TaxQue

ARB FinTech LLP | taxque.in

Privacy Policy

DOCUMENT ID	TQ-PP
VERSION	1.1
EFFECTIVE DATE	20 June 2026
SUPERSEDES	-
SUPERSEDED	09 August 2026
STATUS	ARCHIVED - superseded
CONTENT SHA-256	0cfc5f9fdbb3a7901768d102524f1112641b21efc39b5f51b3417ed655dd290b

SUMMARY OF CHANGE

Complete rewrite for compliance with the Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025, replacing the general policy carried over from the previous site. Adds an itemised data/purpose register; explicit Aadhaar-handling terms (no authentication performed by us, OTP entered by the client, masked storage); formal disclosure of sharing with Associate Professionals as a core, consented feature of the service; PMLA reporting-entity obligations where applicable; a statutory retention schedule by record category; DPDP breach-notification timelines (Board and Data Principals, plus CERT-In); and expanded Data Principal rights including nomination. Introduces new purposes of processing and new categories of recipient (Associate Professionals; additional named data processors), and is recorded as a material change accordingly.

TaxQue - a trademarked brand of **ARB FinTech LLP**

Document Control

Document ID | TQ-PP

Version | 1.1

Effective Date | 20 June, 2026

Last Updated | 09 Aug, 2026

Status | Public - published on Platform

Supersedes | Privacy Policy dated 20 January, 2025

Review Cycle | Annually, or on material change in law

Owner | Grievance Officer, ARB FinTech LLP

ARB FinTech LLP · LLPIN ABC-5112 · GSTIN 10ABZFA6377J1ZX
Registered Office: KH No. 1508, Village Lemuwari, Ward No. 08, Block Patepur, District Vaishali, Bihar - 843114, India
Branch Office: Surbhi Vihar, Mithapur, Patna, Bihar - 800001, India
Contact:info@taxque.in · +91 93112 56088 · https://www.taxque.in

---

PART A - PRELIMINARY

1. About Us and Scope of this Policy

1.1 This Privacy Policy ("**Policy**") is issued by **ARB FinTech LLP**, a limited liability partnership incorporated under the Limited Liability Partnership Act, 2008, operating under the trademarked brand **"TaxQue"** ("**TaxQue**", "**we**", "**our**", "**us**").

Registered Office | KH No. 1508, Village - Lemuwari, Ward No. - 08, Block - Patepur, District - Vaishali, Bihar - 843114, India

Branch / Correspondence Office | Surbhi Vihar, Mithapur, Patna, Bihar - 800001, India

LLP Identification Number (LLPIN) | ABC-5112

GSTIN | 10ABZFA6377J1ZX

Website | https://www.taxque.in

Email | info@taxque.in

Telephone | +91 93112 56088

1.2 **The TaxQue brand.** "TaxQue" is a registered trade mark used by ARB FinTech LLP under authority of its proprietor. All services described in this Policy are provided by, and all data-protection obligations under this Policy are owed by, **ARB FinTech LLP**. Rights in the mark are governed by our Terms of Service; nothing in this Policy grants you any licence or right to use it.

1.3 **What we do.** TaxQue is a service-delivery and technology platform for accounting, bookkeeping, business and entity registration, taxation, and statutory compliance services. We coordinate and deliver these services through a network of independent practising professionals and firms (defined below as **Associate Professionals**).

1.4 **Scope.** This Policy governs all personal data we collect through our website, mobile applications, web portals, WhatsApp and telephonic channels, physical intake at either office, and any other means (collectively, the "**Platform**"), whether you are a prospective, current, or former client.

1.5 **Statutory framework.** This Policy is issued under and is to be read with:

- the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") and the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**");
- the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**");
- the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and rules and regulations thereunder;
- the Central Goods and Services Tax Act, 2017, the Income-tax Act, 1961, the Companies Act, 2013, and the Limited Liability Partnership Act, 2008;
- the Prevention of Money-Laundering Act, 2002 ("**PMLA**"), where applicable; and
- directions issued by the Indian Computer Emergency Response Team ("**CERT-In**").

1.6 **Transitional note.** The DPDP Rules were notified on 13 November 2025 with phased enforcement. The Data Protection Board of India is operational; penalty provisions commence 13 November 2026; and full substantive compliance is required by 13 May 2027. We are implementing the requirements of this Policy on a rolling basis ahead of those dates and will publish updates as each phase takes effect.

1.7 **Relationship to other documents.** This Policy addresses personal data. Commercial terms, scope of engagement, fees, professional disclaimers, and limitation of liability are governed by our **Terms of Service** and the **Engagement Letter** applicable to your service. Where there is conflict on a data-protection matter, this Policy prevails.

2. Definitions

"Associate Professional" - an independent practising Chartered Accountant, Company Secretary, Cost and Management Accountant, Advocate, GST Practitioner, e-Return Intermediary, tax consultant, or a firm or LLP of any of them, empanelled or engaged by us to execute all or part of your work.

"Data Principal" / **"you" -** the individual to whom the personal data relates; where the data relates to a child or a person with a disability with a lawful guardian, it includes the parent or lawful guardian.

"Personal Data" - any data about an individual who is identifiable by or in relation to such data.

"Processing" - any operation on personal data, including collection, storage, use, sharing, disclosure, erasure, or destruction.

"Secure Vault" - the partitioned, access-controlled document repository in which your uploaded and generated documents are stored in encrypted form on managed cloud infrastructure.

PART B - OUR ROLE AND YOUR CONSENT

3. Our Role: Data Fiduciary

3.1 In respect of personal data you provide to us, **ARB FinTech LLP is the Data Fiduciary**. We determine the purpose and means of processing.

3.2 **Associate Professionals process your data as our Data Processors.** They are engaged by us, act on our written instructions under contract with us, and **we are accountable to you for their processing.** You are not required to contact or pursue any Associate Professional. **Every request, question, or complaint about your data is to be brought to us**, and we will deal with it under Clauses 17 and 20.

3.3 **Statutory duties of practising professionals.** Where a professional signs or certifies a document in their own name, or discharges a duty placed on them personally by law (including under the Chartered Accountants Act, 1949, the Company Secretaries Act, 1980, the Cost and Works Accountants Act, 1959, the Advocates Act, 1961, or the PMLA), those duties arise by statute and exist alongside our obligations. They cannot be assumed by us by contract. **This does not reduce our accountability to you, and does not require you to approach anyone other than us.**

3.4 We will tell you, on request and at the point of assignment, which Associate Professional is handling your matter.

3.5 **Significant Data Fiduciary.** We have assessed, and will reassess annually, whether we meet the criteria for designation as a Significant Data Fiduciary. If designated, we will appoint an India-resident Data Protection Officer, conduct periodic Data Protection Impact Assessments and independent audits, and publish those particulars here.

4. Consent, Notice, and Withdrawal

4.1 **Separate notice.** Before we collect your personal data, we present a **standalone Consent Notice** setting out, in itemised form, the specific personal data to be collected, the specific purpose of each item, and the specific service enabled by it. That Notice is presented independently of this Policy, our Terms of Service, and any other document. **This Policy is not, by itself, your consent.**

4.2 **Granular consent.** Consent is sought purpose-by-purpose, and our Consent Notice distinguishes two classes:

(a) Core purposes - those without which the engaged service cannot lawfully or practically be delivered, including preparation and submission of your filings, sharing with the Associate Professional assigned to your matter (Clause 8), transmission to the relevant Government portal, and retention of statutory records. Declining a core purpose means we cannot accept the engagement.

(b) Optional purposes - including analytics cookies, promotional communications, and retention of your profile for future re-engagement. These may be declined or withdrawn individually at any time **without any effect on the service you have engaged**.

This separation exists so that withdrawal of an optional purpose can be given effect immediately and in isolation, without interrupting your filings.

4.3 **Language.** The Consent Notice is available in English and Hindi, and on request in any language listed in the Eighth Schedule to the Constitution of India.

4.4 **Withdrawal of consent.** You may withdraw consent at any time, wholly or for a specific purpose. **Withdrawal is as easy as giving consent.** You may withdraw:

- by email to **info@taxque.in** with the subject line "Withdrawal of Consent", stating which purpose or purposes you are withdrawing;
- by email to **info@taxque.in** with the subject line "Withdrawal of Consent"; or
- by written notice to either office address in Clause 1.1.

4.5 **Consequences of withdrawal.** Withdrawal is prospective. It does not affect the lawfulness of prior processing. Where the withdrawn data is essential to a service, we will be unable to continue that service and will tell you so before the withdrawal takes effect. Withdrawal does **not** entitle erasure of records we are required by law to retain (see Clause 12), and does not reverse filings already lodged with a government authority.

4.6 **What consent is not.** We do not treat continued use of the Platform, silence, pre-ticked boxes, or bundled acceptance of multiple documents as consent.

4.7 **Consent Managers.** Once Consent Manager registration opens under the DPDP Rules, you may route and manage your consent through a registered Consent Manager. We will publish details when we integrate with one.

PART C - DATA WE COLLECT AND WHY

5. Itemised Description of Personal Data and Purposes

We collect only what is necessary for the specific service you engage. The following is the itemised description required under Rule 3 of the DPDP Rules.

5.1 Identity and Contact Data

Data Item	Specific Purpose	Service Enabled
Full name, date of birth, gender	Identification on statutory filings and portal records	All services
Father's / spouse's name	Mandatory field in ITR, PAN, and MCA forms	Tax filing; entity registration
Residential and business address	Statutory address fields; place-of-supply determination	GST; ITR; MCA filings
Email address	Delivery of filings, acknowledgements, OTPs, deadline notices	All services
Mobile number (primary and alternate)	OTP-based portal authentication; filing confirmations	All services
Photograph / specimen signature	DSC issuance; MCA and PAN forms	Entity registration; DSC

5.2 Statutory and Government Identifiers

Data Item	Specific Purpose	Service Enabled
Permanent Account Number (PAN)	Mandatory identifier for income-tax filings and TDS	ITR; TDS; entity registration
GSTIN	Identification of the registered person on the GST Network	GST returns; reconciliation
TAN	Deductor identification for TDS returns	TDS filing
DIN / DPIN	Director/Designated Partner identification on MCA portal	Company & LLP compliance
CIN / LLPIN	Entity identification on MCA portal	ROC filings
Aadhaar number or Virtual ID	Stating the number in statutory forms where the form requires it. Authentication is performed by the Government portal with UIDAI, not by us	Only where legally required - see Clause 6
Passport, Voter ID, Driving Licence	Alternative identity and address proof for registration and DSC	Entity

registration; DSC

Digital Signature Certificate details	Affixing signature on statutory forms on your authorisation	MCA, GST, IT filings

5.3 Financial and Business Data

Data Item	Specific Purpose	Service Enabled
Bank account number, IFSC, cancelled cheque	Refund credit; bank-account validation on IT and GST portals	ITR; GST refunds
Bank statements	Preparation of books of account; reconciliation	Accounting; audit support
Sales and purchase invoices; e-way bills	Computation of output tax, input tax credit, and turnover	GST returns
Salary, TDS certificates (Form 16/16A), Form 26AS, AIS/TIS	Computation of taxable income and tax credits	ITR
Investment, insurance, loan, and donation proofs	Substantiating deductions and exemptions claimed	ITR
Capital-gains records; property documents	Computation of capital gains	ITR
Books of account, ledgers, trial balance	Preparation of financial statements	Accounting; ROC filings
Partnership deed, MOA, AOA, LLP agreement, board resolutions	Statutory filings and entity constitution records	Entity registration; ROC
Payment card / UPI / netbanking details	Collection of our professional fees	Billing

5.4 Third-Party Personal Data You Provide

Where you provide personal data of others - employees, directors, partners, dependants, vendors, customers, or deductees - **you warrant that you have the authority and the lawful basis to disclose it to us and to our Associate Professionals for the purposes in this Policy**, and you are responsible for issuing any notice or obtaining any consent those individuals are entitled to.

What we do on our side. This warranty allocates responsibility between you and us; it does not displace our own obligations under the DPDP Act, which we discharge independently. We process such data solely on your documented instruction and only for the engaged service; we apply the same security safeguards, retention limits, and access controls as to your own data; we do not use it for any other purpose; and if we become aware that data has been furnished without a lawful basis, we will stop processing it, tell you, and erase it unless a statutory obligation requires retention. An individual whose data you have furnished may exercise the rights in Clause 16 by writing to us, and we will act on the request and inform you.

5.5 Technical and Usage Data

Data Item	Specific Purpose
IP address, device identifier, browser and OS	Session security; fraud and intrusion detection; audit logging
Login timestamps, session and access logs	Security-incident detection, investigation, and remediation
Clickstream, page response times, navigation paths	Diagnosing and correcting Platform faults
Interface preferences (e.g. display mode)	Restoring your saved settings

5.6 Communications

Call recordings (where you are informed at the start of the call), WhatsApp and email correspondence, and support tickets - retained as the record of instructions received and advice given, and as evidence in the event of a dispute or professional inquiry.

5.7 Channels Through Which We Receive Your Data

We receive your documents and information through the following channels. Each is treated differently, and you may ask us to use one channel only.

Channel	How it is handled
Website / client portal upload	The primary and recommended channel. Files are transmitted over TLS 1.3 and

written to encrypted object storage (Cloudflare R2). This is the most secure route and we ask you to use it wherever possible.

Email to info@taxque.in | Attachments are downloaded to the Secure Vault and the source message is retained only as the record of your instruction. Email is not an encrypted medium end-to-end; please do not send Aadhaar, passwords, or portal credentials by email.

WhatsApp | Received only on the official TaxQue business number, never on a personal account. Messages are transmitted with WhatsApp's end-to-end encryption. Documents are transferred to the Secure Vault, deleted from the chat, and cleared from device storage by a scheduled purge. See Clause 11.7.

In person at either office | Physical documents are scanned to the Secure Vault; originals are returned to you or securely destroyed on your instruction.

Please do not send us Aadhaar numbers, OTPs, portal passwords, or Digital Signature Certificate PINs through WhatsApp or email. Where these are needed, we will direct you to the secure route.

6. Aadhaar - Specific Terms

6.1 We do not perform Aadhaar authentication. ARB FinTech LLP is **not** an Authentication User Agency (AUA), e-KYC User Agency (KUA), Sub-AUA, or requesting entity under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. We have no connection to the Central Identities Data Repository (CIDR) and we do not authenticate any Aadhaar number ourselves. Accordingly, the notification and authorisation process for private entities under the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020, as amended in 2025, does not apply to us.

6.2 Authentication happens on the Government portal, directly with you. Where a statutory filing requires Aadhaar verification, the authentication is performed by the Government portal concerned in conjunction with UIDAI. The One-Time Password (OTP) is generated by UIDAI and delivered by UIDAI **directly to the mobile number and email address registered against your Aadhaar -** not to us, and not through us.

6.3 Why an Aadhaar OTP is requested - the specific filings. So that you always know why verification is being sought, the following are the only circumstances in which an Aadhaar OTP will arise in the course of our services:

Filing / Service	Why Aadhaar verification is required	Governing provision
GST registration (Form GST REG-01)	Aadhaar authentication of the proprietor, partner, director, or authorised signatory. Without it, registration proceeds only after physical verification of the place of business.	Rule 8(4A), CGST Rules, 2017
GST amendment, revocation, refund	Re-authentication of the authorised signatory	CGST Rules, 2017
Income Tax return e-verification	Verifying the return after filing, in place of a physical ITR-V	Section 139, Income-tax Act, 1961
Income Tax e-filing portal registration / password reset	Identity verification on the portal	Income-tax Rules
PAN-Aadhaar linkage	Mandatory linkage of PAN with Aadhaar	Section 139AA, Income-tax Act, 1961
Company / LLP incorporation (SPICe+, FiLLiP), DIR-3 KYC	Verification of the proposed director or designated partner on the MCA portal	Companies Act, 2013; MCA Rules
Digital Signature Certificate issuance	eKYC verification by the licensed Certifying Authority	IT Act, 2000; CCA guidelines

If you receive an Aadhaar OTP that does not correspond to a filing you have engaged us for and authorised, **do not share it with anyone**, and report it to us at info@taxque.in immediately.

6.4 Handling of the OTP - you enter it. The OTP is yours, and our standing practice is that **you enter it yourself**. Where a filing requires it, we will prepare the submission and then ask you to complete the authentication step directly - by screen-sharing, by our sharing the portal session with you, or by your entering the OTP on your own device.

We do not ask clients to send Aadhaar OTPs to us by WhatsApp, SMS, or email. In the rare case where a portal's design makes contemporaneous entry unavoidable and you elect to communicate the OTP to us during a live, scheduled call for a filing you have expressly authorised, it is used **once, immediately, for that single transaction only**, and is **never stored, logged, recorded, screenshotted, or retained** in any system of ours. An Aadhaar OTP expires within minutes and cannot be reused.

We will never request an Aadhaar OTP by unsolicited call, message, or email, and never outside a filing you have specifically instructed. If anyone claiming to represent TaxQue asks you for an OTP in any other circumstance, do not share it and report it to info@taxque.in immediately.

6.5 The Aadhaar number itself. Where a statutory form requires the Aadhaar number to be stated, we enter it into that form on the Government portal on your authorisation. In our own records we hold it only in **masked form (last four digits)** or as an encrypted reference, and only for so long as the filing or the statutory retention period requires. We do not maintain a searchable database of Aadhaar numbers.

6.6 Biometrics. We do not collect, receive, process, or store fingerprint, iris, facial, or any other biometric or core biometric information at any time, for any purpose.

6.7 No onward use. Aadhaar-related data is used solely for the specific filing for which you provided it. It is not shared with any Associate Professional or third party except where the statutory form itself requires it, is not used for marketing, profiling, or analytics, and is not used to link or match your records across services. We observe Section 29 of the Aadhaar Act and the applicable UIDAI regulations on use, storage, and disclosure.

6.8 Your right to decline, and the alternatives. Aadhaar verification is sought with your separate, specific consent. You may decline, and we will tell you what follows in your particular case. Lawful alternatives generally include:

- **GST registration -** proceed without Aadhaar authentication, in which case the officer conducts physical verification of the place of business before registration is granted;
- **Income Tax return verification -** verify through net banking, bank account EVC, demat account EVC, Digital Signature Certificate, or by posting a signed ITR-V to CPC Bengaluru;
- **Company and LLP filings -** verification through Digital Signature Certificate and alternative identity documents.

Declining Aadhaar verification may lengthen processing timelines or require additional documents. It does not affect your entitlement to our services.

7. Portal Credentials and Filing Authorisation

7.1 To file on your behalf, we may need access to your credentials for the Income Tax e-filing portal, GST portal, MCA/V3 portal, TRACES, EPFO, ESIC, or similar systems.

7.2 **Credentials are stored encrypted, are accessible only to the specific personnel and Associate Professional assigned to your matter, and are never used for any purpose other than executing the work you have engaged us for.**

7.3 By providing credentials or a Digital Signature Certificate, **you expressly authorise TaxQue and the assigned Associate Professional to access those portals and to prepare, sign where authorised, and submit filings on your behalf.** Every access is logged.

7.4 **You may revoke this authorisation at any time in writing.** On revocation, or on conclusion of your engagement, we delete stored credentials within thirty (30) days. **We strongly recommend you change your portal passwords upon conclusion of any engagement.**

7.5 We are not responsible for the availability, accuracy, downtime, rejection, or security of any government portal, nor for consequences arising from portal failure, statutory changes, or actions of the relevant authority.

PART D - SHARING AND DISCLOSURE

8. Sharing with Associate Professionals - Core Disclosure

8.1 Please read this clause carefully. It describes how we deliver your work.

TaxQue does not perform every professional function in-house. **We share your personal and financial data with Associate Professionals for the specific purpose of executing your engagement.** This is a core, disclosed feature of our service model, not an incidental transfer.

8.2 **Who receives your data.** Only the Associate Professional(s) assigned to your specific matter, and only the categories of data necessary for that matter. Assignment is made on the basis of the service required, statutory qualification, and jurisdiction.

8.3 **Categories of Associate Professional:**

- Practising Chartered Accountants and CA firms - audit, certification, ITR, accounting
- Practising Company Secretaries and CS firms - ROC, MCA, secretarial compliance
- Practising Cost and Management Accountants - cost records, cost audit
- Advocates - representation, opinions, litigation support
- GST Practitioners enrolled under the CGST Rules - GST filings
- e-Return Intermediaries registered with the Income Tax Department - ITR transmission

8.4 **Contractual safeguards.** Every Associate Professional is bound by a written agreement with us requiring: purpose limitation to the assigned matter; confidentiality surviving termination; security safeguards equivalent to our own; a prohibition on onward disclosure without our written authorisation; a prohibition on retention beyond the statutory minimum; immediate breach notification to us; and return or certified deletion of data on completion.

8.5 **Professional obligations.** Associate Professionals are additionally bound by the confidentiality and ethical codes of their respective statutory institutes (ICAI, ICSI, ICMAI, Bar Council).

8.6 **Your consent.** Your consent to this sharing is sought expressly and separately at onboarding. **If you decline, we will not be able to deliver services requiring professional certification, attestation, or signature.**

8.7 **We remain accountable.** Sharing your data with an Associate Professional does not transfer our responsibility for it. We are accountable to you for the processing carried out by every Associate Professional on your matter, and we will not decline a request or complaint on the ground that the processing was carried out by a professional rather than by us. The statutory duties described in Clause 3.3 exist alongside, and do not reduce, that accountability.

9. Other Recipients

9.1 **Government authorities and portals.** Data is transmitted to the Goods and Services Tax Network (GSTN), the Income Tax Department, the Ministry of Corporate Affairs, CBDT, EPFO, ESIC, State Commercial Tax Departments, and Registrars - solely to execute the filing you have authorised.

9.2 **Data Processors.** Application and database hosting (Hostinger, Mumbai); object storage for website and portal uploads (Cloudflare R2); document storage and archival (Microsoft Corporation - OneDrive); network security, DDoS mitigation, and content delivery (Cloudflare); email service provider; messaging services (Meta Platforms - WhatsApp); payment gateways; SMS delivery providers; OCR and document-extraction services; and accounting or practice-management software vendors. The providers named above are those engaged as at the date of this version and are given as examples of each category. Each is contractually bound under Section 8(2) of the DPDP Act to process only on our instructions with equivalent safeguards -

including, in the case of Microsoft Corporation, the Microsoft Products and Services Data Protection Addendum applicable to our Microsoft 365 subscription. **We remain responsible to you for their processing.**

9.3 **Professional advisers and auditors** - our own legal counsel, auditors, and insurers, under privilege or confidentiality.

9.4 **Changes of provider.** We maintain a current list of Data Processors, available free of charge on written request to info@taxque.in. Replacing a provider within an existing category - for example, moving from one hosting or storage provider to another - is not a material change and does not require advance notice, provided the replacement is bound by equivalent contractual safeguards and the categories of data and purposes are unchanged. Advance notice under Clause 21.2 is required only where we introduce a **new category** of recipient, a new purpose, or a new category of data.

9.5 **Legal and regulatory disclosure.** We disclose where required by: a court order, decree, or summons; a notice or summons from a tax, regulatory, or investigative authority; a lawful direction under the Income-tax Act, CGST Act, Companies Act, PMLA, or Code of Criminal Procedure / BNSS; or a CERT-In direction. Where legally permitted, we will inform you before disclosing.

9.6 **Legal claims.** We may disclose data to the extent necessary to establish, exercise, or defend a legal claim, including recovery of unpaid fees and defence of a professional negligence or disciplinary proceeding.

9.7 **Business transfer.** In a merger, amalgamation, conversion, or transfer of the LLP or its business, data may transfer to the successor entity, which will remain bound by this Policy. You will be notified.

9.8 We do not sell your personal data. We do not share it for third-party advertising or profiling. We do not use your financial data to train machine-learning models.

10. Anti-Money Laundering

10.1 Certain activities we facilitate - including entity formation and management of client assets or accounts - may attract obligations under the PMLA for the Associate Professional carrying them out, following the Ministry of Finance notifications of 3 and 9 May 2023 designating practising CAs, CSs, CMAs, and advocates carrying out specified financial transactions on behalf of clients as reporting entities.

10.2 Where applicable, KYC records are retained and reports are furnished to the Financial Intelligence Unit - India as required by law. **Such reporting is a statutory obligation, is not subject to your consent, and may not be capable of disclosure to you.**

10.3 Company formation activity limited to filing the declaration under Section 7(1)(b) of the Companies Act, 2013 is excluded from this framework by the notification of 9 May 2023.

PART E - SECURITY, RETENTION, AND TRANSFERS

11. Security Safeguards and Breach Notification

11.1 **Technical measures.** AES-256 encryption at rest; TLS 1.3 in transit; a partitioned Secure Vault architecture preventing cross-client access; no storage of client data on local or personal devices; Web Application Firewall; DDoS mitigation; role-based access control on least-privilege principles; multi-factor authentication for all internal accounts; masking and tokenisation of identifiers; and monitored, immutable access logging.

11.2 **Organisational measures.** Background verification of personnel; signed confidentiality undertakings; periodic training; documented incident-response procedures; vulnerability patching; periodic penetration testing and internal audit; and secure destruction of physical documents and decommissioned media.

11.3 **Log retention.** Logs and processing records are retained for a minimum of one (1) year for the detection, investigation, and remediation of unauthorised access, or longer where the law requires.

11.7 **Messaging and device controls.**

(a) Company account only. Client communication over WhatsApp takes place solely through the official TaxQue business number operated by the LLP. Personnel are prohibited from receiving, requesting, or holding client documents on personal WhatsApp accounts, personal email, or personal devices.

(b) Transfer and deletion. Documents received through the business number are transferred to the Secure Vault and the corresponding chat content and attachments are then deleted from the messaging application.

(c) Scheduled device purge. Client data is removed from the local storage of all devices used for client communication under a documented internal schedule, and the purge is logged. Residence of a document on a device is transient, limited to the period between receipt and the next scheduled purge. The applicable interval is set out in our internal Device Handling Procedure and is kept under review.

(d) Configuration. Media auto-download to device storage and cloud chat backup are disabled on all devices used for client communication, so that client documents are not written to the device gallery and are not replicated to any third-party backup service.

(e) Device security. Devices used for client work are access-protected, encrypted at rest, and capable of remote wipe. Loss or theft of any such device is treated as a potential personal data breach and handled under Clauses 11.4 and 11.5.

11.4 **Breach notification - DPDP.** On becoming aware of a personal data breach, we will:

(a) inform the Data Protection Board of India **without delay**, with the nature, extent, timing, and location of the breach and its likely impact;
(b) furnish a **detailed report to the Board within 72 hours** (or such longer period as the Board allows), covering the broad facts and causes, mitigation measures taken and proposed, findings on the person responsible, remedial steps to prevent recurrence, and a summary of the intimations issued to affected Data Principals; and
(c) intimate **every affected Data Principal without delay** - in plain language, describing the breach, the data affected, the likely consequences, the mitigation undertaken, the protective steps you may take, and our contact particulars.

There is no minimum threshold. Every breach is notified, regardless of size or severity.

11.5 **CERT-In.** Where the incident is a reportable cyber security incident, we will additionally report it to CERT-In **within six (6) hours** of becoming aware. This is a separate and parallel obligation.

11.6 **Your responsibility.** You must keep your password confidential, use multi-factor authentication where offered, verify that communications originate from a @taxque.in address, and notify us immediately at info@taxque.in of any suspected compromise. **We will never ask for your password by phone, email, or WhatsApp.** No system is impregnable, and we do not warrant absolute security.

12. Retention Schedule

We retain personal data only as long as the purpose is served, or as the following statutory minimums require - whichever is longer:

Record Category	Retention Period	Legal Basis
GST records, invoices, returns	72 months from the due date of furnishing the annual return	CGST Act Section 36
GST records under appeal, revision, or investigation	1 year after final disposal, or 72 months, whichever is later	CGST Act Section 36 proviso
Income-tax records and supporting documents	Six (6) years from the end of the relevant assessment year; longer where reassessment proceedings are live	Income-tax Act; Rule 6F

Books of account of companies and LLPs	eight (8) financial years immediately preceding the current year	Companies Act Section 128(5)
Entity incorporation and ROC records	Permanently, or as the Registrar requires	Companies Act; LLP Act
KYC records where PMLA applies	5 years from the end of the client relationship or transaction	PMLA Section 12
Access, security, and processing logs	Minimum 1 year	DPDP Rules, Rule 6
Consent records and notice versions	Duration of processing plus 3 years	DPDP Act Section 8
Engagement records, advice, correspondence	Duration of engagement plus 3 years	Limitation Act, 1963
Account profile and dashboard data	Erased when the purpose ceases - on withdrawal of consent, completion of purpose, or 12 months of non-engagement - subject to the statutory minimums above	DPDP Act Section 8(7); Rule 8
Documents for a cancelled engagement where no filing was made	Erased within 30 days of cancellation or refund settlement, whichever is later	DPDP Act Section 8(7); Rule 8
Payment and fee records	8 years	Companies Act; Income-tax Act

12.1 **Erasure is automatic, not on request.** Section 8(7) of the DPDP Act requires erasure once the purpose is no longer served; it is not optional and does not depend on your asking. Where a retention period expires and no statutory obligation, live proceeding, or unresolved dispute requires continued retention, we erase the data and instruct our Data Processors to do the same.

12.1A **What automatic erasure does NOT affect.** For the avoidance of doubt, automatic erasure applies only to data whose statutory and contractual retention periods have **already expired**. It does **not** apply to, and will **not** delete, any of the following while their retention periods in the table above are running:

- filed returns, acknowledgements, computations, and their supporting documents;
- books of account, financial statements, and audit records;
- incorporation, ROC, and entity constitution records;
- KYC records held under the PMLA;
- any record relevant to a pending or anticipated assessment, scrutiny, appeal, notice, investigation, or dispute.

Where a notice, audit, or proceeding arises, the relevant records are placed under a **legal hold** and are retained until the matter is finally concluded, notwithstanding any expiry of the ordinary retention period.

12.2 **Notice before non-engagement erasure.** Erasure triggered by prolonged non-engagement affects only your account profile and dashboard data - never records under statutory retention. Before any such erasure we will give you notice at your registered email address and mobile number **at least thirty (30) days in advance**, and a reminder at least forty-eight (48) hours before, so that you may download your documents, object, or re-engage. A single response from you resets the period.

12.2B **Cancelled engagements.** Where you cancel a service and **no filing has been made to any authority**, the purpose for which your documents were collected is extinguished and no statutory retention period arises. Those documents are erased within thirty (30) days of cancellation or refund settlement, whichever is later, and any Associate Professional who received them is instructed to erase or return them and to confirm having done so. We retain only the transaction record - invoice, payment and refund records, and cancellation correspondence - under its own retention period. Where a filing **was** made before cancellation, the statutory periods in the table above continue to apply and the records are not erased. This mirrors Clause 3.4 of our Refund, Cancellation and Service Modification Policy.

12.2A **Export your records.** You may at any time request a complete copy of the documents we hold for you, free of charge, by writing to info@taxque.in. We recommend you retain your own copies of all filed returns and supporting records independently of our Platform.

12.3 Where erasure is not technically feasible from backup media, data is isolated, blocked from processing, and destroyed on the ordinary backup expiry cycle.

13. Cross-Border Transfers

13.1 **Where your data is held.**

Layer	Provider	Location
Application server and database	Hostinger	Mumbai, India
Website and portal file uploads	Cloudflare R2	Automatic placement across Cloudflare's network; no jurisdictional restriction applied
Document storage and archival	Microsoft OneDrive (Microsoft 365), encrypted	Microsoft 365 tenant default region
Email	Microsoft 365 (Exchange Online)	Microsoft 365 tenant default region
Network security, WAF, content delivery	Cloudflare	Global edge locations
Messaging	Meta Platforms (WhatsApp)	Global

Cloudflare's edge network may cache non-personal static content outside India. Personal data is not stored at edge locations.

13.2 **No persistent local storage.** Client data is not stored on office computers, local drives, removable media, or personal devices. Documents received through email or messaging may reside transiently on a company-controlled device between receipt and transfer to the Secure Vault, and are removed by the scheduled purge described in Clause 11.7(c). Working copies created during preparation of a filing are deleted on completion. No client data is held on personal devices at any time.

13.3 **Legal position on transfers.** Under Section 16 of the DPDP Act, transfer of personal data outside India is permitted **except to territories restricted by the Central Government by notification**. We do not transfer personal data to any restricted territory, and we monitor such notifications on a continuing basis.

13.4 Where a sectoral law or regulator imposes a stricter localisation requirement on any category of data, that stricter requirement prevails and we comply with it.

13.5 We will update this Clause on any material change to our infrastructure or storage locations.

14. Cookies and Tracking

14.1 **Strictly necessary cookies -** session authentication, security, load balancing, and CSRF protection. These are essential; the Platform cannot function without them.

14.2 **Preference cookies** - remembering interface settings. Optional.

14.3 **Analytics cookies -** measuring Platform performance and diagnosing faults. **Optional and set only with your consent.**

14.4 You may accept or reject each non-essential category independently through the cookie banner on first visit, and may change your choice at any time via *Cookie Settings* in the footer. **Rejecting is as easy as accepting.** We do not use advertising or cross-site tracking cookies.

15. Communications

15.1 **Transactional communications -** filing acknowledgements, deadline reminders, OTPs, invoices, and security alerts - are integral to the service and are sent for as long as your engagement subsists.

15.2 **Promotional communications** are sent only with your separate opt-in and may be withdrawn at any time without affecting service delivery.

15.3 Commercial communications are sent in compliance with TRAI's Telecom Commercial Communications Customer Preference Regulations. Registration on the National Do Not Disturb registry does not suspend transactional communications you have consented to as part of your engagement.

PART F - YOUR RIGHTS

16. Rights of the Data Principal

Under the DPDP Act you have the following rights:

16.1 Right to access information - a summary of the personal data being processed, the processing activities undertaken, and the identities of all Data Fiduciaries and Data Processors with whom it has been shared, together with a description of what was shared.

16.2 Right to correction, completion, updating, and erasure - correction of inaccurate or misleading data, completion of incomplete data, updating, and erasure of data no longer necessary for the purpose, subject to the statutory retention obligations in Clause 12.

16.3 Right to withdraw consent - as set out in Clause 4.4.

16.4 Right to grievance redressal - as set out in Clause 20, exercisable before approaching the Data Protection Board.

16.5 Right to nominate - you may nominate one or more individuals to exercise your rights in the event of your death or incapacity. Send your nomination by email to **info@taxque.in** with the subject line "Nomination", stating the nominee's full name, relationship to you, address, email, and mobile number, or deliver it in writing to either office. We will acknowledge and record the nomination, and will give effect to it on production of a death certificate or an order or certificate evidencing incapacity. You may revoke or replace a nomination at any time by the same means.

17. How to Exercise Your Rights

17.1 Submit a request by email to **info@taxque.in** with the subject line "**Data Principal Request**", or in writing to either office address in Clause 1.1. We maintain a register of all such requests and their disposal.

17.2 Your request must state your **registered email address and registered mobile number** so that we can identify you. Where the request concerns statutory filings, please also provide the relevant PAN or GSTIN. We may seek additional verification for high-risk requests; we will not use verification information for any other purpose.

17.3 **Response timelines:**

Request Type	Acknowledgement	Resolution
Access to information	48 hours	15 business days
Correction, completion, updating	48 hours	15 business days
Erasure	48 hours	30 business days
Withdrawal of consent	48 hours	Effective within 5 business days
Nomination	48 hours	15 business days
Grievance	48 hours	14 business days (statutory outer limit: 90 days)

17.4 **Your duties.** The DPDP Act requires you to furnish authentic and accurate information, not to impersonate another person, not to suppress material information, and not to register false or frivolous grievances. Furnishing false or incomplete information may result in an incorrect filing, for which we cannot be responsible.

17.5 We do not charge for exercising your rights. We may decline manifestly excessive or repetitive requests, giving reasons in writing.

18. Children and Persons with Disabilities

18.1 The Platform is not intended for independent use by persons below eighteen (18) years of age.

18.2 Where a service necessarily concerns a child - such as a minor's PAN, a minor's income clubbed under Section 64(1A) of the Income-tax Act, or a minor as a nominee, shareholder, or beneficiary - we process the child's data **only on verifiable consent of the parent or lawful guardian**, verified through the identity and age documents of the parent or guardian.

18.3 We do not undertake tracking, behavioural monitoring, or targeted advertising directed at children.

18.4 The same protections apply to a person with a disability who has a lawful guardian, on the guardian's verified consent.

18.5 If you believe a child's data has been collected without valid parental consent, write to info@taxque.in and we will verify and erase it.

PART G - LIMITATIONS AND LEGAL TERMS

19. Accuracy, Disclaimers, and Limitations

19.1 **Accuracy of information supplied.** Our services depend entirely on the completeness and accuracy of the data you supply. **You are solely responsible for the accuracy, authenticity, and completeness of all information and documents you provide.** We do not independently audit or verify them unless an audit is the engaged service. We are not liable for any assessment, demand, penalty, interest, prosecution, rejection, or loss arising from information that is inaccurate, incomplete, delayed, or suppressed by you.

19.2 **Review before filing.** Where a draft return, statement, or form is shared with you for approval, your approval constitutes your confirmation of its correctness.

19.3 **No professional advice by the Platform.** Content on the Platform is general information. It is not tax, legal, accounting, or investment advice. Professional advice is given only in a written engagement by a qualified professional.

19.4 **Third-party systems.** We do not control government portals or third-party services and are not liable for their downtime, errors, rejections, data loss, or changes in procedure.

19.5 **Statutory changes.** Tax and corporate law change frequently, sometimes retrospectively. We do not warrant that any position taken will not be altered by subsequent legislation, notification, circular, or judicial decision.

19.6 **Outcomes.** We do not guarantee any particular outcome, refund, approval, registration, or absence of scrutiny.

19.7 **Limitation of liability.** To the maximum extent permitted by law, our aggregate liability arising out of or in connection with any engagement shall not exceed **the greater of (a) the professional fees actually received by us for that specific engagement, or (b) Rs. 25,000 (Rupees Twenty-Five Thousand)** . The monetary floor at (b) applies equally to engagements undertaken at nominal cost, at concessional rates, or free of charge, so that no engagement carries a nil cap.

19.7A **Single source.** The cap in Clause 19.7 is the same cap stated at Clause 11.1 of our Terms of Service. Where the two differ for any reason, **the Terms of Service prevail** , so that only one limitation of liability applies across all our documents.

19.8 **Matters not limited.** Nothing in Clause 19.7 limits or excludes liability for fraud or fraudulent misrepresentation; wilful misconduct; gross negligence; death or personal injury caused by negligence; our statutory obligations under the DPDP Act, which cannot be contracted out of; or any other liability which cannot lawfully be limited or excluded under Indian law. Subject to the foregoing, we are not liable for indirect, incidental, consequential, punitive, or exemplary loss, or for loss of profit, business, goodwill, or opportunity. Detailed limitation terms are in our Terms of Service.

19.9 **Indemnity.** You agree to indemnify and hold harmless ARB FinTech LLP, its designated partners, employees, and Associate Professionals against claims, demands, penalties, and costs (including reasonable legal fees) arising from information you supplied that was false, incomplete, or misleading; from your breach of this Policy or the Terms of Service; from your failure to hold authority to disclose third-party data under Clause 5.4; or from your unlawful use of the Platform.

19.10 **Force majeure.** We are not liable for delay or failure caused by events beyond our reasonable control, including government portal failure, network or power outage, cyber-attack notwithstanding reasonable safeguards, natural disaster, epidemic, strike, or change in law.

20. Grievance Redressal

20.1 **Grievance Officer.** Md Afzal serves as Grievance Officer under the DPDP Act, 2023 and the Information Technology Act, 2000, and additionally as Grievance Officer and Nodal Officer under the Consumer Protection (E-Commerce) Rules, 2020. He is resident in India. Where we are designated a Significant Data Fiduciary, a separate India-resident Data Protection Officer will be appointed under Clause 3.5 and these details updated.

Name	Md Afzal
Designation	Grievance Officer and Nodal Officer, TaxQue by ARB FinTech LLP
Address	Surbhi Vihar, Mithapur, Patna, Bihar - 800001, India
Email	info@taxque.in
Telephone	+91 93112 56088
Hours	Monday to Saturday, 10:00 - 18:00 IST (excluding public holidays)

20.2 We acknowledge every privacy grievance **within 48 hours** and aim to resolve it **within 14 business days**, and in any event within the statutory limit of ninety (90) days.

20.2A **Commercial grievances.** The same Grievance Officer also handles complaints about refunds, cancellations, billing, and service quality. Those are governed by our Refund, Cancellation and Service Modification Policy and carry a shorter outer limit of **one (1) month** under the Consumer Protection (E-Commerce) Rules, 2020. Where a complaint raises both privacy and commercial matters, each aspect is dealt with under its own timeline, and we will tell you in the acknowledgement which applies to which part.

20.3 **Escalation to the Board.** If you are not satisfied with our response, or if we do not respond within the applicable period, you may complain to the **Data Protection Board of India** in the manner prescribed under the DPDP Act and DPDP Rules. **You should ordinarily exhaust the grievance mechanism above before approaching the Board.** Details are published at https://www.meity.gov.in.

20.4 Complaints concerning an Associate Professional acting in independent professional capacity may additionally be raised with their institute (ICAI, ICSI, ICMAI) or Bar Council.

21. Changes to this Policy

21.1 We may revise this Policy to reflect legal, technical, or operational change. The version number and date at the head of this document indicate the current version.

21.2 **Material changes -** including any new purpose of processing, new category of recipient, or new category of data **-** will be notified at least **fifteen (15) days** in advance by email to your registered address and by notice on your dashboard.

21.3 **A new purpose requires fresh consent.** We will not process your data for a purpose you have not consented to merely because this Policy has been updated. Continued use of the Platform is not consent to a new purpose.

21.4 Archived versions are available on request.

22. Governing Law and Jurisdiction

22.1 This Policy is governed by and construed in accordance with the laws of India.

22.2 Subject to Clause 22.4, the courts at **Hajipur and Vaishali, Bihar** shall have exclusive jurisdiction over all disputes, differences, and claims arising out of or in connection with this Policy, to the exclusion of all other courts.

22.3 Nothing in this Clause limits the jurisdiction of the Data Protection Board of India, or of any tax, corporate, or regulatory authority exercising statutory powers.

22.4 **Consumer rights preserved.** Where you qualify as a "consumer" under the Consumer Protection Act, 2019, **nothing in Clause 22.2 restricts your statutory right under Section 34(1)(d) of that Act to institute a complaint before a Consumer Commission within whose jurisdiction you ordinarily reside, work for gain, or personally work.** Clause 22.2 applies to commercial and other non-consumer disputes.

23. Severability and Miscellaneous

23.1 If any provision is held invalid or unenforceable, it shall be severed and the remainder shall continue in full force.

23.2 Our failure to enforce any provision is not a waiver of it.

23.3 Headings are for convenience only.

23.4 This Policy is executed in English. Translations are provided for convenience; in the event of conflict, the English version prevails.

24. Acknowledgement

By submitting the standalone Consent Notice referred to in Clause 4.1, you confirm that you have read and understood this Policy; that you are eighteen (18) years of age or older, or are a parent or lawful guardian consenting on behalf of a child; that where you act for a firm, company, LLP, trust, or other entity, you are duly authorised to bind it; and that the information you furnish is true, accurate, and complete.

DOCUMENT SET

This document forms part of the TaxQue legal document set. In the event of conflict, the following order of precedence applies:

Priority	Document	ID	Governs
1	Privacy Policy	TQ-PP	All matters concerning personal data
2	Refund, Cancellation and Service Modification Policy	TQ-RCP	Refunds, cancellation, and service migration
3	Terms of Service	TQ-TOS	All other contractual matters

Grievance Officer and Nodal Officer: Md Afzal · info@taxque.in · +91 93112 56088
Surbhi Vihar, Mithapur, Patna, Bihar - 800001, India · Monday to Saturday, 10:00 AM-06:00 PM IST

ARB FinTech LLP · LLPIN ABC-5112 · GSTIN 10ABZFA6377J1ZX
Registered Office: KH No. 1508, Village - Lemuwari, Ward No. - 08, Block - Patepur, District - Vaishali, Bihar - 843114, India

Branch Office: Surbhi Vihar, Mithapur, Patna, Bihar - 800001, India