

ANICA FOODS LLP

CORPORATE PRIVACY, INFORMATION GOVERNANCE & DATA SHIELD POLICY

Export Brand: Indian Shroom Company | <https://indianshroom.com>

Principal Place of Business: Hyderabad, Telangana – 500034, Republic of India

Document Reference	AFLLP/LEG/POL/2026-V2.0 (supersedes AFLLP/LEG/POL/2026-V1.0 in its entirety)
Issuing Entity (Data Fiduciary)	Anica Foods LLP, a limited liability partnership registered under the Limited Liability Partnership Act, 2008, trading internationally under its export brand “Indian Shroom Company” GSTIN 36ABWFA3372N1ZP IEC ABWFA3372N FSSAI Licence 30260616124921326
Structure of this Policy	Part A – Privacy Notice (statutory notice to individuals) Part B – Commercial Data, Confidentiality & Non-Circumvention Terms (binding on accepting Counterparties) Schedule 1 – Itemised Personal Data Inventory Annex 1 – Counterparty Acknowledgement & Consent
Principal Legal Framework	Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 (as and when each provision comes into force) Information Technology Act, 2000 and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (while in force) Indian Contract Act, 1872 Arbitration and Conciliation Act, 1996 Foreign laws to the extent they mandatorily apply (Clause A15)
Audit Methodology Reference	Second-party audits conducted in accordance with the guidelines of ISO 19011:2026 (Guidelines for auditing management systems). Anica Foods LLP is not a certification body and does not issue certificates.
Effective Date & Review	Effective 1 October 2026 Scheduled review on or before 13 May 2027 (commencement of the substantive obligations under the DPDP Rules, 2025) and at least annually thereafter
Status	Public document Adopted by resolution of the Designated Partners

HOW TO READ THIS POLICY

This Policy is issued by Anica Foods LLP (“AFLLP”, “Anica”, “we”, “us” or “our”). It has two parts that serve two different legal functions, and the distinction is deliberate:

- **Part A (Privacy Notice)** tells every individual whose personal data we process what we collect, why, on what legal basis, with whom it is shared, how long it is kept and how to exercise their rights. Part A is a notice under Section 5 of the Digital Personal Data Protection Act, 2023 (“**DPDP Act**”). It does not take away, and cannot be read as taking away, any right that an individual has under applicable law.
- **Part B (Commercial Terms)** governs the commercial information, codes, audit outputs, highlights and insights that we exchange with businesses. Part B binds a Counterparty only once it has been accepted in the manner set out in Clause B1 (for example, by written acceptance of Annex 1, or by accepting a quotation, proforma invoice, purchase order, sales contract, audit booking or consultancy engagement that incorporates this Policy by reference). Merely visiting our website does not bind anyone to Part B.

Where a separately signed Master Multi-Shipment Supply Agreement, Memorandum of Understanding or Non-Circumvention & Non-Disclosure Agreement exists between Anica and a Counterparty, that signed document prevails over Part B to the extent of any inconsistency. Capitalised terms are defined in Clause B2 or where they first appear.

PART A — PRIVACY NOTICE

OPERATIONAL REALITY & LEGAL SHIELD: TRANSPARENT NOTICE IS OUR FIRST LINE OF DEFENCE

Anica is a business-to-business merchant-exporter and a second-party audit agency. We collect only the personal data we need to verify, audit, trade with and ship for our Counterparties. We verify every Counterparty through KYC, we refer to Counterparties by internal codes outside our core registers, and we never sell or share our database or knowledge base. We share only code-indexed highlights and aggregated insights, as described below.

A1. WHO WE ARE AND WHOM THIS NOTICE COVERS

A1.1 Data Fiduciary. Anica Foods LLP determines the purpose and means of the processing described in this Part A and is the “Data Fiduciary” under Section 2(i) of the DPDP Act. “Indian Shroom Company” is Anica's export brand and is not a separate legal entity.

A1.2 Our business. Anica is a trading company. It does not own a manufacturing unit. It operates (i) as a quality-assurance agency conducting second-party audits of farmers, Farmer Producer Organisations (“FPOs”), processors and other suppliers; (ii) as a curated merchant-exporter of agricultural and food products; and (iii) as a mushroom-farm consultancy.

A1.3 Persons covered. This Part A applies to the personal data of the following individuals (each a “Data Principal”):

- (a) proprietors, partners, directors, authorised signatories, employees and representatives of our suppliers, farmers, FPOs, cooperatives, aggregators, processors, packers, cold stores, testing laboratories, logistics providers, freight forwarders, customs brokers, inspection agencies and other service providers;
- (b) individual farmers and sole proprietors who deal with us in their own name;
- (c) proprietors, officers and representatives of buyers, importers, distributors, food manufacturers and brands, including clients who commission a second-party audit and clients of our farm consultancy;
- (d) individuals present at premises we audit, to the limited extent described in Clause A2.1(e);
- (e) individuals who contact us through indianshroom.com, email, telephone, WhatsApp Business, Instagram or Facebook; and
- (f) retail and direct-to-consumer customers, when and if we commence such sales (Clause A13).

A1.4 Outside the scope of this notice. This Part A does not cover (i) information about a business entity that is not personal data (which is governed by Part B), (ii) data that has been anonymised so that no individual can be identified, or (iii) third-party websites and platforms, which are governed by their own policies.

A2. PERSONAL DATA WE COLLECT

A2.1 Categories. An itemised description of the personal data we process, for each category of Data Principal, together with the specified purpose, legal basis and retention period, is set out in **Schedule 1**, which forms part of this notice. In summary, we collect:

- (a) **Identity and contact data:** name, designation, organisation, business address, business email address, telephone and WhatsApp number, country.
- (b) **KYC and verification data:** Permanent Account Number (PAN), passport, voter identity card or driving licence; photograph appearing on such document; signature; beneficial-ownership declarations; board resolutions and letters of authority for signatories. **Aadhaar:** we accept an Aadhaar document only if the Data Principal voluntarily chooses to provide it, and only in masked form (first eight digits redacted). We do not ask for, accept or store an unmasked Aadhaar number, and we do not make Aadhaar a condition of dealing with us.
- (c) **Registration data of individual traders and farmers:** GSTIN, IEC, FSSAI licence or registration, APEDA or Spices Board registration, FPO or cooperative membership details, and similar identifiers where the holder is an individual or sole proprietor.
- (d) **Financial data:** bank account details for making or receiving payments (for example, a cancelled cheque or bank letter), invoices, payment and export-realisation records, credit reports, credit-insurance limits and bank references.

(e) **Audit and site data:** photographs, video and audio recordings of premises, equipment and processes (which may incidentally capture individuals present); recordings of remote (online) audit sessions; notes of audit interviews; the names and roles of persons interviewed; farm location and GPS coordinates; and test reports. Where hygiene or food-handler requirements are audited, we sight the relevant records (for example, medical-fitness or training certificates) but record only whether the requirement is met; we do not copy or retain medical records.

(f) **Communications data:** the content and metadata of emails, WhatsApp, Instagram and Facebook messages, call notes, and enquiries submitted through our website form (name, company, email, telephone, country, product interest, quality grade and message).

(g) **Technical data:** basic server and access logs (such as IP address, browser type and timestamps) recorded by our website hosting and platform providers. We do not currently use analytics or advertising cookies (Clause A16).

A2.2 What we do not seek. We do not seek personal data revealing religion, caste, political opinion, sexual orientation, health or biometric data, except incidentally as described in Clause A2.1(e), and we ask Counterparties not to send it.

A2.3 Children. Our business is not directed at children (persons under eighteen years). We do not knowingly process a child's personal data. We do not photograph minors during audits. Any image or record that incidentally captures a minor is blurred or deleted, and any observation relevant to child-labour compliance is recorded as a finding without identifying the child.

A3. SOURCES OF PERSONAL DATA

We collect personal data (i) directly from the Data Principal; (ii) from the organisation the Data Principal represents; (iii) from public registers and official portals (for example, GSTN, the Ministry of Corporate Affairs, DGFT, FSSAI, APEDA and court records); (iv) from service providers such as testing laboratories, customs brokers, freight forwarders, banks, the Export Credit Guarantee Corporation of India and credit-information agencies; (v) from a client who commissions an audit of its own supplier (such client being responsible under Clause B3.5 for having the right to share that data); and (vi) from trade directories, trade fairs and published business sources.

A4. PURPOSES FOR WHICH WE PROCESS PERSONAL DATA

We process personal data only for the following specified purposes:

- (1) responding to enquiries and preparing quotations and samples;
- (2) onboarding and KYC verification of Counterparties, including checks against government registers, sanctions and denied-party lists, credit and credit-insurance sources, litigation records and adverse media;
- (3) planning, conducting and following up second-party audits, remote surveillance audits, laboratory testing, quality rating and corrective and preventive action (CAPA);
- (4) negotiating, concluding, performing and administering procurement, sales, audit and consultancy engagements, including packing, logistics, export documentation, payments and export realisation;
- (5) complying with the laws that apply to us, including customs, foreign trade, GST, income-tax, foreign exchange, food safety, plant quarantine and export promotion requirements, and the import requirements of destination countries;
- (6) traceability, product recall, complaint and claim handling;
- (7) internal record-keeping, search, reporting and business management through our internal platform, ANICA.AI (Clause A8);
- (8) preparing aggregated and anonymised insights (once data is anonymised it is no longer personal data);
- (9) sending business updates to persons who have opted in (Clause A14);
- (10) establishing, exercising or defending legal rights and claims; and
- (11) information security, backup, logging and incident response.

We will not use personal data for a purpose that is materially different from the above without first giving a fresh notice and, where required, obtaining fresh consent.

A5. LEGAL BASIS FOR PROCESSING

A5.1 Under Indian law. We process personal data on the following grounds recognised by the DPDP Act:

(a) **Consent (Section 6):** which is obtained through this notice together with a clear affirmative action, such as the written acceptance of Annex 1, the submission of KYC documents after receiving this notice, or a written “I accept” reply by email or WhatsApp. Consent is free, specific, informed, unconditional and unambiguous, is limited to the personal data necessary for the specified purpose, and may be withdrawn at any time (Clause A9.3).

(b) **Certain legitimate uses (Section 7):** including where a Data Principal has voluntarily provided personal data for a specified purpose and has not indicated that they do not consent to its use (Section 7(a)), for example when sending an enquiry or a business card; where we must disclose information to the State or its instrumentalities under law (Section 7(d)); and where we must comply with a judgment, decree or order (Section 7(e)).

(c) **Exemptions (Section 17):** to the extent applicable, including processing necessary for enforcing any legal right or claim (Section 17(1)(a)) and processing in the interest of prevention, detection or investigation of any offence or contravention of law (Section 17(1)(c)).

A5.2 Transitional position. Until the relevant provisions of the DPDP Act and the DPDP Rules, 2025 come into force, we also comply with Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (“**SPDI Rules**”). Where we collect sensitive personal data or information within the meaning of the SPDI Rules (for example, bank account details), we do so with the provider’s consent in writing, which includes consent given electronically through Annex 1.

A5.3 Outside India. Where a foreign data-protection law mandatorily applies to our processing, the additional legal bases and rights described in Clause A15 apply.

A6. COUNTERPARTY CODES AND PSEUDONYMISATION

OPERATIONAL REALITY & LEGAL SHIELD: UNIQUE COUNTERPARTY CODES

Every verified supplier, vendor, service provider and buyer is assigned an internal unique code. Outside our core contact registers, and in everything we share with other Counterparties, you are referred to by that code, not by name.

A6.1 Assignment. After KYC verification, each Counterparty is assigned a unique alphanumeric code (a “**Code**”) generated by an internal, pre-defined method. Codes are assigned and maintained under the control of Anica’s Designated Partners.

A6.2 Use. Outside our core contact registers, our records, audit highlights and communications with other Counterparties identify a Counterparty by its Code.

A6.3 Candid limitation. A Code is a pseudonymisation measure, not anonymisation: Anica can link a Code back to the Counterparty, so data held against a Code that relates to an individual remains personal data and receives the full protection of this notice. The Code system reduces, but cannot by itself eliminate, the risk that a third party with independent knowledge might identify a Counterparty. For this reason Part B contractually prohibits any attempt at de-anonymisation.

A7. WITH WHOM WE SHARE PERSONAL DATA

OPERATIONAL REALITY & LEGAL SHIELD: NO DATABASE SHARING — HIGHLIGHTS BY CODE ONLY

We do not sell, rent, lease, license or trade our database, contact registers or knowledge base, and we do not give any company, firm or individual access to them. What we share with other Counterparties is limited to code-indexed highlights, redacted audit dossiers and aggregated insights, subject to the narrow exceptions in this Clause A7.

A7.1 Other Counterparties (highlights by Code). A buyer may receive code-indexed highlights, a quality score or grade, and a redacted audit dossier concerning a supplier. Redaction removes names, addresses, GPS coordinates, contact details, registration numbers, logos, faces and any other information that could reasonably identify the supplier or an individual. A supplier may receive specifications, schedules and packing instructions

indexed by the buyer's Code. We do not exchange the names or contact details of suppliers and buyers with each other except under Clauses A7.2 and A7.4, or with the prior written consent of the Counterparty concerned.

A7.2 Commissioned audits. Where a client commissions a second-party audit of a supplier that the client has itself named, the full audit report naming that supplier is delivered to the commissioning client. The supplier is informed of this in advance and gives its written consent when the audit is booked. Anica's proprietary rating methodology and formulae are never disclosed.

A7.3 Service providers acting on our behalf (Data Processors). We use service providers who process data on our instructions, including providers of cloud email, storage and productivity services; messaging and social-media platforms (WhatsApp Business, Instagram and Facebook); server hosting located in India; secure private networking; software and configuration hosting; automated and artificial-intelligence-assisted processing services, some of which are located outside India (Clause A8); our chartered accountant; legal advisers; and NABL-accredited testing laboratories. Samples sent to laboratories are labelled with the supplier Code and lot reference only. We engage these providers under contract, including on the provider's standard data-processing terms where applicable, and they must keep the data confidential and protect it with reasonable security safeguards.

A7.4 Authorities and the export chain. We disclose the minimum personal data necessary to customs (including ICEGATE), the Directorate General of Foreign Trade, GST and income-tax authorities, the Reserve Bank of India and authorised dealer banks, FSSAI, APEDA, the Spices Board, plant-quarantine and export-inspection authorities, destination-country authorities, shipping lines, airlines, freight forwarders, customs brokers, inspection agencies, insurers, the Export Credit Guarantee Corporation of India and banks handling letters of credit. **Regulatory carve-out:** where the law of India or of a destination country, or a competent authority, requires the identity of a manufacturer, processor, packer or farm (for example, food-facility registration, prior notice of imported food, registration of overseas manufacturers, establishment approvals, or phytosanitary, origin or organic certificates), we disclose only the fields so required, to the authority and to the persons who must handle the document with the goods. We inform the supplier in advance where practicable.

A7.5 Legal process and protection of rights. We may disclose personal data where required by law or by an order of a court, tribunal or authority; to establish, exercise or defend legal claims; and, under obligations of confidentiality, to a successor entity in connection with a lawful conversion, reorganisation, merger or transfer of Anica's business.

A8. AUTOMATED AND AI-ASSISTED PROCESSING — HUMAN VERIFICATION

A8.1 What we do. Anica operates an internal business-management platform, ANICA.AI, which uses automated tools, including artificial-intelligence-assisted tools, to capture, classify, index, search, summarise and translate communications and documents, and to prepare drafts for human review. Some of these tools run on our own equipment in India; others are provided by third-party service providers located inside or outside India.

A8.2 Human verification. No message is sent to a Counterparty, no price is quoted, no audit finding or rating is finalised, and no decision to onboard, suspend or terminate a Counterparty is taken, without review and approval by a Designated Partner of Anica. We do not take decisions that produce legal or similarly significant effects for an individual solely by automated means.

A8.3 Provider terms. We use externally hosted AI services only on commercial terms under which, according to the provider's published terms, the data we submit is not used to train the provider's general-purpose models.

A9. YOUR RIGHTS AND DUTIES

A9.1 Rights. Subject to the DPDP Act and the rules made under it, a Data Principal has the right to:

- (a) obtain a summary of the personal data we process and the processing activities undertaken, and the identities of other Data Fiduciaries and Data Processors with whom it has been shared, together with a description of the data shared (Section 11);
- (b) have inaccurate or misleading personal data corrected, incomplete personal data completed, and personal data updated (Section 12);
- (c) have personal data erased when it is no longer necessary for the specified purpose, unless its retention is necessary for compliance with law (Section 12);
- (d) withdraw consent at any time, with the same ease with which it was given (Section 6(4));

(e) have a grievance redressed by our Grievance Officer (Section 13) and, after exhausting that remedy, complain to the Data Protection Board of India (Section 13(3)); and

(f) nominate another individual to exercise these rights in the event of death or incapacity (Section 14).

A9.2 Duties. Under Section 15 of the DPDP Act, a Data Principal must comply with applicable law, must not impersonate another person, must not suppress material information or furnish false particulars (including in KYC documents), must not register a false or frivolous grievance or complaint, and must furnish only verifiably authentic information when seeking correction or erasure. A breach of these duties may attract a penalty under the DPDP Act.

A9.3 Consequences of withdrawal or erasure. Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal. After withdrawal, we will stop processing for purposes that depend on consent within a reasonable time, and we will cause our Data Processors to do the same. Because verified KYC is a precondition to every engagement (Clause B3.1), withdrawal of consent or erasure of KYC data may require us to suspend or end the engagement. Personal data that we must retain under law (Clause A10) will continue to be retained for the period so required.

A9.4 How to exercise rights. Write to the Grievance Officer (Clause A18) from the email address or WhatsApp number registered with us, with the subject line “DATA REQUEST”. We may take reasonable steps to verify identity before acting.

A10. DATA RETENTION

OPERATIONAL REALITY & LEGAL SHIELD: STATUTORY RETENTION PREVAILS OVER ERASURE REQUESTS

Trade, tax, customs, foreign-exchange and quality records must be kept for years after a shipment. We keep them for the periods below and no longer. After that they are erased or irreversibly anonymised.

Record type	Retention period
Enquiries and contacts that do not lead to an engagement	3 years from the last communication
KYC records, contracts, quotations, purchase and sale records, shipping and customs documents, invoices, payment and export-realisation records, tax records, audit reports and dossiers, laboratory reports and CAPA records (including audit photographs and recordings, which may be reduced to evidential extracts)	8 years from the end of the financial year in which the relationship ended or the last transaction or audit took place, whichever is later. This covers the retention requirements of the Limited Liability Partnership Act, 2008, the Central Goods and Services Tax Act, 2017, the Income-tax Act, 2025, and customs and foreign-exchange requirements
Records relevant to a pending assessment, audit, investigation, recall, claim, arbitration or litigation	Until final resolution (including any appeal), and then the applicable period above
System, access and processing logs	Not less than one year (DPDP Rules, 2025), and in any event not less than 180 days in India where required by the CERT-In Directions of 28 April 2022
Business-update (marketing) contact list	Until opt-out; a minimal suppression record is kept so that we can honour the opt-out

On expiry, records are erased or irreversibly anonymised. Encrypted backups are overwritten in the ordinary course of the backup rotation cycle.

A11. SECURITY SAFEGUARDS AND PERSONAL DATA BREACHES

A11.1 Safeguards. We maintain reasonable security safeguards appropriate to the nature of the data and the size of our organisation, including:

- (a) access to personal data restricted to Anica's Designated Partners and to persons with a need to know (such as our chartered accountant) who are bound by confidentiality;
- (b) internal systems reachable only over a private, encrypted network, and not exposed to the public internet except where an external platform integration strictly requires it;
- (c) two-step verification on business email and messaging accounts;
- (d) encrypted backups of our databases;
- (e) separate logs of automated actions and of human approval decisions;
- (f) masking of Aadhaar, pseudonymisation through Codes, and redaction before external sharing; and
- (g) contractual confidentiality and security obligations on Data Processors.

A11.2 No absolute guarantee. No method of electronic storage or transmission is completely secure. We therefore do not represent that personal data can never be accessed without authorisation, but we commit to maintaining the safeguards above and to reviewing them periodically.

A11.3 Breach response. If a personal data breach occurs, we will act promptly to contain it. We will intimate each affected Data Principal, and intimate the Data Protection Board of India without delay and furnish a detailed report within seventy-two hours of becoming aware of the breach (or such longer period as the Board may allow), as required by the DPDP Rules, 2025. Where an incident is reportable to the Indian Computer Emergency Response Team (CERT-In), we will report it within six hours of noticing it, in accordance with the CERT-In Directions of 28 April 2022.

A12. TRANSFERS OF PERSONAL DATA OUTSIDE INDIA

International trade requires personal data to cross borders: to buyers, destination authorities, shipping lines and banks abroad, and to service providers whose infrastructure is located outside India. Under Section 16 of the DPDP Act, we transfer personal data outside India except to any country or territory that the Central Government has restricted by notification, and we will comply with any such restriction. Where a foreign law requires additional safeguards for data we receive from that jurisdiction, we will put them in place (Clause A15).

A13. RETAIL AND DIRECT-TO-CONSUMER CUSTOMERS

Anica currently operates on a business-to-business basis. If and when Anica commences retail or direct-to-consumer sales, this Part A will apply to customers' personal data (name, delivery address, telephone number, email address, order and payment records), together with a supplementary notice presented at the point of order. Consumer orders will be processed only with the consent required by law, and any grievance mechanisms required by the Consumer Protection Act, 2019 and the rules made under it will be provided. We will not knowingly accept orders from, or process the personal data of, a child except with verifiable consent of the parent or lawful guardian as required by Section 9 of the DPDP Act.

A14. BUSINESS UPDATES AND MARKETING

We send business updates, product bulletins and market highlights only to persons who have opted in or who, as existing business contacts, have been given a clear opportunity to opt out. Every such message contains a simple way to unsubscribe (for WhatsApp, a reply of "STOP"), and opt-outs are honoured promptly. Transactional messages about an ongoing enquiry, audit, order or shipment are not marketing and will continue while the engagement lasts.

A15. COUNTERPARTIES OUTSIDE INDIA

A15.1 European Union and United Kingdom. Where the EU General Data Protection Regulation or the UK GDPR applies to our processing, Anica Foods LLP is the controller; we rely on the performance of a contract (Article 6(1)(b)), compliance with a legal obligation (Article 6(1)(c)), our legitimate interests in operating a verified B2B supply chain, preventing fraud and assuring quality (Article 6(1)(f)), and consent for marketing (Article 6(1)(a)). Data subjects have the rights of access, rectification, erasure, restriction, portability and objection, the right to withdraw consent and the right to lodge a complaint with their supervisory authority. Where we receive personal data from the EU or UK, transfers to India rely on an appropriate transfer mechanism (such as the European Commission's Standard Contractual Clauses or the UK International Data Transfer Addendum) or, for occasional transfers, on a derogation permitted by law.

A15.2 United States and Canada. We will honour access and correction requests from business contacts in these jurisdictions, and we will comply with any federal, state or provincial privacy law to the extent it applies to us.

A15.3 Gulf Cooperation Council and Middle East. We will comply with the data-protection laws of the United Arab Emirates, the Kingdom of Saudi Arabia and other GCC states to the extent they apply to our processing.

A15.4 Asia-Pacific. We will comply with the Personal Information Protection Law of the People's Republic of China, Japan's Act on the Protection of Personal Information and other Asia-Pacific laws to the extent they apply to our processing.

A15.5 Higher standard prevails. Where a foreign law that mandatorily applies grants an individual greater rights than this notice, we will honour those rights.

A16. WEBSITE AND COOKIES

indianshroom.com currently uses no analytics, advertising or tracking cookies. Only strictly necessary technical cookies and server logs, if any, are used by our hosting provider to deliver and secure the website. Enquiries submitted through the website form are routed to our internal communication system and handled under this notice. If we introduce analytics or similar technologies, we will update this notice and, where the law requires, seek consent before placing them.

A17. LANGUAGE OF THIS NOTICE

This Policy is issued in English, and the English text prevails. On request, we will provide a summary of this Part A in Telugu or Hindi, and, within a reasonable time, in any other language specified in the Eighth Schedule to the Constitution of India, as contemplated by Section 5(3) of the DPDP Act.

A18. GRIEVANCE OFFICER AND CONTACT FOR DATA QUESTIONS

Grievance Officer	Mr. Cassian Mario John, Designated Partner. He is also the person able to answer questions about the processing of personal data (Section 8(9) of the DPDP Act; Rule 5(9) of the SPDI Rules)
Entity	Anica Foods LLP (Export Brand: Indian Shroom Company)
Address	Hyderabad, Telangana – 500034, Republic of India
Email	founder@indianshroom.com (subject line: "DATA REQUEST" or "GRIEVANCE")
Telephone / WhatsApp	+91 63047 48642
Response timelines	Acknowledgement within 3 business days; resolution within one month of receipt of a complete request, and in any event within the period prescribed under the DPDP Rules, 2025
Escalation	If a grievance is not resolved, the Data Principal may complain to the Data Protection Board of India. Individuals protected by the GDPR or UK GDPR may complain to their supervisory authority.

A19. CHANGES TO THIS NOTICE

We will update this Part A when the law, our operations or our service providers change. The current version, with its reference number and effective date, is available on request and on indianshroom.com. We notify active Counterparties of material changes by email or WhatsApp. Where a change requires fresh consent, we will seek it and will not rely on continued interaction alone.

PART B — COMMERCIAL DATA, CONFIDENTIALITY & NON-CIRCUMVENTION TERMS

OPERATIONAL REALITY & LEGAL SHIELD: BINDING COMMERCIAL TERMS WITHOUT A MANDATORY MoU OR NC-NDA

Anica does not require an MoU or NC-NDA for enquiries, samples, KYC, audits or single consignments. Instead, these Part B terms travel with every Annex 1 acceptance, quotation, proforma invoice, purchase order, sales contract, audit booking and consultancy engagement. They protect our network, our audit intellectual property and our codes.

B1. APPLICATION AND ACCEPTANCE

B1.1 Acceptance. This Part B binds a Counterparty from the earliest of: (a) its written acceptance of Annex 1, including a reply stating “I ACCEPT AFLLP/LEG/POL/2026-V2.0” sent by email or WhatsApp from its registered address or number, which constitutes a valid electronic contract under Section 10A of the Information Technology Act, 2000; (b) its acceptance of, or performance under, any quotation, proforma invoice, purchase order, sales contract, audit booking or consultancy engagement that incorporates this Policy by reference; or (c) its receipt of any Highlights, Audit Output or Anica Network Information after having been notified that such receipt is subject to this Part B.

B1.2 No browse-wrap. Visiting indianshroom.com, without more, does not bind any person to this Part B.

B1.3 Order of precedence. In case of conflict, the following prevail in descending order: (i) a signed Master Multi-Shipment Supply Agreement, MoU or NC-NDA; (ii) the specific sales contract, purchase order or proforma invoice; (iii) this Part B; (iv) Part A. Nothing in this Part B limits any statutory right of an individual under data-protection law.

B2. DEFINITIONS

- (a) “**Counterparty**” means any supplier, farmer, FPO, processor, vendor, service provider, buyer, importer, distributor, audit client or consultancy client that deals with Anica, together with its affiliates, officers, employees and agents.
- (b) “**Anica Network Information**” means the identity, location, contact details, capabilities, prices or terms of any supplier, buyer, vendor or service provider that are disclosed by Anica, made identifiable through Anica, or linked to a Code.
- (c) “**Confidential Information**” means all non-public information disclosed by or on behalf of Anica, including Anica Network Information, Codes, Highlights, Audit Output, specifications, prices, costings, lab results and Derived Insights, whether disclosed orally, in writing or electronically, and whether or not marked confidential.
- (d) “**Highlights**” means code-indexed summaries, quality parameters, scores, grades and redacted audit dossiers provided by Anica.
- (e) “**Audit Output**” means all audit plans, checklists, instruments, questionnaires, evidence compilations, findings, nonconformity registers, reports, dossiers, scores and grades created by or for Anica, and Anica’s proprietary quality-rating framework, methodology and formulae.
- (f) “**Derived Insights**” means aggregated and anonymised analyses, benchmarks, market intelligence and publications that Anica creates from its information.
- (g) “**Restricted Period**” means the period of the Counterparty’s engagement with Anica and twenty-four (24) months after the later of (i) the last disclosure of Anica Network Information to the Counterparty, and (ii) the Counterparty’s last transaction with Anica.
- (h) “**Diverted Business**” means any purchase, sale, supply, service or other transaction concluded in breach of Clause B6.

B3. KYC, WARRANTIES AND SCREENING

OPERATIONAL REALITY & LEGAL SHIELD: MANDATORY COUNTERPARTY KYC — NO UNVERIFIED ONBOARDING

Complete and truthful KYC is a condition precedent to every firm quotation, sample dispatch, audit, purchase order and consignment. False KYC shifts the resulting loss onto the party that supplied it.

B3.1 Condition precedent. Submission of complete, authentic and current KYC documentation, and its verification by Anica, is a condition precedent to (i) any firm quotation, (ii) dispatch of commercial samples, (iii) scheduling of a second-party audit, (iv) issue of a purchase order, and (v) acceptance of a consignment. Anica may refuse, suspend or end any engagement, without liability, where KYC is incomplete, unverifiable, outdated or adverse.

B3.2 Warranties. The Counterparty warrants that all documents, declarations and information it provides are genuine, accurate, complete and duly authorised, and that it will notify Anica of any material change within seven (7) days.

B3.3 Verification and screening. The Counterparty authorises Anica to verify its information with government registers (including GSTN, MCA, DGFT/IEC, FSSAI, APEDA and the Spices Board), to screen it against sanctions and denied-party lists (including those of the United Nations, the United States, the European Union, the United Kingdom and India), to obtain credit reports, credit-insurance limits and bank references, and to search litigation records and adverse media.

B3.4 Voluntary compliance posture. Anica is not a reporting entity under the Prevention of Money-laundering Act, 2002. It conducts KYC and sanctions screening voluntarily, as a matter of commercial prudence and to protect its supply chain.

B3.5 Personal data supplied by Counterparties. Where a Counterparty provides Anica with personal data of its own personnel, farmers, sub-suppliers or any other individual (including a client naming a supplier for a commissioned audit), the Counterparty warrants that it is entitled to do so, and that it has given those individuals any notice and obtained any consent that the law requires.

B4. SECOND-PARTY AUDITS

OPERATIONAL REALITY & LEGAL SHIELD: ISO 19011-BASED SECOND-PARTY AUDITS AS ANICA'S PROPRIETARY USP

Our audit programme is our unique selling proposition as a merchant-exporter. Audit Output and the quality-rating framework belong to Anica. Findings are honest professional opinions on sampled evidence at a point in time, and auditees are given a fair right of reply.

B4.1 Standard and status. Anica conducts second-party audits in accordance with the guidelines of ISO 19011:2026, using audit criteria drawn from applicable requirements, which may include the Codex Alimentarius General Principles of Food Hygiene and HACCP, good agricultural, hygiene and manufacturing practices, FSSAI and APEDA requirements, buyer specifications and destination-market requirements. Anica is not a certification body or an accredited inspection body. Its audits do not result in certification, and Anica makes no claim to accreditation.

B4.2 Cadence. Unless otherwise agreed, the audit programme comprises an annual on-site physical audit, quarterly remote surveillance audits, and lot-specific sampling for testing by NABL-accredited laboratories.

B4.3 Auditee obligations and site media. The auditee shall provide safe access, records and personnel reasonably required. The auditee consents to Anica taking photographs and video and audio recordings of premises, equipment and processes, and to the recording of remote audit sessions, which will be announced at the start of each session. The auditee shall inform its personnel that such media may be captured and shall identify any area where photography is prohibited for safety or legal reasons. Anica blurs faces before any external sharing, does not photograph minors, and keeps farm GPS coordinates internal and never shares them, including in redacted dossiers.

B4.4 Ownership of Audit Output. All Audit Output, and all copyright, database rights, trade secrets and other intellectual property in it, including compilations protected under the Copyright Act, 1957, vest in and remain with Anica. The auditee retains ownership of its own pre-existing documents and information. It grants Anica a non-exclusive, perpetual, royalty-free licence to use them for the purposes set out in this Policy, including audit, rating, Highlights, dossiers, regulatory disclosure and the defence of claims. No auditee, buyer or other person acquires any right, title or licence in Audit Output except as expressly granted in writing.

B4.5 Disclosure to the auditee and right of reply. The auditee will receive its findings, classified as Major Nonconformity, Minor Nonconformity, Observation or Opportunity for Improvement, together with its final score or grade. Anica's rating methodology and formulae are trade secrets and will not be disclosed. The auditee may submit a written response or CAPA plan within fourteen (14) days of receiving the findings. Any response received within that time will be attached to every Highlight or dossier concerning that audit that is subsequently shared. Anica may revise a score on receipt of verified new evidence.

B4.6 Sharing of results. Results are shared only as described in Clauses A7.1 and A7.2: redacted and code-indexed for buyers, and as a full named report for a client that has commissioned an audit of a supplier it has named, with that supplier's prior written consent.

B4.7 Nature of findings and disclaimer. Audit findings, scores and grades are professional opinions, formed in good faith on the basis of sampled evidence at the time of the audit. They are not a warranty or guarantee of any product, lot or facility, a certification, or a form of insurance. Passing an audit creates no obligation on Anica to purchase any product or to enter into any agreement. Anica shall have no liability to an auditee for any loss of business, reputation or opportunity arising from a finding, score, suspension or disqualification made in good faith under this Clause B4. Audit Output may be relied upon only by the person to whom Anica issues it, and only for the purpose for which it is issued.

B4.8 Liability for goods sold. Where Anica sells goods as principal, its liability for those goods is governed exclusively by the sales contract for those goods. An audit carried out before such a sale does not enlarge that liability.

B5. CODES, HIGHLIGHTS AND CONFIDENTIALITY

B5.1 No de-anonymisation. The Counterparty shall not, directly or indirectly, attempt to decode, reverse-engineer, trace or identify the person behind any Code or redacted dossier, including by using labels, lot numbers, packaging marks, metadata, shipping documents, laboratory references or enquiries to third parties.

B5.2 Confidentiality. The Counterparty shall keep all Confidential Information strictly confidential, use it solely for evaluating and performing its dealings with Anica, and disclose it only to its own employees and professional advisers who need to know it and who are bound by confidentiality obligations no less protective than these. The Counterparty is responsible for any breach by such persons.

B5.3 Exclusions. The obligations in Clause B5.2 do not apply to information that the Counterparty proves by contemporaneous written records (a) was lawfully in its possession before disclosure by Anica without restriction, (b) is or becomes public other than through its breach, or (c) was independently developed without use of Confidential Information. Disclosure compelled by law is permitted only to the minimum extent required, with prompt prior notice to Anica where lawful.

B5.4 Inadvertent disclosure. If the Counterparty receives the identity behind a Code by mistake or through any regulatory document described in Clause A7.4, it shall treat that identity as Confidential Information and Anica Network Information, shall not use it for any purpose other than the transaction concerned, and shall notify Anica.

B5.5 Duration. Confidentiality obligations survive for five (5) years after the end of the engagement, and indefinitely for Anica's rating methodology, formulae and other trade secrets.

B6. NON-CIRCUMVENTION AND NON-SOLICITATION

OPERATIONAL REALITY & LEGAL SHIELD: ANTI-DISINTERMEDIATION PROTECTION

A Counterparty that learns of a supplier or buyer through Anica may not bypass Anica to deal with that party during the Restricted Period. This protects Anica's Confidential Information and its investment in audit and verification. It does not stop anyone from trading generally.

B6.1 Covenant. During the Restricted Period, the Counterparty shall not, directly or indirectly (including through any affiliate, agent, broker, freight forwarder, customs broker or other intermediary), solicit, negotiate or transact with any person whose identity, capability or terms it first learned from, or could identify only through, Anica Network Information, in respect of the same or substitutable products or services, otherwise than through Anica. It shall also not induce any such person to reduce or terminate its dealings with Anica.

B6.2 Exceptions. Clause B6.1 does not apply where (a) the Counterparty proves, by documentary evidence dated before Anica's disclosure and notified to Anica within seven (7) days of that disclosure, a pre-existing relationship with the person concerned; (b) the Counterparty proves by contemporaneous written evidence that it identified and dealt with that person independently of any Anica Network Information; or (c) Anica has given its prior written consent, which may be subject to commercial terms.

B6.3 Nature of the restriction. The parties acknowledge that this restriction is limited in duration and scope. It exists to protect Anica's Confidential Information, goodwill and investment in audit and verification, and it does not restrain the Counterparty from carrying on any lawful trade with persons it has not identified through Anica.

B6.4 Anica's freedom. Nothing in this Part B restricts Anica from dealing with any person in any market.

B7. REMEDIES FOR BREACH

B7.1 Interim relief. A breach of Clauses B5 or B6 may cause Anica harm that damages alone cannot adequately remedy. Anica may seek interim or injunctive relief from an emergency arbitrator under Clause B13 or from a competent court under Section 9 of the Arbitration and Conciliation Act, 1996. The Counterparty agrees not to oppose such relief on the ground that damages would be an adequate remedy.

B7.2 Liquidated damages. For each breach of Clause B6, the Counterparty shall pay Anica, as liquidated damages, fifteen percent (15%) of the gross value of all Diverted Business concluded during the Restricted Period. The parties agree that this amount is a genuine pre-estimate of Anica's likely loss of margin and of the unrecovered cost of sourcing, onboarding, auditing and verifying the counterpart concerned. Such loss is difficult to quantify precisely, and the amount constitutes reasonable compensation within the meaning of Section 74 of the Indian Contract Act, 1872.

B7.3 Account. On Anica's reasonable written request in connection with a suspected breach of Clause B6, the Counterparty shall within thirty (30) days furnish a true account, supported by documents, of its dealings with the person concerned during the Restricted Period.

B7.4 Other remedies and costs. These remedies are in addition to any other remedy available at law, including damages for breach of Clause B5, provided that there is no double recovery for the same loss. The Counterparty shall bear the reasonable costs of enforcement, including legal fees, as determined by the arbitral tribunal or court.

B8. DATABASE SOVEREIGNTY AND DERIVED INSIGHTS

OPERATIONAL REALITY & LEGAL SHIELD: NO DATABASE SHARING — INSIGHTS ONLY

We do not share our database or knowledge base with any company, individual or firm. We do share insights and highlights derived from our information, which are aggregated so that no individual source can be identified.

B8.1 No sale or access. Anica does not sell, rent, lease, license, trade or give access to its databases, contact registers, audit archives, pricing models or knowledge base to any person, except to Data Processors acting on its instructions, as required by law, or as described in Clause A7.

B8.2 Anonymisation standard. Derived Insights are compiled only from aggregated, anonymised data. No figure is published unless it is drawn from at least three (3) unrelated sources and no single source accounts for more than sixty percent (60%) of it. Locations are not disclosed at a level of detail that would identify a source.

B8.3 Ownership and permitted use. All intellectual property in Derived Insights belongs to Anica. A recipient receives a limited, non-exclusive, non-transferable and revocable right to use Derived Insights for its own internal business purposes only, and shall not publish, resell or redistribute them without Anica's written consent.

B8.4 No reliance. Highlights and Derived Insights (including crop calendars, market intelligence, price trends and quality summaries) are provided for information only, "as is" and "as available". Anica gives no warranty as to their accuracy, completeness or fitness for any purpose. Recipients must make their own independent verification before acting on them.

B9. LIMITATION OF LIABILITY

OPERATIONAL REALITY & LEGAL SHIELD: LIABILITY LIMITED TO THE VALUE OF THE TRANSACTION

Anica's aggregate liability is limited to the value it actually received for the specific consignment, audit or service in question. Information provided free of charge carries no liability except for fraud or wilful misconduct.

B9.1 Excluded losses. To the maximum extent permitted by law, Anica shall not be liable for any indirect, incidental, special or consequential loss, or for loss of profit, revenue, business opportunity, contract or goodwill, however arising. This includes loss arising from transit deterioration, natural weight or moisture variation, shipping delays, container roll-overs, port congestion, customs delays, demurrage, detention or cold-chain failures caused by third parties.

B9.2 Cap. Anica's total aggregate liability for all claims arising out of or in connection with a consignment, audit, consultancy or other service, whether in contract, tort (including negligence), breach of statutory duty or otherwise, shall not exceed the price or fee actually received by Anica for that specific consignment, audit or service.

B9.3 Free information. In respect of Highlights, Derived Insights, website content and other information provided free of charge, Anica shall have no liability except for fraud or wilful misconduct.

B9.4 Non-excludable liability. Nothing in this Policy excludes or limits liability for fraud or wilful misconduct, or any liability that cannot lawfully be excluded or limited, including the statutory rights of Data Principals and any penalty imposed by a competent authority.

B10. INDEMNITY BY COUNTERPARTIES

The Counterparty shall indemnify and hold harmless Anica, its Designated Partners, employees and agents against all losses, penalties, fines, demurrage, costs and reasonable legal fees arising from: (i) any false, forged, misleading or outdated KYC information; (ii) any breach of Clauses B5 or B6; (iii) any unauthorised disclosure of Confidential Information; (iv) any failure of goods supplied by the Counterparty to comply with applicable food-safety, pesticide-residue (MRL), labelling, packaging or phytosanitary requirements; and (v) any breach of data-protection law in relation to personal data that the Counterparty supplied to Anica. Anica shall notify the Counterparty of any third-party claim within a reasonable time and shall not settle it without consulting the Counterparty, provided that the Counterparty acts promptly.

B11. CONTRACTUAL INDEPENDENCE AND NON-MANDATORY MoU / NC-NDA

OPERATIONAL REALITY & LEGAL SHIELD: PRINCIPAL-TO-PRINCIPAL MERCHANT-EXPORTER

Anica deals on a principal-to-principal basis. MoUs and NC-NDAs are signed only for committed, multi-shipment contracts. Every other dealing is governed by our commercial documents and this Part B.

B11.1 Principal-to-principal. Anica deals as an independent merchant-exporter on a principal-to-principal basis. Nothing in this Policy or in any enquiry, sample, audit, quotation or information exchange creates a partnership, joint venture, agency, fiduciary relationship, employment or exclusivity.

B11.2 MoU and NC-NDA not mandatory. Anica does not require or sign an MoU, letter of intent or bilateral NC-NDA for enquiries, catalogue or price requests, samples, sensory or technical evaluation, KYC, audits, or single or occasional consignments. These are governed by Anica's quotation, proforma invoice, purchase order or sales contract together with this Part B.

B11.3 Multi-shipment contracts. An MoU or bilateral NC-NDA is executed, at Anica's discretion, only where Anica and a Counterparty enter into a committed contract for multiple shipments or consignments, typically recurring over six (6) months or more and supported by appropriate payment security. No Counterparty may assert the existence of such an agreement unless it has been signed by a Designated Partner of Anica.

B11.4 Non-exclusivity. Unless a signed agreement expressly provides otherwise, Anica may source from and sell to any competing party in any territory, and may decline further business after any consignment without liability.

B12. FORCE MAJEURE

Anica is not liable for any failure or delay caused by events beyond its reasonable control. These include natural disasters, crop failure and blight, epidemics, war, sanctions, embargoes, changes in export or import policy (including export bans, minimum export prices and tariff changes), port or transport strikes, container shortages, shipping-line insolvency, failure of power or telecommunication networks, and cyber-attacks that defeat

reasonable security safeguards. Anica will notify the affected Counterparty and take reasonable steps to mitigate the effect.

B13. GOVERNING LAW AND DISPUTE RESOLUTION

OPERATIONAL REALITY & LEGAL SHIELD: INSTITUTIONAL ARBITRATION SEATED IN HYDERABAD

Commercial disputes are resolved by a sole arbitrator under the rules of the International Arbitration and Mediation Centre, Hyderabad. Statutory data-protection complaints by individuals remain with the Data Protection Board of India.

B13.1 Governing law. This Policy and all non-contractual obligations arising from it are governed by the laws of India. The United Nations Convention on Contracts for the International Sale of Goods does not apply.

B13.2 Arbitration. Any dispute arising out of or in connection with Part B or any commercial dealing to which it applies, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration administered by the International Arbitration and Mediation Centre, Hyderabad ("IAMC"), under the IAMC arbitration rules in force at the time of commencement (the International Arbitration Rules where the dispute is an international commercial arbitration). The tribunal shall consist of a sole arbitrator appointed in accordance with those rules. The seat and venue of arbitration shall be Hyderabad, Telangana, India, and the language shall be English. The award shall be final and binding and may be enforced in any jurisdiction, including under the New York Convention.

B13.3 Courts. Subject to Clause B13.2, the courts at Hyderabad, including the High Court for the State of Telangana, shall have exclusive supervisory jurisdiction, including over applications for interim measures under Section 9 of the Arbitration and Conciliation Act, 1996. Anica may also seek interim relief or enforcement in any court where the Counterparty or its assets are located.

B13.4 Statutory complaints preserved. Nothing in this Clause B13 prevents an individual from exercising statutory rights before the Data Protection Board of India or any other competent regulator.

B14. GENERAL PROVISIONS

B14.1 Amendments. Anica may amend this Policy by publishing a new version with a new reference number. Amendments to Part B apply to engagements, transactions and disclosures after the Counterparty has been notified of them, and not to concluded transactions without the Counterparty's consent.

B14.2 Severability. If any provision is held invalid or unenforceable, it shall be read down to the maximum extent enforceable, and the remaining provisions shall continue in full force.

B14.3 Survival. Clauses B4.4, B4.7, B5, B6, B7, B8, B9, B10 and B13 survive the completion or termination of any engagement for the periods stated or, where no period is stated, for as long as necessary to give them effect.

B14.4 Electronic records. This Policy, Annex 1 acceptances and related communications are electronic records under the Information Technology Act, 2000. Acceptance by email or WhatsApp in accordance with Clause B1.1 is valid and binding.

B14.5 Assignment and waiver. Anica may assign its rights under this Part B to a successor to its business. No failure or delay in exercising any right operates as a waiver of it.

B14.6 Notices. Notices to Anica shall be sent to founder@indianshroom.com. Notices to a Counterparty may be sent to its registered email address or WhatsApp number.

SCHEDULE 1 — ITEMISED PERSONAL DATA INVENTORY

This Schedule forms part of the notice in Part A. "S." refers to a section of the DPDP Act, 2023. Retention periods are as described in Clause A10.

Data Principal	Personal data	Specified purposes	Legal basis	Retention
Enquirers; website and social-media contacts	Name, company, email, telephone/WhatsApp, country, product interest, quality grade, message	Respond, quote, send samples, follow up	S.7(a); consent	3 years from last contact if no engagement
Individual farmers, FPO members and sole-proprietor suppliers	Identity and contact; KYC documents (masked Aadhaar only if volunteered); registrations; bank details; farm location and GPS; certifications; test reports	KYC, audits, procurement, payment, traceability, regulatory compliance	Consent; S.7(a), (d), (e); SPDI written consent (bank details)	8 years after FY of last transaction or audit
Personnel of processors, vendors and service providers	Name, designation, contact; signatory ID and authority; bank details where an individual	Contracting, coordination, payment, compliance	Consent; S.7(a)	8 years after FY of last transaction
Personnel of buyers, importers and distributors	Name, designation, contact; signatory ID; screening and credit results; trade and payment records	Quotations, contracts, export documents, realisation, credit and sanctions checks	Consent; S.7(a), (d); Clause A15 bases	8 years after FY of last transaction
Individuals at audited sites	Images, video and audio incidentally captured; interview notes; names and roles of interviewees; compliance status of hygiene and training records (no medical records copied)	Audit evidence, findings, CAPA follow-up	Consent (via auditee notice, Clause B4.3); S.7(a)	With the audit record: 8 years; faces blurred for any external use
Commissioned-audit and consultancy clients	Contact, signatory ID, billing and project data	Service delivery, reporting, invoicing	Consent; S.7(a)	8 years after FY of last service
Business-update recipients	Name, email or WhatsApp number, preferences	Business updates and bulletins	Consent (opt-in)	Until opt-out; minimal suppression record
All users of our systems and channels	Access, IP and processing logs	Security, audit trail, incident response	Legal obligation; S.7(d)	Not less than 1 year
Retail customers (future, Clause A13)	Name, delivery address, telephone, email, order and payment records	Order fulfilment, grievances, legal compliance	Consent; S.7(a)	8 years after FY of order (tax records)