

Transit Technologies, LLC

California Privacy Rights Annex

Effective Date: 8/23/2026

Last Updated: 9/10/2026

This California Privacy Rights Annex ("Annex") supplements the Transit Technologies, LLC Enterprise Privacy Policy and applies solely to California residents ("consumers"). It is provided pursuant to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (together, the "CCPA"). Terms used in this Annex have the meanings given in the CCPA. Where information is processed on behalf of a customer (for example, a transit agency, employer, school, broker, or fleet operator), Transit Technologies acts as a "service provider," and requests concerning that information should be directed to the applicable customer as described in the Enterprise Privacy Policy.

Transit Technologies, LLC, together with its affiliates, subsidiaries, acquired entities, and branded platforms ("Transit Technologies," "we," "us," or "our"), is committed to protecting personal information. This Privacy Policy is the single enterprise privacy policy for Transit Technologies and its operating brands, including Bytecurve, busHive, CTS Software / TripMaster, Ecolane, FASTER Asset Solutions, MJM Innovations, Passio Technologies (including ParaPlan, Passio Navigator, Passio Connect, and Passio GO), TripShot, and Vestige (including Vestige View, Vestige GPS, and Persa Monitoring). References to any of these brands from their websites, applications, or services incorporate this Privacy Policy.

1. Notice at Collection

At or before the point of collection, we provide notice of the categories of personal information collected, the purposes for which they are used, whether they are sold or shared, and the retention criteria applied. This Annex, together with the Enterprise Privacy Policy, serves as our notice at collection for the services that link to it.

2. Categories of Personal Information

In the preceding 12 months, we have collected the following categories of personal information as defined by the CCPA. Sources, purposes, and disclosure recipients for each category are described in Sections 2, 3, and 5 of the Enterprise Privacy Policy.

Category	Collected	Notes: sources, purposes, disclosures
Identifiers (name, alias, postal address, email, phone, IP address, account name, device identifiers)	Yes	Collected from you, your organization, and automatically; disclosed to service providers, affiliates, and sponsoring organizations for business purposes.
Customer records (Cal. Civ. Code § 1798.80(e)) (contact details,	Yes	Collected from you; payment card data is handled by payment processors and not stored on our servers.

payment information processed by third-party gateways)		
Protected classifications (age, date of birth, gender, nationality, citizenship, disability-related information where submitted for eligibility or accommodation)	Yes	Collected only where you or your organization submit it for a requested service (e.g., paratransit eligibility); disclosed to service providers and the sponsoring customer.
Commercial information (products or services purchased or considered, product registration, warranty and service records)	Yes	Collected from you and your organization; disclosed to service providers and affiliates.
Internet or other electronic network activity (browsing, usage, log, email-interaction, and analytics data)	Yes	Collected automatically; disclosed to analytics and, on certain sites, advertising or data partners.
Geolocation data (precise or approximate location, GPS, vehicle location, boarding and offboarding events)	Yes	Collected where you or your organization enable location features; disclosed to service providers, sponsoring organizations, and transportation providers as needed to deliver the service.
Audio, electronic, visual, or similar information (support call or message content; in-vehicle camera or safety-system recordings where deployed)	Yes	Collected through support interactions and, in certain fleet-safety deployments, through in-vehicle systems administered by the customer.
Professional or employment-related information (employer, job details, career submissions)	Yes	Collected from you or your employer; disclosed to service providers.
Education information (school or campus affiliation in student-transportation deployments)	Yes	Generally processed on behalf of the customer as a service provider.
Sensitive personal information (account log-in credentials; precise geolocation; health, medical, and mobility information; government identification images submitted for verification)	Yes	Collected only as reasonably necessary for the requested service; see Section 4 of this Annex.
Inferences (preferences and product-interest profiles drawn from the above)	Yes	Derived internally for personalization and analytics.
Biometric information	Yes	Collected only in the VestigeView solution where you or your organization enable a feature including facial geometry.

3. Sale and Sharing of Personal Information

We do not sell personal information for monetary consideration, and we have no actual knowledge of selling or sharing the personal information of consumers under 16 years of age.

Certain of our websites work with online data or advertising partners that may associate site visits or logins with other personal information for marketing communications. This activity may constitute "sharing" for cross-context behavioral advertising under the CCPA. You may opt out at any time using the "Your Privacy Choices / Do Not Sell or Share My Personal Information" link in the footer of the applicable website, or by enabling an opt-out preference signal such as the Global Privacy Control ("GPC") in your browser. We honor GPC signals as an opt-out of sale/sharing for the browser or device sending the signal.

4. Sensitive Personal Information

We collect and use sensitive personal information only for the purposes permitted by the CCPA, including providing the services you or your organization request, verifying identity, maintaining security and integrity, preventing fraud, and complying with law. We do not use or disclose sensitive personal information to infer characteristics about consumers, and we do not use it for purposes that would require a "Right to Limit" notice under the CCPA. If our practices change, we will update this Annex and provide the required link.

5. Retention

We retain each category of personal information for as long as reasonably necessary for the purposes described in the Enterprise Privacy Policy, including providing services, complying with legal, tax, accounting, and contractual obligations, resolving disputes, and enforcing agreements. Retention criteria include the nature and sensitivity of the information, the purposes for which it was collected, applicable legal requirements, and customer-directed retention in hosted or managed environments.

6. Your California Rights

Subject to applicable exemptions, California residents have the right to:

- Know / Access: request the categories and specific pieces of personal information we have collected, the categories of sources, the purposes for collection, and the categories of third parties to whom it was disclosed
- Delete: request deletion of personal information we collected from you
- Correct: request correction of inaccurate personal information
- Opt out of sale or sharing: direct us not to sell or share your personal information
- Limit use of sensitive personal information: where applicable (see Section 4)
- Non-discrimination: exercise your rights free from discriminatory treatment

7. How to Submit a Request

You may submit a request to know, delete, or correct by:

- Email: privacy@transit.tech
- Toll-free: +1 855 313 4622

- [Data Subject Request](#)

We will confirm receipt within 10 business days and respond within 45 calendar days, which may be extended once by an additional 45 days where reasonably necessary, with notice to you. Requests to opt out of sale/sharing are honored within 15 business days.

Verification

We verify requests by matching information you provide against information we maintain. Depending on the sensitivity of the request, we may require additional verification, which for high-risk requests may include an image of government-issued identification, used solely for verification and then deleted. If we cannot verify your identity, we may deny the request and will explain why.

Authorized agents

You may designate an authorized agent to submit a request on your behalf. We may require the agent to provide proof of your written authorization or a valid power of attorney, and we may require you to verify your own identity directly with us.

8. Shine the Light

California Civil Code Section 1798.83 permits California residents to request certain information regarding disclosure of personal information to third parties for their direct marketing purposes. We do not disclose personal information to third parties for their own direct marketing purposes. California residents may make inquiries under this provision using the contact information in Section 7.

9. Contact

Questions about this Annex or our California practices may be directed to privacy@transit.tech or to the mailing address in the Enterprise Privacy Policy.