Logista Response Privacy Policy

Effective: Oct 29, 2026 **Last updated:** Oct 29, 2026 **Previous versions:** available on request to `privacy@logistaresponse.com`

Please read first. Logista Response (the "Service") is provided by Preston Solutions & Support LLC ("PSS," "we," "us," "our"). This Privacy Policy explains how we handle personal data when you visit our website, ask us about the Service, create an account, or use the Service. **When an organization (a "Customer") uses the Service to run its own emergency-response and inventory operations, that Customer — not us — decides how the data its people and partners enter into the Service is used. For that data we act as a Processor (Service Provider) on the Customer's behalf, and the Customer's own privacy policy and our Data Processing Addendum (DPA) govern it.** This Policy covers the personal data for which we decide the purposes and means (we act as a Controller): website visitors, prospects, account administrators, end users signing in to the Service, and the operational data we generate to run and secure it. This Policy is our single, comprehensive privacy disclosure, including jurisdiction-specific detail for EU/UK GDPR and US state law.

Table of contents

1. Who we are and what this Policy covers
2. Our privacy commitments
3. The personal data we collect
4. How we use personal data
5. How we share personal data
6. International data transfers
7. How long we keep personal data
8. Your privacy rights
9. Cookies and similar technologies
10. Sensitive personal information
11. Children's privacy
12. How we protect your data
13. Data breach notification
14. Changes to this Policy
15. How to contact us

1. Who we are and what this Policy covers

Who we are. Preston Solutions & Support LLC, a Texas limited liability company, operating the Service under the brand "Logista Response." Postal address: 330 Texoma Plains Dr, Conroe, TX 77304, USA.

What this Policy covers. Personal data we process as a **Controller** (under GDPR/UK GDPR) or **Business** (under CCPA/CPRA):

- Visitors to our website and people who contact us about the Service
- Account administrators and end users who sign in to the Service
- Operational data we generate (security logs, telemetry, support records)

What this Policy does not cover. Personal data a Customer enters into the Service about its own personnel, agents, sites, assets, or operations ("Customer Content"). For that data the Customer is the Controller and we act as a Processor / Service Provider on the Customer's documented instructions; the Customer's own privacy policy and our DPA govern it. If you are an end user of a

Customer's account and want to exercise rights over Customer Content, contact your organization's administrator; we will assist them as required.

2. Our privacy commitments

We hold ourselves to these principles for every piece of personal data we handle:

- **Lawfulness and transparency.** We process personal data only where we have a lawful basis, and we tell you how we use it.
- **Purpose limitation and minimization.** We collect only the data we need for a specific purpose, and we do not repurpose it for something incompatible.
- **No sale, no behavioral ads, no surprises.** We do not sell your personal information, and we do not share it for cross-context behavioral advertising. We do not use Customer data for marketing, profiling, or training AI/ML models.
- **Accuracy and your control.** We help you keep your data accurate and exercise your rights over it.
- **Security and accountability.** We protect personal data with the safeguards described in Section 12 and can demonstrate how we meet these commitments.

3. The personal data we collect

3.1 Website visitors and prospects

Category	Examples	When we collect it
Identifiers	Name, business email, employer, job title, phone	When you fill in a form, request a demo, subscribe, or contact us
Internet activity	IP address, browser type, operating system, pages viewed, referring URL, timestamps	Automatically when you visit the website
Inferences	Topics you've shown interest in, sales-funnel stage	Derived from the above

3.2 Account administrators and end users

Category	Examples	Source
Account profile	Name, work email, job title, phone and address (if entered), organization, group/site assignments, role, profile photo (if uploaded)	You or your Customer administrator
Authentication data	Hashed password (where a local password is used), OAuth/SSO identifiers, MFA enrolment status, session metadata	You and your identity provider
Activity logs	Login timestamps, source IP, actions taken in the Service, audit-trail records	Generated automatically

Support communications	Messages, screenshots, recordings you share with support	You, when you contact us

3.3 Data from third parties

- **Customer SSO providers** (Azure AD, Okta, Google Workspace, etc.) — the identifiers your provider releases (typically email, name, group claims), to authenticate you.
- **Error-monitoring vendor** (Sentry) — error messages, stack traces, and a browser/device fingerprint tied to an error event, to diagnose issues. We configure data-scrubbing to suppress form contents and known sensitive fields, and we do not send IP addresses.
- **Analytics vendor** (Amplitude) — de-identified product-usage events tied to a tenant identifier, to improve the Service.

4. How we use personal data

We use personal data for the purposes below. For visitors and users in the EEA, UK, and Switzerland, the “legal basis” column states the GDPR basis we rely on.

Purpose	Legal basis (GDPR)
Provide the Service: authenticate users, route requests, render the application	Performance of a contract; legitimate interests
Secure the Service: detect and respond to abuse, fraud, and security incidents	Legitimate interests; legal obligation (where applicable)
Provide customer support	Performance of a contract; legitimate interests
Communicate with you: service notices, security announcements, billing	Performance of a contract; legitimate interests
Marketing and prospect outreach (B2B)	Legitimate interests; consent where required by local law
Analytics and product improvement (de-identified, tenant-scoped)	Legitimate interests
Comply with legal obligations and enforce our terms	Legal obligation; legitimate interests

You can object to processing based on legitimate interests at any time — see Section 8.

5. How we share personal data

We share personal data only as described here.

Recipient	Purpose	Safeguards
Sub-processors (cloud hosting, error monitoring, analytics, transactional email, content delivery,	Operating and securing the Service	Bound as a “service provider”/“contractor” under CCPA/CPRA and by GDPR Article 28 terms; restricted from selling, sharing, or retaining data outside the contracted

geocoding, bot-detection)		purpose. The current list is in our Sub-processor List.
Customers	When you are an end user of a Customer's account, the Customer can see your activity within their tenant	The Customer's own privacy policy; our DPA
Professional advisors (lawyers, auditors, insurers)	Legal, audit, and risk management	Confidentiality obligations; only as needed
Authorities and law enforcement	When required by law or to protect rights, safety, or property	We assess every request and push back on overbroad requests where lawful
An acquirer or successor	As part of a merger, acquisition, financing, or sale of the business	Confidentiality during diligence; the recipient is bound by this Policy or a successor with no less protection

We do not sell personal information, and we do not share it for cross-context behavioral advertising as those terms are defined under the CCPA/CPRA. We do not knowingly sell or share the personal information of consumers under 16.

6. International data transfers

Our primary processing takes place in the United States (AWS, US West — Oregon, us-west-2), and stored personal data primarily resides in the United States. Some sub-processors process limited operational data outside the United States; the Sub-processor List gives per-vendor locations.

Where personal data is transferred from the EEA, UK, or Switzerland to a country without an adequacy decision, we rely on the EU Standard Contractual Clauses, the UK International Data Transfer Addendum, and the Swiss-recognized clauses, and we apply supplementary technical measures (encryption at rest with customer-managed keys; TLS 1.2+ in transit). We do not currently rely on the EU–US Data Privacy Framework. On request we will provide a copy of the relevant clauses (commercial terms redacted).

7. How long we keep personal data

We keep personal data only as long as necessary for the purposes in Section 4, or as required by law.

Category	Retention
Marketing-website analytics and prospect communications	Up to 3 years from last interaction, unless you ask us to delete sooner
Account profile and authentication data	For the life of the account. When an account is closed it is deactivated at once and anonymised within 90 days (in practice after a 30-day period in which an administrator can reverse an accidental closure). Anonymising overwrites the name, email, phone, address and job title, deletes the profile photo and the

	sign-in identity, and keeps the history of inventory movements intact under an anonymous name. Security audit logs that name the account are kept until they expire (see below), a deleted photo stays in storage version history for up to 180 days, and text people typed into the Service, such as notes and comments, is not changed.
In-application activity logs (the record of inventory movements and other actions users take in the Service)	Per the Customer's contracted retention period, with Customer Content
Customer Content	Per the Customer's contracted retention period; deleted within 30 days of Customer request following contract termination
Database backups (point-in-time recovery, and offsite copies)	35 days; deleted or anonymised records may persist within this immutable window and are unrecoverable thereafter
Support tickets	Up to 3 years after closure
Accounts created by single sign-on that are never added to an organization	Anonymised 90 days after creation
Security audit logs (sign-ins, sessions, access changes; includes email, source IP and browser)	400 days, in the database, its archive and the archive's offsite replica
Records of emails the Service sent	1 year
Application and access logs (server logs, including source IP)	365 days

When we no longer need personal data we delete or de-identify it. Where deletion isn't immediately feasible (for example, within the 35-day backup window), we isolate the data and let it expire.

8. Your privacy rights

Your rights depend on where you live and which laws apply.

8.1 Common rights (GDPR, UK GDPR, and most US state laws)

- **Access** — get a copy of the personal data we hold about you.
- **Correction** — have inaccurate data corrected.
- **Deletion** — have personal data deleted in defined circumstances. For an account, we anonymise it as described in Section 7, as soon as the request is verified rather than on the closure schedule.
- **Portability** — receive certain data in a portable format.
- **Restriction / Objection** — restrict or object to processing based on legitimate interests, including direct marketing.

- **Withdraw consent** — where we rely on consent, withdraw it at any time.
- **No solely-automated decisions** — we do not make decisions with legal or similarly significant effects about you using solely automated means.

8.2 EU / UK (GDPR)

We respond within **one month**, extendable by two months for complex requests (we'll tell you if we extend). You may also lodge a complaint with your supervisory authority — for the UK, the Information Commissioner's Office at ico.org.uk. You can reach our privacy team using the contact details in Section 15.

8.3 California (CCPA/CPRA) and other US states

California consumers have the rights to know, delete, correct, opt out of sale/sharing, limit the use of sensitive personal information, and non-discrimination. **We do not sell or share personal information**, so there is nothing to opt out of; if that ever changes we will add a "Do Not Sell or Share My Personal Information" link to our website. Residents of Colorado, Connecticut, Virginia, Utah, Texas, Oregon, Montana, Iowa, and similar states have comparable rights. We respond to verifiable US state-law requests within **45 days**, extendable by a further 45 days with notice.

8.4 How to exercise your rights

- **Email:** `privacy@logistaresponse.com`
- **Postal:** Preston Solutions & Support LLC, Attn: Privacy Requests, 330 Texoma Plains Dr, Conroe, TX 77304, USA

We will verify your identity before acting — typically by confirming you control the account email. If your request concerns Customer Content (where we are a Processor), we may refer it to the relevant Customer and will tell you when we do. If we decline a request in whole or in part, we will tell you why and how to appeal.

9. Cookies and similar technologies

Category	Purpose	Examples
Strictly necessary	Authentication, session, security	Session cookies; CSRF tokens
Functional / preferences	Remember language and UI choices	Theme/locale preferences
Analytics / performance	Understand usage so we can improve the Service	Amplitude (production-only, after sign-in; tenant-scoped)
Error monitoring	Diagnose application errors	Sentry (event identifier and stack trace; no advertising data)

We do not use advertising or behavioral-targeting cookies. You can control non-essential cookies through your browser. We honor the **Global Privacy Control (GPC)** signal as an opt-out of "sale"/"sharing"; because we do not sell or share, GPC confirms your existing posture. We do not currently respond to "Do Not Track" headers.

10. Sensitive personal information

We collect only a limited set of "sensitive personal information" (CCPA/CPRA), strictly to operate and secure the Service:

- **Account credentials** — hashed passwords, OAuth/SSO tokens, MFA enrolment data, and session identifiers, used solely to authenticate you and secure your account.
- **Precise geolocation** — only when a Customer enables location-verified check-in (a configurable per-site option), used solely to verify an end user is at the site they claim, and retained per the Customer's configuration.

We do **not** collect government identification numbers, financial account or payment-card data, biometric or genetic data, racial or ethnic origin, religious beliefs, union membership, health data, or sexual-orientation data. We do not use sensitive personal information to infer characteristics about you, and we use it only to provide the Service you or your Customer requested.

11. Children's privacy

The Service is a workforce/operational tool for emergency-response and inventory-management organizations. It is not directed to children under 16, and we do not knowingly collect personal data from children under 16. If you believe we have, contact `privacy@logistaresponse.com` and we will delete it. Customers operating in children's-services contexts are responsible for any parental/guardian consent required under COPPA or applicable state law before adding personnel under 16 to their account.

12. How we protect your data

We maintain administrative, technical, and physical safeguards designed to protect personal data, organized against the AICPA SOC 2 Trust Services Criteria. Highlights:

- **Encryption.** Customer-managed KMS keys protect production data stores; all transit uses TLS 1.2 or higher.
- **Access controls.** Production access uses short-lived federated tokens; sensitive operations require multi-factor authentication.
- **Threat detection.** Continuous monitoring with findings centralized in AWS Security Hub.
- **Audit trail.** API activity captured in AWS CloudTrail with log-file validation.

A fuller, customer-facing overview (*Logista Response — Security Controls Overview*) is available from your account team or `security@logistaresponse.com`. No security control is perfect, and we do not claim the Service is invulnerable to every possible threat.

13. Data breach notification

If we learn of a personal data breach affecting data we control, we will:

- **Notify the relevant supervisory authority within 72 hours** of becoming aware (GDPR Art. 33), unless the breach is unlikely to result in a risk to individuals' rights and freedoms.
- **Notify affected Customers without undue delay** — for breaches affecting Customer Content, by default within **48 hours of confirming impact**, unless a different timeline is set by the Customer's executed DPA.
- **Notify affected individuals** where required by law or where we determine notice is appropriate.

If you believe your account has been compromised, contact `security@logistaresponse.com` immediately.

14. Changes to this Policy

We may update this Policy from time to time. When we do, we will update the “Last updated” date, post the new Policy at the same URL, and — if the change is material — take reasonable steps to notify you in advance through the Service, by email, or by a banner on the website. You can request a previous version from `privacy@logistaresponse.com`.

15. How to contact us

For	Contact
Privacy questions and rights requests	`privacy@logistaresponse.com`
Security questions and vulnerability reports	`security@logistaresponse.com`
Legal notices	`legal@logistaresponse.com`
Postal	Preston Solutions & Support LLC, Attn: Privacy Requests, 330 Texoma Plains Dr, Conroe, TX 77304, USA

This Policy is provided for transparency and to satisfy our obligations under applicable privacy laws. It does not create or modify any contract between you and us. If you access the Service through a Customer, the Customer’s agreement with us governs the contractual aspects of your access. If any provision of this Policy conflicts with a written agreement signed by us and by you (or by the Customer), that signed agreement controls.

Revision history

Version	Date	Changes
1.0	2025-12-09	Privacy provisions originally issued as part of the PSS Data Privacy and Cybersecurity Policy.
2.0	2026-06-30	Issued as a standalone, external-facing Privacy Policy. Reconciled controller/processor split, data collected, sharing, international transfers, retention, rights deadlines, sensitive-PI scope, cookies, children, and breach-notification timelines.
2.1	2026-10-29	§3.2, §3.3, §7, §8.1: closed accounts are anonymised within 90 days instead of deleted, orgless single sign-on accounts after 90 days, and an erasure request at once; in-application activity logs follow the Customer’s contract; retention stated for security audit logs (400 days), email records (1 year) and application logs (365 days); backup window corrected from 31 to 35 days, including offsite copies; Sentry receives no IP addresses.