Data Processing Agreement

VizPass — visitor and gate management · BeyondBoxAI Technologies Pvt. Ltd.

Version 1.0 · Last updated: 8 September 2026

This Data Processing Agreement ("DPA") is between **BeyondBoxAI Technologies Pvt. Ltd.** ("we", "us", the *processor*) and the organisation that holds a VizPass account ("you", the *customer*). It forms part of the Terms of Service and applies whenever we process personal data inside your VizPass account on your behalf. Where this DPA and the Terms disagree on the handling of personal data, this DPA wins.

It is written to line up with the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025: you are the *data fiduciary* for the people recorded at your gates and for your own staff; we are the *data processor* acting on your instructions. It is not a contract for our own website and trial contacts — that is covered by the Privacy Policy, where we act as fiduciary ourselves.

1. Definitions

- **Customer Data** — every record you or your users put into your VizPass account, or that VizPass creates from them: visitor, driver, courier and contractor records, gate passes, photographs, identity details, vehicle numbers, material and delivery entries, host and staff accounts, and the activity log.
- **Personal data**, **data principal**, **data fiduciary**, **data processor** and **personal data breach** carry the meanings given in the DPDP Act, 2023.
- **Sub-processor** — a third party we engage to process Customer Data on our behalf. The current list is in Annex C.
- **Account owner** — the person whose email address created the account, or whoever you later nominate as the owner in settings. Notices under this DPA go to that address.

2. Who decides what

You decide what is collected at your gate, why, how long it is kept and who inside your organisation may see it. VizPass gives you the controls to make those decisions real: which fields are captured, whether ID and photo capture are on, the wording of the notice shown to

visitors, the retention period, and each user's role. We do not make those decisions for you and we do not use Customer Data for any purpose of our own — not for training, not for analytics sold to anyone, not for contacting the people in your register.

3. Our instructions from you

We process Customer Data only on your documented instructions. Your instructions are: (a) the Terms and this DPA; (b) the way you have configured your account; (c) actions your users take in the product; and (d) written requests you send to us. If we believe an instruction breaks the DPDP Act or another law that binds us, we will tell you before acting on it. We never act on an instruction from a visitor or a third party about your data; we route them to you.

4. What we undertake

1. **Confidentiality.** Only BeyondBoxAI staff who need access to operate or support the service can reach Customer Data, and each of them is bound by a written confidentiality obligation.
2. **Security.** We keep the technical and organisational measures in Annex B in place and do not weaken them during the term. We may improve them.
3. **Helping you answer people.** When a visitor or staff member asks you to access, correct or erase their record, VizPass lets you answer access and correction requests yourself: search the register, open the record, correct it, export what is held. Erasure of a single record before its retention date is done by us on your written request. For that, and for anything else the product does not expose, we act within **five working days**, free of charge unless the request is manifestly excessive.
4. **Helping you give notice.** Every account carries an editable visitor privacy notice. It is linked from the public check-in page, and each pass records the moment the visitor confirmed it together with a fingerprint of the exact wording in force. You are responsible for the wording; we are responsible for showing it and keeping the evidence.
5. **Breach notification.** Clause 8.
6. **Return and deletion.** Clause 9.
7. **Showing our work.** Clause 10.

8. **Sub-processors.** Clause 6. We stay responsible to you for anything a sub-processor does with Customer Data.

5. What you undertake

- You have a lawful basis for recording the people you record, and you tell them what you collect and why. The visitor notice in VizPass is a tool for that; review its wording before your first visitor and whenever you change what you capture.
- You collect only what your purpose needs. Every check-in field, including photograph and identity document, can be set to off, optional or required per form; leave off what your gate does not need.
- You set a retention period that matches your legal obligations, and you understand that records older than it are deleted automatically every night (clause 9).
- You give each user the role their job needs and remove access when someone leaves. Everything a user does under their login is treated as your instruction.
- You handle data-principal requests and Data Protection Board correspondence for your own account; we assist.

6. Sub-processors

You authorise the sub-processors listed in Annex C. We will give the account owner at least **30 days' notice by email** before adding or replacing a sub-processor that will handle Customer Data. If you object on reasonable data-protection grounds and we cannot offer an alternative, you may terminate the affected part of the service without penalty and export your data under clause 9. Features whose only purpose is to send data to a named provider (WhatsApp messaging, AI reading of an ID) touch your data only when you enable the channel or an operator uses the feature.

7. Where your data lives

The VizPass application, its database and its backups run on managed infrastructure in **Mumbai, India**. Customer Data does not leave Indian infrastructure in normal operation. Two exceptions exist, both under your control:

- **WhatsApp messages** — when you use WhatsApp for passes, host alerts or OTPs, the phone number and message content pass through Meta's WhatsApp Business platform,

whose infrastructure is not confined to India.

- **AI reading of an ID** — when an operator presses *Scan* on an identity document, that image is sent to the AI provider named in Annex C, whose servers are outside India, to pre-fill the name and number. Nothing is sent if the operator types the details instead, and nothing is saved until the operator confirms the form.

We make no other transfer of Customer Data outside India without your prior written instruction.

8. If something goes wrong

If we become aware of a personal data breach affecting Customer Data we will notify the account owner **without undue delay, and in any case within 72 hours** of becoming aware, and we will not wait for the investigation to finish before telling you. The notice will state, as far as we know at the time: what happened and when; which data and roughly how many people are affected; what we have done and are doing; and a named contact. We will update you as we learn more and give you what you need to notify the Data Protection Board and the affected people under the DPDP Rules. We do not notify the Board or data principals on your behalf unless you ask us to in writing. Where the affected data is data for which we are the fiduciary, we notify the Board ourselves.

9. Retention, export and deletion

- **While the account is open**, records are kept for the retention period you set in Company Settings (minimum 12 months, or “keep everything”). A nightly job deletes gate passes, delivery entries, visitor profiles that no longer have a pass, and their photographs and ID images once they pass that age. A visitor who is still checked in is never deleted. Each run is written to the activity log.
- **You can export at any time** — visitor, pass, courier, material and activity registers download as CSV from Reports without asking us.
- **When the account ends** (cancellation, non-renewal or termination), your export rights survive for a **30-day wind-down window**. After that window we delete the account's Customer Data, including files, within a further 30 days, save for anything the law requires us to retain. Nightly backups holding the deleted data expire within 14 days after that. We confirm deletion in writing on request.

10. Showing our work

Once a year, or after a breach affecting your data, you may ask us in writing for the information needed to demonstrate that we meet this DPA. We answer with written responses and supporting evidence (configuration, logs, this Annex B) within 30 days. If a written answer is genuinely insufficient, you or an independent auditor bound by confidentiality may audit the relevant systems at your cost, on at least 30 days' notice, during business hours, without disrupting other customers, and no more than once in any twelve months unless a breach has occurred.

11. Liability, term and law

Liability under this DPA is subject to clause 9 of the Terms. This DPA lasts as long as we hold any Customer Data for you, including the wind-down and deletion periods in clause 9, and survives termination of the Terms until deletion is complete. It is governed by the laws of India, and the courts at our registered office have exclusive jurisdiction.

12. Changes

We may update this DPA to reflect changes in the law, in our sub-processors or in the product. Material changes are notified to account owners by email before they take effect, and never reduce the protection you have during a paid term. The version number and date at the top identify the text; the version in force when you signed up is recorded on your account.

Annex A — Details of the processing

Subject matter	Operating a visitor and gate management service for your sites.
Duration	The term of your VizPass account, plus the wind-down and deletion periods in clause 9.
Nature and purpose	Recording who enters and leaves your premises; pre-registration and approval of visits; issuing passes; notifying hosts; recording deliveries and material movement; reporting; keeping an audit trail — all at your instruction.
Data principals	Visitors, drivers, couriers, contractors and other people arriving at your gate; your own employees and users of the account.

Categories of personal data	Name, mobile number, email, organisation, person visited, purpose, arrival and departure times, vehicle number, photograph, identity document type and number and image (where you switch capture on), delivery and material details, consent timestamp. For users: name, email, mobile, role, login and activity records.
Sensitive data	None is required by the product. Do not enter health, financial or biometric data into free-text fields; VizPass has no fields designed for them.

Annex B — Security measures

- **Tenant isolation.** Every record carries the company it belongs to, and every query is scoped to that company. One customer's users cannot reach another customer's register.
- **Encryption in transit.** HTTPS everywhere with HSTS (one-year max-age, subdomains included), a Content-Security-Policy, and hardened cookie settings (Secure, HttpOnly, SameSite=Lax).
- **Access control.** Seven roles and 57 individual permissions; a guard can check in a visitor without being able to export the history. Passwords are stored with bcrypt only. Sessions expire on inactivity.
- **Visitor-facing pages.** The public check-in page shows your privacy notice; the pass records the consent moment and the notice fingerprint.
- **Audit trail.** Actions in the system are written to an activity log that cannot be edited afterwards.
- **Retention enforcement.** A nightly purge applies each customer's retention period (Annex D shows where it is set) and logs what it removed.
- **Backups.** A compressed database backup is taken automatically every night and the most recent 14 days are kept on the same Indian infrastructure; a heartbeat records each run so a silent failure is visible. Restores are done on request, with the restore point confirmed first.
- **Operations.** Debug mode is off in production; application errors are logged for us and never shown to a visitor. Production access is limited to named BeyondBoxAI staff over key-based SSH.

- **What is not in place.** We do not hold ISO 27001 or SOC 2 certification, and we do not claim encryption of the database at rest beyond what the hosting provider applies to its storage. The security page keeps this list current.

Annex C — Sub-processors

These are the only third parties that handle Customer Data on our behalf. Entries marked *optional* receive data only when you switch the feature on.

Sub-processor	What it does for VizPass	Data it sees	Where
Hostinger International Ltd.	Hosting of the application, database and nightly backups; outbound platform email (SMTP).	All Customer Data at rest; email addresses and message content for platform email.	Mumbai, India (data centre); company registered in Cyprus.
Meta Platforms, Inc. (WhatsApp Business Platform) — *optional*	Delivery of gate passes, host alerts, OTPs and other WhatsApp messages you send from VizPass, through BeyondBoxAI's WhatsApp Business account.	Recipient phone number and message content.	Global (not confined to India).
Anthropic, PBC — *optional*	Reads an identity document image when an operator presses *Scan*, to pre-fill the check-in form.	The ID image for that one scan; not used for model training under the API terms.	United States.
Google LLC (Gemini API) — *optional*	As above, used when the first provider is unavailable.	As above.	United States.
Your own email provider — *optional*	If you configure your own SMTP mailbox in Company Settings, notifications go through it instead of ours.	Recipient addresses and message content.	Your choice; not our sub-processor.

Not sub-processors: Google Analytics and Cloudflare Turnstile run on our public marketing website only and never receive Customer Data from inside an account. No payment provider currently receives data from VizPass; online payment is not switched on.

Annex D — Where the controls are

Decision	Where you make it
Wording of the visitor privacy notice	Company Settings → Visitor privacy notice (shown at `/visit/<your-slug>/privacy`)
Retention period	Company Settings → Keep visitor records for (months)
Which fields are captured (photo, ID, vehicle…)	Visitors → Gate setup → Check-in form, per field: off / optional / required
Who can see and export what	Users → role per person
Export	Reports → any register → Download CSV
Avoid sending an ID image to an AI provider	Type the details in instead of pressing Scan on the check-in form
Correct one person's record	Visitors → open the record → Edit
Erase one person's record early	Write to us (Contact below); done within five working days

Contact

Data-protection matters under this DPA:

Amreesh Nehra, BeyondBoxAI Technologies Pvt. Ltd.

sales@beyondboxai.com · +91 81304 68801

The Corenthum, Tower B, 5th floor, Sector 62, Noida 201301