materials, fixtures, or contract-grade furnishings procured via the platform, including implied warranties of merchantability, structural durability, code compliance, or fitness for a specific commercial architectural application. NAVYOR assumes no civil, tort, or product liability for manufacturing defects, job-site delivery delays, freight damage, installation failures, or business interruption sustained by the Business User or its underlying commercial clients. Commercial remedies remain strictly governed by the applicable Third-Party Trade Vendor's enterprise terms of sale.

13.1 **Third-Party Artificial Intelligence and Cloud Infrastructure Providers**

a. **Technical Integration and Infrastructure Sub-Processing:**

The Services rely on and interface with designated third-party application programming interfaces ("APIs"), machine learning models, and cloud infrastructure to deliver automated spatial analyses, computer vision processing, and generative media synthesis. Subject to the specific functional workflows initiated by the User, User Content—including photographic assets, architectural plans, dimensional metadata, room imagery, and associated textual prompts—may be transmitted to, ingested by, and processed across cloud systems maintained by the following vetted sub-processors:

- **Fal, Inc. (Fal.ai):** For diffusion-based algorithmic image synthesis, visual transformations, and automated content moderation workflows;

- **Google LLC / Google Cloud Platform (Google Gemini):** For multimodal spatial reasoning, contextual semantic analysis, Stock Keeping Unit ("SKU") identification, and automated data tagging;

- **Amazon Web Services, Inc. (AWS Rekognition):** For algorithmic visual search, automated object detection, and spatial indexing; and

- **Amazon Web Services, Inc. (AWS S3):** For encrypted object storage, persistent digital hosting, and foundational system archival.

b. **Processing Scope and Artificial Intelligence Governance:**

- **Need-to-Know Processing:** The Company transmits User Content to third-party sub-processors solely to the extent strictly necessary to execute the computational, rendering, or analytical outputs expressly requested by the User.

- **Exclusion from Model Training:** All data transmissions to the aforementioned sub-processors are executed via developer-tier, commercial enterprise API architectures. Pursuant to the respective Data Processing Addenda ("DPAs") and enterprise service terms binding the

Company and each vendor, API payloads submitted by or through the Company are contractually excluded from being used, retained, or ingested to train, tune, or align general-market foundational or public AI models.

- **Diagnostic and Security Caching:** Users acknowledge that sub-processors may temporarily retain ephemeral diagnostic logs and technical telemetry strictly for statutory compliance, fraud detection, security verification, and rate-limiting purposes, in conformity with enterprise security protocols.

- **Independent Provider Frameworks:** While the Company enforces standard contractual safeguards and encryption protocols, data processed beyond the Company's direct server environment remains subject to the documented security baselines and administrative policies of the respective infrastructure provider.

13.2 **Financial Transactions and Payment Aggregator Infrastructure (Cashfree)**

a. **Appointment of Authorized Payment Aggregator:**

The Company engages **Cashfree Payments India Private Limited ("Cashfree")**, an entity authorized and regulated by the Reserve Bank of India ("RBI") as a Payment Aggregator, to administer digital payment processing, merchant settlements, and transactional routing across the Services.

b. **Division of Technical and Operational Responsibilities:**

To maintain compliance with applicable regulatory mandates and data security standards, transactional handling and financial data custody are apportioned as follows:

- **Direct Handling of Sensitive Payment Credentials (Cashfree):**
  All payment instrument capture, routing, and tokenization—including full debit and credit card numbers, Card Verification Value ("CVV") codes, net-

banking authentication parameters, and Unified Payments Interface ("UPI") PINs—are executed exclusively through Cashfree's PCI-DSS Level 1-certified infrastructure via secure iframes, Software Development Kits ("SDKs"), or encrypted redirect pathways. The Company does not intercept, inspect, process, or store raw, unencrypted cardholder data or sensitive payment authentication credentials on its systems. All such handling is governed independently by Cashfree's user agreements and privacy disclosures under the regulatory oversight of the RBI.

- **Commercial Records and Statutory Compliance (The Company):**
  The Company captures, logs, and retains non-sensitive transactional metadata necessary to establish commercial records, satisfy statutory bookkeeping obligations, and provide operational support. These data elements are limited to

    - **Commercial Reconciliation:** Internal order identifiers, gateway transaction references, transaction statuses (e.g., authorized, failed, pending), currency denominations, and settled amounts;

    - **Taxation and Accounting:** Billing entity identity, corporate or business designations, registered physical addresses, and Goods and Services Tax Identification Numbers ("GSTIN"), retained for generating, issuing, and archiving statutory tax invoices and audit trails pursuant to applicable tax legislation; and

    - **Dispute and Refund Administration:** Transaction summary data utilized to authenticate users, process cancellations, facilitate approved refunds or chargebacks, and investigate billing discrepancies.

c. **Scope of Transmission and Commercialization Restrictions:**

User data shared with Cashfree is strictly restricted to billing and verification fields reasonably required to authenticate the transaction (including payor name, registered billing address, email address, telephone contact number, and invoice value). The Company covenants that it shall not sell, license, lease, assign, or otherwise commercialize financial transaction data or user personal information to any third party for marketing, promotional, or monetary consideration.

14. Modifications, Amendments, and Periodic Regulatory Review

14.1 **Reservation of Unilateral Amendment Authority**

NAVYOR hereby expressly reserves the legal right, exercisable within its reasonable commercial discretion, to amend, restate, modify, supplement, or supersede this Privacy Policy in whole or in part at any time. Such amendments may be executed to ensure continuous alignment with applicable statutory, regulatory, or administrative frameworks, to integrate advancements in enterprise infrastructure and technical sub-processors, or to accommodate structural modifications to NAVYOR's Business-to-Business marketplace architectures, procurement workflows, and commercial operations.

14.2 **Advance Notification Framework for Material Revisions**

In the event that any proposed modification constitutes a "Material Revision"—defined objectively as any structural modification that substantially expands the categories or volume of business entity or representative data collected, authorizes novel classifications of commercial third-party sub-processors, materially broadens discretionary enterprise disclosures, or adversely curtails the legal rights or procedural remedies of registered business users:

Mandatory Advance Notice Period NAVYOR shall undertake commercially reasonable endeavours to furnish formal notice to all registered business entities not less than thirty (30) calendar days prior to the operational effective date of such Material Revision.

Prescribed Modes of Transmission: Formal notice shall be transmitted via prominent administrative notices, pinned dashboard alerts, or persistent modal notifications within the authenticated enterprise portal, or dispatched via electronic mail to the designated primary corporate administrative address associated with the Business User's registered account.

Immediate Enforceability of Administrative Updates Non-substantive grammatical corrections, typographical rectifications, administrative clarifications, corporate registry updates, or expedited statutory compliance notices that do not diminish the contractual protections or privacy assurances afforded to the Business User shall take legal effect immediately upon digital publication on the platform.

14.3 **Legal Effectivity, Deemed Assent, and Exclusive Recourse**

The operative version of this Privacy Policy shall govern all commercial engagements, platform integrations, and transactional interactions across the NAVYOR marketplace commencing on the date designated in the "Effective Date" or "Last Updated" preamble set forth herein.

- **Constructive and Binding Enterprise Assent:** The continued access, administrative login, API synchronization, placement of commercial purchase orders, execution of procurement contracts, or subscription renewal by a Business User or its authorized personnel subsequent to the formal posting or effective date of an amended Policy shall constitute unequivocal, legally binding, and irrevocable acceptance of the modified terms by the business entity.

- **Exclusive Remedy for Non-Assent:** If a Business User objects to or refuses to be bound by any revised term or condition, its sole and exclusive legal recourse shall be to immediately cease all utilization of the Services, terminate enterprise platform sessions, and submit a formal petition for corporate account de-registration and associated data sanitization in accordance with Sections 7 and 8 of this Policy; provided, however, that such de-registration shall remain subject to the prior settlement of all accrued commercial liabilities, open trade receivables, pending purchase orders, and mandatory statutory fiscal retention schedules.

15. Contact and Communications

For any inquiries, questions, formal complaints, or statutory requests concerning this Privacy Policy, data privacy practices, or personal information handling, Users may contact the designated representatives of the Company:

- **Corporate Entity:** Navyor Technologies Private Limited
- **Registered Office Address:** B-2201, Lake Verandah, Hiranandani, Akshaynagar, Near Hulimavu Lake, Bangalore – 560076, Karnataka, India
- **Electronic Mail:** help@navyor.com
- **Official Website:** https://www.navyor.com
- **Verification Requirement:** To ensure proper security and prompt processing, privacy-related requests must include sufficient identifying information to enable the Company to verify the User's account and fully comprehend the nature of the request.

16. Governing Law, Dispute Resolution, and Forum Jurisdiction

16.1 Governing Law and Choice of Substantive Rule

This Privacy Policy, including its formation, validity, interpretation, performance, breach, and all non-contractual obligations or claims arising out of or in connection with the subject matter hereof, shall be governed by, construed under, and enforced in accordance with the substantive and procedural laws of the Republic of India, without giving legal effect to any principles of conflict of

laws or private international law rules that would mandate or permit the application of the statutory framework of any other jurisdiction.

16.2 **Mandatory Statutory Carve-Outs for Consumer and Privacy Entitlements**

The choice of Indian law set forth in Section 16.1 shall operate without prejudice to, and shall not operate to derogate from, any non-waivable, mandatory statutory protections, procedural safeguards, or fundamental rights explicitly afforded to the User under prevailing data protection statutes (including the Digital Personal Data Protection Act, 2023) or mandatory consumer protection enactments in force within the specific territorial jurisdiction where the User maintains ordinary residence.

16.3 **Exclusive Forum and Judicial Jurisdiction**

Subject to the exhaustion of statutory grievance redressal mechanisms and statutory recourse available before the competent data protection supervisory authority (such as the Data Protection Board of India), the Courts and judicial tribunals possessing competent subject-matter jurisdiction situated at **[Bengaluru, Karnataka]**, India, shall have exclusive, competent, and final jurisdiction to entertain, adjudicate, and settle any suit, action, legal petition, or formal proceeding arising out of, relating to, or concerning the interpretation, validity, or enforcement of this Privacy Policy.

16.4 **Waiver of Inconvenient Forum**

Each party hereby irrevocably and unconditionally submits to the exclusive jurisdiction of the competent courts designated in Section 16.3, and waives any affirmative defense, objection, or plea asserting lack of personal jurisdiction, improper venue, or *forum non conveniens* in respect of any proceeding properly instituted in such judicial forums.

© 2026 Navyor Technologies Private Limited. All rights reserved.