BYTEFALCON TECHNOLOGIES PRIVATE LIMITED

Xenora Platform

DATA PROTECTION POLICY

Privacy, Security & Compliance Framework

Attribute	Details
Document Version	2.0 — Revised
Effective Date	April 15, 2026
Previous Version	1.0 — April 14, 2026
Review Cycle	Annual or upon material change in applicable law
Jurisdiction	India (Primary) | Gulf (UAE/KSA) | European Union | United States
Governing Law	DPDPA 2023, IT Act 2000, GDPR 2016/679, UAE PDPL 2021
Governing Courts	Exclusive jurisdiction — Courts of Chennai, Tamil Nadu, India
Classification	Public — Customer-Facing / Enterprise B2B Compliance
Issuing Authority	ByteFalcon Technologies Pvt Ltd — Data Protection Officer

ByteFalcon Technologies Private Limited
Tamil Nadu, India | xenora.ai
CIN: U62013TN2026PTC192479| GST : 33AAOCB6812C1ZY

1. Introduction and Scope

ByteFalcon Technologies Private Limited ("Company", "We", "Us") operates Xenora ("Platform"), a multi-tenant AI-powered document collection and workflow automation platform at xenora.ai. This Data Protection Policy ("Policy") sets forth the principles, obligations, and technical safeguards governing the collection, processing, storage, transfer, and deletion of personal data processed through the Platform.

This Policy applies to all data processed on behalf of Tenants (business customers and their end-users), all ByteFalcon employees and contractors, and all integrated third-party services and AI model providers used within the Platform.

Applicable Legal Framework

India: DPDPA 2023 | IT Act 2000 | IT (SPDI) Rules 2011 | CERT-In Directions 2022
European Union: GDPR — Regulation (EU) 2016/679
UAE: Federal Decree-Law No. 45 of 2021 on Personal Data Protection (PDPL)
KSA: Personal Data Protection Law (PDPL), Royal Decree No. M/19 (2021)
United States: CCPA / CPRA (California), where applicable
Standards: ISO/IEC 27001:2022 | OWASP ASVS | NIST Cybersecurity Framework

2. Definitions

For the purposes of this Policy, the following terms shall have the meanings assigned below:

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person (Data Principal), per DPDPA 2023 and GDPR Article 4(1).
Sensitive Personal Data	Categories listed under IT (SPDI) Rules 2011, Rule 3 — including financial data, health data, and biometric data.
Tenant	A business entity subscribing to Xenora acting as Data Fiduciary / Controller in respect of its own customers' data.
Data Principal / User	An end-user whose personal data is processed by the Platform at the direction of a Tenant.
Data Fiduciary / Controller	ByteFalcon Technologies for its own processing; the Tenant for processing its customers' data.
Data Processor	ByteFalcon Technologies when processing personal data on behalf of and under instructions of a Tenant.
Sub-Processor	A third-party service provider engaged by ByteFalcon Technologies to process data on its behalf.
Processing	Any operation on personal data including collection, storage, use, transmission, or deletion.
Breach / Incident	Any accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal data.

3. Data Transmission Security

ByteFalcon Technologies implements the following controls to ensure all personal data is transmitted securely, consistent with IT (SPDI) Rules 2011, Rule 8, and GDPR Article 32:

3.1 WhatsApp Channel Security

Where the Platform's WhatsApp-first document collection interface is used, communications are protected by WhatsApp's native end-to-end encryption (E2EE) based on the Signal Protocol. WhatsApp Business API (Meta) acts as a communication sub-processor under a Data Processing Agreement consistent with GDPR Article 28 and the DPDPA 2023 consent framework.

3.2 Web-Based Secure Link Transmission

All data submitted via the Platform's web portal or secure link interface is transmitted exclusively over HTTPS using TLS 1.2 or higher (TLS 1.3 preferred). HTTP Strict Transport Security (HSTS) is enforced on all web-facing endpoints. TLS certificates are provisioned and renewed via automated certificate management.

3.3 OTP Authentication for Secure Links

Access to all secure document submission links is protected by a One-Time Password (OTP) mechanism delivered via a verified channel. OTPs are cryptographically random, time-limited (maximum 10 minutes), and single-use, consistent with OWASP ASVS Level 2 requirements.

3.4 Encryption at Rest

All personal data stored within the Platform's database infrastructure is encrypted at rest using AES-256 encryption (NIST FIPS 197). Encryption keys are managed through a dedicated key management system isolated from the encrypted data stores.

4. Tenant Data Isolation and Access Security

4.1 Schema-Level Tenant Isolation

Each Tenant's data is logically segregated within a dedicated database schema. The application layer enforces Tenant context at every query execution point, preventing cross-tenant data leakage. No shared tables contain commingled Tenant personal data.

4.2 Tenant-Specific Encryption Keys

Each Tenant is assigned a unique, independently managed encryption key. Key lifecycle management (generation, rotation, revocation) is conducted at the Tenant level. Compromise of one Tenant's key does not affect any other Tenant's data.

4.3 Passwordless Authentication

The Platform does not store user passwords. Authentication is implemented through:

- **Magic Link + OTP:** A time-limited, cryptographically signed login link delivered to the user's registered email, supplemented by an OTP for identity confirmation.
- **OpenID Connect (OIDC):** Users may authenticate via Google Workspace or Microsoft Azure AD using OIDC, delegating credential management to the identity provider. ByteFalcon does not store or access identity provider credentials.

5. Data Retention and Deletion Policy

ByteFalcon Technologies adopts a Tenant-controlled data retention model. Personal data is retained for the minimum period necessary to fulfil contractual obligations unless applicable law mandates otherwise.

5.1 Default Retention

All Tenant data is retained for the duration of the active subscription and until a deletion request is initiated by the authorised Tenant Administrator. ByteFalcon Technologies does not proactively purge Tenant data during an active subscription without an explicit deletion instruction.

5.2 Tenant-Initiated Deletion

Tenants retain full and exclusive authority to initiate deletion. The following deletion scopes are supported:

- Organisation-Level Deletion: Complete and permanent deletion of all data associated with the Tenant's organisation, including all cases, files, transactions, timelines, audit logs, and processing records.
- Case-Level Deletion: Targeted deletion of a specific customer case or multiple selected cases. All associated records, files, transaction history, timelines, and metadata are permanently removed.

Upon execution of any deletion request, Xenora does not retain any archive, backup copy, secondary storage instance, or processing artefact of the deleted data. Deletion is irreversible. ByteFalcon Technologies expressly disclaims any obligation or ability to restore deleted data.

5.3 Trial User Data

Personal data associated with Trial accounts is automatically and permanently deleted thirty (30) calendar days after the trial period concludes, unless the Tenant converts to a paid subscription prior to that date.

5.4 Deactivated and Overdue Accounts

1. Read-Only Access Period: The Tenant is granted read-only access for six (6) months from the date of deactivation or the first payment default.
2. Notification: Prior to expiry of the read-only period, the Tenant is notified in writing via registered email of the impending permanent deletion.
3. Permanent Deletion: Upon expiry of the six-month period, all Tenant data is permanently and irreversibly . No restoration is available after this point.

5.5 Data Collected Through a Provider (Processor Relationship)

Where a business uses Xenora/DocFlow to collect your documents on your behalf — for example, your chartered accountant, auditor, HR team, or loan processor (your "Provider") — that Provider is the Data Fiduciary / Controller of your data, and ByteFalcon acts solely as a Data Processor on their documented instructions.

To exercise access or deletion rights over such data:

1. **Contact your Provider first**. They hold the direct relationship with you and are responsible for responding to your request under the DPDPA 2023 (and GDPR / UAE PDPL where applicable).
2. **If they do not respond**, write to dpo@xenora.ai with proof of your request to the Provider. We will notify them and, unless they raise a lawful objection, assist in deleting your data.

6. Security Audits and Vulnerability Management

6.1 Continuous Code Security Scanning

The Platform’s codebase is subject to automated static application security testing (SAST) and dependency vulnerability scanning on a continuous (daily) basis. Vulnerabilities are triaged by severity and tracked to remediation.

6.2 OWASP Compliance

ByteFalcon Technologies designs and maintains the Platform in accordance with the OWASP Top 10 Application Security Risks and OWASP ASVS. Development teams undergo periodic security training aligned to OWASP guidance.

6.3 CVE Remediation SLA

Upon identification or public disclosure of a CVE affecting the Platform or its dependencies:

Severity	Remediation Timeline
Critical (CVSS 9.0–10.0)	Within 24 hours of disclosure / identification
High (CVSS 7.0–8.9)	Within 72 hours
Medium (CVSS 4.0–6.9)	Within 14 calendar days
Low (CVSS 0.1–3.9)	Within 30 calendar days or next scheduled release

7. Artificial Intelligence and Model Usage Policy

Core AI Data Commitment

Tenant and User data is NEVER used to train any AI model — internal or external.

All AI processing is performed solely to respond to queries within active session context.

7.1 Ethical AI Use

AI capabilities within Xenora and all ByteFalcon products are restricted to lawful, ethical, and purpose-limited applications. AI shall not be used for discriminatory profiling, automated decisions with significant legal effect without human oversight, or any purpose that violates applicable law or the rights of Data Principals.

7.2 Prohibition on Client Data for Model Training

ByteFalcon Technologies expressly warrants that no Personal Data, Sensitive Personal Data, or organisational data belonging to Tenants or their end-users is used to fine-tune, pre-train, or otherwise train any proprietary or internal machine learning model operated or developed by ByteFalcon Technologies.

7.3 Third-Party AI Model Providers

The Platform utilises APIs provided by third-party AI model providers, currently including Anthropic, PBC. The following confirmed protections apply:

- **No Training on API Data:** Under Anthropic's published commercial API terms, prompt and response data submitted via API is never used for model training and is automatically deleted within 7 days of processing.
- **No Opt-In to Training Programmes:** ByteFalcon Technologies does not opt in to any model training or data contribution programmes offered by third-party AI providers on behalf of Tenants.
- **API-Level Protection Only:** The above protections reflect Anthropic's standard commercial API terms and are not based on a separately negotiated Zero Data Retention (ZDR) enterprise agreement, which ByteFalcon Technologies has not entered into as of the effective date of this Policy.
- **Forward-Looking ZDR Commitment:** In the event ByteFalcon Technologies enters into a formal Zero Data Retention (ZDR) or equivalent agreement with any AI provider, this Policy will be updated accordingly with 14 days' prior notice to Tenants.

> **Note on ZDR**
> Zero Data Retention (ZDR) is an enterprise-tier arrangement requiring a separately negotiated agreement with Anthropic. ByteFalcon Technologies currently provides protection through the standard commercial API terms (7-day deletion, no training use), which is the correct and accurate characterisation of our current AI data handling. We will pursue formal ZDR arrangements as Xenora scales to enterprise tier.

8. Sub-Processor Register

The following third-party sub-processors may process personal data on behalf of ByteFalcon Technologies. All are subject to data processing agreements consistent with DPDPA 2023, GDPR Article 28, and applicable Gulf regulations:

Sub-Processor	Service | Data Protection | Location
Anthropic, PBC	AI Model API. Commercial API terms — no training use; 7-day log deletion. (United States)
Google Cloud Platform (GCP)	Cloud Infrastructure & Database Hosting. GCP DPA with GDPR SCCs; ISO 27001 certified. (Configurable regions)
Razorpay Software Pvt Ltd	Payment Processing — India (INR). PCI-DSS compliant; RBI regulated. (India)
Stripe, Inc.	Payment Processing — International (USD/AED). Stripe DPA with GDPR SCCs. (United States / EU)
Meta (WhatsApp Business API)	Communication Channel. WhatsApp Business API Data Processing Terms. (United States)

Langfuse (Self-Hosted)	LLM Observability. Self-hosted by ByteFalcon on own infrastructure — data does not leave ByteFalcon's servers.

This register is reviewed and updated periodically. Material additions will be notified to Tenants with at least 14 days' prior notice.

8.1 Document Collection via WhatsApp

For convenience, Xenora/DocFlow offers WhatsApp as a channel for collecting documents. Where this channel is used, your documents pass through the infrastructure of Meta Platforms, Inc. (WhatsApp Business API), which acts as a named Sub-Processor for message and media delivery. Documents are retrieved promptly and stored within our own secured infrastructure.

If your organisation prefers not to route documents through Meta, the WhatsApp channel can be disabled at any time under **Settings → Notifications → WhatsApp Notifications.** Once disabled, no documents will be collected via WhatsApp; collection will instead occur only through our secure web and desktop upload links.

9. Acceptable Use, Violations, and Suspension

9.1 Prohibited Conduct

Tenants, Tenant Users, and any third party accessing the Platform are prohibited from:

- Attempting to gain unauthorised access to another Tenant's data or organisational environment;
- Using the Platform for any unlawful purpose including fraud, harassment, or distribution of illegal content;
- Circumventing, disabling, or interfering with any security control, access control mechanism, or encryption;
- Using AI features for purposes that violate the IT Act 2000, Bharatiya Nyaya Sanhita 2023, or any applicable law, including generation of harmful, abusive, or deceptive content.

9.2 Consequences of Violation

4. Immediate suspension of account access, with or without prior notice, at ByteFalcon Technologies' reasonable discretion;
5. Preservation of relevant data and activity logs as evidence, to the extent required by applicable law or for legal proceedings;
6. Reporting to relevant law enforcement authorities or regulatory bodies, as required under the IT Act 2000, DPDPA 2023, or other applicable statutes;
7. Civil and/or criminal liability for harm caused to ByteFalcon Technologies, other Tenants, or affected Data Principals.

9.3 Unauthorised Access to Tenant Documents

Any individual or application that accesses, retrieves, copies, or processes a Tenant's documents without prior written authorisation from that Tenant shall be in violation of Sections 43 and 66 of the IT Act 2000, and applicable DPDPA 2023 provisions. Such acts may attract civil penalties and criminal prosecution. ByteFalcon Technologies will immediately suspend such access, preserve evidence, and report to appropriate authorities.

10. Security Incident and Data Breach Response

ByteFalcon Technologies maintains a documented Incident Response Plan (IRP) aligned to CERT-In Directions 2022, GDPR Articles 33–34, and UAE PDPL Article 27.

10.1 Containment and Immediate Response

Upon detection of a security incident, ByteFalcon Technologies' first obligation is immediate containment to prevent further harm. Measures may include suspension of affected services, revocation of compromised credentials, network isolation, or emergency infrastructure failover.

10.2 Notification to Affected Tenants — 72 Hours

ByteFalcon Technologies shall notify all reasonably identified affected Tenants within seventy-two (72) hours of becoming aware of a personal data breach, consistent with GDPR Article 33 and DPDPA 2023 breach notification provisions. The initial notification shall include:

- Nature and description of the breach;
- Categories and approximate volume of Personal Data and Data Principals affected;
- Likely consequences of the breach;
- Measures taken or proposed to address and mitigate the breach.

10.3 Regulatory Notification

Where required by applicable law, ByteFalcon Technologies shall notify CERT-In under the CERT-In Directions 2022, and the Data Protection Board of India upon its establishment under DPDPA 2023, within the prescribed timeframe. Notification to the applicable Gulf or EU supervisory authority shall be made where Tenants or affected Data Principals are located in those jurisdictions.

10.4 Post-Incident Audit

Following containment, ByteFalcon Technologies shall conduct a comprehensive forensic audit to determine root cause, scope of impact, and affected Data Principals. Affected Tenants shall receive a written Incident Report detailing findings and remediation measures within a reasonable timeframe.

11. Third-Party and Vendor-Induced Incidents

8. ByteFalcon Technologies shall immediately conduct an internal impact assessment upon becoming aware of a Sub-Processor security incident or service disruption that may affect Tenant data.
9. Affected Tenants shall be notified within seventy-two (72) hours of ByteFalcon Technologies becoming aware of the Sub-Processor incident, including a preliminary impact assessment and remedial steps underway.
10. ByteFalcon Technologies shall cooperate with the Sub-Processor's incident investigation and independently verify the accuracy of the Sub-Processor's impact assessment through its own audit mechanisms.

All Sub-Processor agreements include binding data protection and breach notification obligations consistent with DPDPA 2023, GDPR Article 28, and applicable Gulf data protection regulations.

12. Rights of Data Principals

ByteFalcon Technologies, as Data Processor, shall assist Tenants (as Data Fiduciaries/Controllers) in fulfilling Data Principal rights under DPDPA 2023 and GDPR. Requests may be submitted to the DPO at dpo@bytefalcon.in. Responses will be provided within 30 calendar days.

Right	Description and Legal Basis
Right of Access	Request confirmation of processing and obtain a copy of personal data. (DPDPA s.11; GDPR Art.15)
Right to Correction	Request rectification of inaccurate or incomplete personal data. (DPDPA s.12; GDPR Art.16)
Right to Erasure	Request deletion of personal data where the purpose has been fulfilled or consent withdrawn. (DPDPA s.12; GDPR Art.17)
Right to Portability	Receive personal data in a structured, machine-readable format. (GDPR Art.20 — EU/EEA Data Principals)
Right to Object	Object to processing based on legitimate interests. (GDPR Art.21 — EU/EEA Data Principals)
Grievance Redressal	Lodge a complaint with the Consent Manager or Data Protection Board of India. (DPDPA s.13)
Right to Nominate	Nominate a representative to exercise rights in the event of incapacity or death. (DPDPA s.14)
Withdraw Consent	Withdraw previously given consent at any time without affecting prior lawful processing.

13. Cross-Border Data Transfers

Where personal data is transferred outside the territory of India — including transfers to AI model providers and cloud infrastructure providers in the United States — ByteFalcon Technologies ensures the following:

13.1 India (DPDPA 2023)

Cross-border transfers are made only to countries or territories notified by the Government of India as providing adequate protection under the DPDPA 2023. The Government of India's adequacy notifications are pending as of the effective date of this Policy. In the interim, transfers to Sub-Processors occur under the data protection terms published by the respective Sub-Processor, which include contractual data protection obligations.

Important — No Independently Signed SCCs

ByteFalcon Technologies currently relies on Sub-Processors' own published data processing terms and Standard Contractual Clauses (where available) for cross-border transfer legitimacy. ByteFalcon Technologies has not independently entered into separate SCC agreements with each Sub-Processor as of this Policy's effective date. This is consistent with standard practice for SaaS companies at this stage. This Policy will be updated as formal transfer mechanisms are put in place.

13.2 European Union / EEA (GDPR)

For transfers involving EU/EEA Data Principals, ByteFalcon Technologies relies on the Standard Contractual Clauses (SCCs) published and adopted by its Sub-Processors (including Google Cloud Platform and Stripe), or on adequacy decisions issued by the European Commission, as applicable.

13.3 Gulf (UAE / KSA)

For Tenants and Data Principals located in the UAE or KSA, ByteFalcon Technologies processes data in accordance with the UAE Federal Decree-Law No. 45 of 2021 and the KSA Personal Data Protection Law. Sub-Processor contractual terms include data protection obligations applicable to Gulf jurisdictions.

14. Children's Privacy

The Xenora Platform is a business-to-business (B2B) professional service not directed at children. Under the Digital Personal Data Protection Act, 2023 (India), a "child" means a person below the age of eighteen (18) years. ByteFalcon Technologies does not knowingly collect personal data from children under 18. If ByteFalcon Technologies becomes aware that personal data of a child has been collected, it shall take immediate steps to delete such data and notify the relevant Tenant.

15. Governing Law and Jurisdiction

This Policy and any dispute or claim arising out of or in connection with it shall be governed by and construed in accordance with the laws of India, including the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and the Indian Contract Act, 1872.

Any disputes arising under this Policy shall be subject to the exclusive jurisdiction of the courts of Chennai, Tamil Nadu, India, without prejudice to the statutory rights of Data Principals under their local applicable law and without prejudice to the ability of regulatory authorities in any jurisdiction to exercise their independent statutory powers.

IP and Emergency Relief

Notwithstanding the above, ByteFalcon Technologies reserves the right to seek injunctive or other equitable relief in any competent court in any jurisdiction to protect its intellectual property, confidential information, or to prevent irreparable harm.

16. Contact, Grievance Officer, and DPO

Under the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, ByteFalcon Technologies designates the following Grievance Officer and Data Protection Officer:

Field	Details
Name	DPO
Designation	Data Protection Officer / Grievance Officer
Organisation	ByteFalcon Technologies Private Limited
Platform	Xenora (xenora.ai)
Email	dpo@bytefalcon.in
Address	21/22, Alandur Road, Aruliayamman Pettai 2nd Steet, Guindy Industrial Estate, Chennai-600032. Tamil Nadu, INDIA
Response SLA	Within 30 calendar days of receipt of a verifiable written request
Escalation	Data Protection Board of India (upon establishment under DPDPA 2023); relevant supervisory authority for EU/Gulf Data Principals

17. Policy Review, Amendment, and Enforcement

This Policy shall be reviewed at minimum annually, or upon any material change in applicable data protection legislation, a significant change in the Platform's data processing activities, or following a material security incident.

Amendments shall be notified to Tenants via the registered email address and published on the Xenora Platform website with a minimum of fourteen (14) days' notice prior to the effective date, except where immediate amendment is required by law or regulatory direction. Continued use of the Platform following the effective date constitutes the Tenant's acceptance of the updated Policy.

This Policy is issued by ByteFalcon Technologies Private Limited and is effective from April 15, 2026.