

TacApp

TacApp Technologies LLC · 8735 Dunwoody Place, STE N, Atlanta, GA 30350, United States · (770) 268-8830
tacapp.io · gettacapp.com · Effective: October 21, 2026 · Last updated: October 17, 2026

EXHIBIT A — DATA PROCESSING ADDENDUM

Exhibit A to the TacApp Terms of Service. How TacApp Technologies LLC processes personal information on behalf of a dealer. This Exhibit is part of the Terms of Service and takes effect with them, for every subscription, with no separate signature. A separately executed copy is available to any dealer whose own procedures require one — write to legal@tacapp.io.

1 • DEFINITIONS

Terms defined in the Terms of Service have the same meaning here.

"Applicable Privacy Law" means the California Consumer Privacy Act as amended by the California Privacy Rights Act, and every other United States state privacy law that applies to a dealer's processing of end-customer data.

"Business" / **"Controller"** means the dealer. **"Service Provider"** / **"Processor"** means TacApp.

"End-Customer Data" means personal information about a dealer's customers, and about other individuals whose information the dealer records, that TacApp processes on the dealer's behalf.

"Security Incident" means any actual or reasonably suspected unauthorized access to, acquisition of, disclosure of, alteration of, loss of, or destruction of End-Customer Data in TacApp's custody — including ransomware, accidental publication or misdirected transmission, and an outage that puts the integrity or recoverability of the data in doubt. It does not include unsuccessful attempts, pings, port scans, or similar events that do not compromise data.

"Subprocessor" means a third party engaged by TacApp to process End-Customer Data.

2 • ROLES

The dealer is the Business and Controller of End-Customer Data. The dealer decides what is collected in its tenant, for what purpose, and for how long within the limits of the Service.

TacApp is the Service Provider and Processor of End-Customer Data. TacApp processes it only on the dealer's documented instructions. The Terms of Service, this Addendum, and the dealer's configuration of the Service are the dealer's documented instructions. TacApp will tell the dealer if, in its opinion, an instruction violates Applicable Privacy Law.

TacApp is a Business and Controller in its own right for dealer account data, billing, support communications, its own websites, and its security operations. The Privacy Policy governs that processing; this Addendum does not.

3 • SCOPE OF PROCESSING

Subject matter	Provision of the white-label loyalty, messaging, booking, training, kiosk, waiver, and incident-record platform
-----------------------	---

Duration	The term of the dealer's subscription, plus the retention periods in Section 9 of the Privacy Policy
Nature and purpose	Hosting, storage, transmission, display, backup, security monitoring, and support, solely to provide the Service. The specific business purposes, listed because a general description is not enough, are: operating a loyalty program and its balances; taking and managing bookings; sending transactional and dealer-initiated messages; checking a customer in at a kiosk or a counter; presenting, versioning, and preserving signed waivers and acknowledgments; recording safety incidents and their evidence; maintaining a dealer's entry-restriction list; issuing and updating loyalty passes; delivering training content; and providing support to the dealer. TacApp processes End-Customer Data for no purpose outside this list
Categories of personal information	Identifiers; date of birth where a record depends on age; visit, booking, and engagement data; message content; signed waivers and acknowledgments; incident records and evidence photographs; entry restriction entries; loyalty pass name and membership code; device and technical data including notification tokens
Categories of individuals	The dealer's customers and members; guardians signing on behalf of minors; minors named in guardian-signed records; individuals named in or present at a recorded incident, including individuals with no account; the dealer's own staff acting in their roles

4 • RESTRICTIONS ON TACAPP

TacApp will not:

1. **sell** End-Customer Data, or **share** it for cross-context behavioral advertising, as those terms are defined in Applicable Privacy Law;
2. retain, use, or disclose End-Customer Data **for any purpose other than performing the Service** specified in the Terms of Service, including any commercial purpose of its own;
3. retain, use, or disclose End-Customer Data **outside the direct business relationship** between TacApp and the dealer;
4. **combine** End-Customer Data with personal information received from, or on behalf of, any other person, or collected from its own interactions with an individual, except as permitted by Applicable Privacy Law to perform a business purpose.

TacApp certifies that it understands the restrictions in this Section and will comply with them.

TacApp will notify the dealer promptly, and in any event within five (5) business days, if it determines that it can no longer meet its obligations under Applicable Privacy Law. On such a notice, and on any reasonable belief that TacApp is processing End-Customer Data in an unauthorized manner, **the dealer may direct TacApp to stop and to remediate, and TacApp will do so.**

Aggregated and de-identified data. TacApp may create data that is aggregated or stripped of identifiers, and use it as described in Section 16 of the Terms of Service. TacApp will maintain and use that data in de-identified form, will not attempt to re-identify it, and will bind any recipient to the same restriction.

5 • CONFIDENTIALITY OF PERSONNEL

TacApp limits access to End-Customer Data to personnel who need it to operate and support the Service. Those personnel are bound by written confidentiality obligations that survive the end of their engagement, receive training appropriate to their role, and have their access to customer records recorded.

6 • SECURITY MEASURES

TacApp maintains administrative, technical, and organizational measures appropriate to the risk, including at minimum:

- encryption of data in transit, and encryption and access controls for data at rest;
- logical isolation of each dealer's tenant;
- role-based access control and recorded access to customer records;
- separate storage for evidentiary records, where the application's key can add records but cannot read or delete them;
- backup with restore testing on a defined schedule;
- vulnerability management and logging appropriate to the Service.

Annex 1 describes how these measures are implemented. TacApp may change specific measures over time but **will not materially reduce the overall level of protection during a dealer's paid term.**

7 • SECURITY INCIDENT NOTIFICATION

TacApp will notify the affected dealer promptly, and in any event within seventy-two (72) hours after becoming aware of a Security Incident. "Becoming aware" means the point at which TacApp has a reasonable basis to believe one has occurred — not the point at which the investigation is complete. **Seventy-two hours is an outer limit, not a schedule.** Many states require a provider in TacApp's position to tell the dealer "immediately" on discovery, and the internal target in Annex 1 G is what makes that word mean something.

The first notice may be incomplete; it is sent when the clock requires, not when the facts are settled. It will describe what is known at the time: the nature of the incident, the categories and approximate volume of data involved, the likely consequences, and the measures taken or proposed. TacApp will provide updates as the investigation progresses.

Who notifies whom. The dealer gives the notices the law requires it to give to individuals and to regulators. TacApp assists with every one of them, and bears the cost where the incident arose in TacApp's systems. **TacApp gives a notice in its own name only where a statute places that duty on a service provider directly,** and tells the dealer before it does. Neither party's notice waits on the other, and TacApp will not make any public statement identifying the dealer without the dealer's prior written consent, unless required by law.

This Section decides whether a dealer is told, not state law. TacApp notifies the dealer of every Security Incident as defined in Section 1 — including one that is reasonably suspected, and an outage that puts recoverability in doubt — whether or not the dealer's state would require a notice of its own.

Where the dealer is a public body, and the law of its state sets a shorter period for notice to the owner of the data, that period applies instead of the seventy-two (72) hours above.

Notification is not an admission of fault by either party.

8 • SUBPROCESSORS

The dealer gives TacApp **general authorization** to engage Subprocessors, subject to this Section.

Current list. The categories of Subprocessors are set out in Section 8 of the Privacy Policy and are public. **TacApp provides the list of the specific Subprocessors to any dealer on request, at no charge, and to a prospective dealer under a confidentiality agreement.** That list is TacApp's Confidential Information under Section 11 of the Terms of Service, and a dealer receiving it may use it for its own compliance purposes and may disclose it to its own auditors and advisors under equivalent confidentiality. **Every Subprocessor stores production data in the United States.** Content delivery and push notification networks operate worldwide, so End-Customer Data may transit infrastructure outside the United States on its way to the device that requested it; **no Subprocessor stores production data outside the United States.**

Changes and objection. TacApp will give dealers **at least thirty (30) days' notice**, by email to the account contact and in the panel, before a new Subprocessor begins processing End-Customer Data. A dealer may object on reasonable grounds relating to data protection within that period. TacApp will work in good faith to resolve the objection; if it cannot, **the dealer may terminate the affected subscription and receive a pro-rata refund of prepaid fees for the unused remainder of the term.**

Flow-down and responsibility. Each Subprocessor is engaged under a written contract imposing obligations at least as protective as those in this Addendum. **TacApp remains fully responsible to the dealer for each Subprocessor's performance.**

9 • ASSISTANCE WITH INDIVIDUAL RIGHTS REQUESTS

Where an individual sends a rights request to TacApp that concerns a dealer's tenant, **TacApp will not respond on its own** except to tell the individual to contact the dealer, and will pass the request to the dealer promptly.

TacApp provides self-service tools in the panel for access, export, correction, and deletion. Where those tools are sufficient, dealers use them and no request to TacApp is needed.

Where they are not sufficient, TacApp will assist the dealer, taking into account the nature of the processing, so that the dealer can meet its statutory deadlines. TacApp will acknowledge such a request within five (5) business days and will provide the assistance within a period that leaves the dealer reasonable time to respond. Assistance is provided at no charge unless a request is manifestly excessive or repetitive, in which case TacApp will agree a reasonable fee in advance.

Limits. Deletion assistance does not extend to evidentiary records during their retention period, as described in Section 9 of the Privacy Policy and Section 11 below.

10 • ASSISTANCE WITH ASSESSMENTS AND AUDITS

TacApp will make available to the dealer the information reasonably necessary to demonstrate compliance with this Addendum, and will contribute to assessments required of the dealer by Applicable Privacy Law.

How. TacApp satisfies this by providing its current security documentation and, where available, the report of an independent third-party audit. **Where that is not sufficient for a dealer's legal obligation, the dealer may audit** — on thirty (30) days' notice, during business hours, no more than once in any twelve-month period, at the dealer's expense, under confidentiality, and without access to the data or systems of any other dealer. A dealer may also audit following a Security Incident affecting it, without regard to the annual limit.

11 • DELETION AND RETURN

During the subscription, the dealer may export its customer list and related records from the panel at any time, without charge.

After the subscription ends, TacApp keeps the tenant available for export for **at least thirty (30) days** — for any reason the subscription ended, including termination by TacApp for breach — then deletes End-Customer Data on its normal cycle: removed from active systems immediately, and from encrypted backups within thirty (30) days as those backups expire.

Evidentiary records are the exception, and it is deliberate. Signed waivers, acknowledgments, incident records, and their photographs remain in write-once storage for the retention period stated in Section 9 of the Privacy Policy — **at least ten (10) years, and longer where the record concerns a minor.** They cannot be deleted or altered during that period, including by TacApp, **except where deletion is compelled by a court order, by binding legal process, or by applicable law;** where that occurs TacApp will notify the affected dealer unless prohibited from doing so, and the deletion itself will be recorded.

The period runs from the record, not from the end of the subscription. Retention is set in the storage itself at the moment a record is written, and a record written in the first month of a subscription is as old as its own date, not as old as the account. **Where a record concerns a minor, it is kept until that person's twenty-sixth birthday or ten years from the record, whichever is later,** because in most states the period in which an injured child may bring a claim does not begin until they reach the age of majority. A retention period set this way can be extended. It is not shortened.

Legal hold. Where a record is the subject of a claim, an investigation, or a preservation request, TacApp places a hold on it that runs independently of the periods above and outlasts them. A hold is recorded, and it is released only on the dealer's written instruction or when the matter it relates to has ended.

The dealer may request a complete copy of its evidentiary records at any time, including after cancellation, at no charge. TacApp releases those records only on the dealer's written instruction or where required by law, and every release is recorded.

The dealer may also direct deletion. At the end of the subscription, or at any time after it, the dealer may elect in writing to take delivery of its complete evidentiary archive and to direct the deletion of TacApp's copy. TacApp delivers the archive at no charge, in a form that preserves each record's signature, its version, and the time it was written, then deletes its own copy and records the deletion. **A dealer that makes this election takes on the retention obligation itself.** Absent that election the period above applies, because a record kept by nobody is a defense available to nobody.

12 · CALIFORNIA-SPECIFIC TERMS

TacApp is a **Service Provider** with respect to End-Customer Data, as that term is defined in Cal. Civ. Code §1798.140(ag). The restrictions and the certification in Section 4 are given for the purposes of that section.

The disclosure of End-Customer Data by a dealer to TacApp is **not a sale and not a share**. TacApp receives no monetary or other valuable consideration for the data itself; it is paid a subscription fee for a service.

TacApp will comply with the applicable obligations of the CCPA, will provide the same level of privacy protection that the CCPA requires of a Business, and will cooperate with a dealer's reasonable steps to stop and remediate unauthorized use.

13 · GENERAL

Conflicts. If this Addendum conflicts with the Terms of Service on the handling of personal information, this Addendum controls.

Liability. The limitation of liability in Section 18 of the Terms of Service applies to claims under this Addendum. Nothing in this Addendum limits either party's obligations to individuals or to a regulator under Applicable Privacy Law.

Term. This Addendum applies for as long as TacApp processes End-Customer Data, and its Sections 4, 5, 7, 11, and 12 survive termination for as long as any End-Customer Data remains.

Changes. TacApp may update this Addendum to reflect changes in Applicable Privacy Law or in the Service, under Section 22 of the Terms of Service. A change that materially reduces a dealer's protections requires the dealer's consent.

Contact. privacy@tacapp.io · security@tacapp.io · TacApp Technologies LLC, 8735 Dunwoody Place, STE N, Atlanta, GA 30350, United States · (770) 268-8830. Section 25 of the Terms of Service lists every address and what each is for.

ANNEX 1 · TECHNICAL AND ORGANIZATIONAL MEASURES

This Annex describes how the measures in Section 6 are implemented. It is written from the system as built, not from intent: a measure appears here because it exists in the code or in a written procedure that is followed. It is updated when the implementation changes, under the commitment in Section 6 not to reduce protection during a paid term.

A · Access control

- **Roles.** Every account is one of: platform administrator; or, within a single dealer's tenant, owner, staff, or instructor. A role is scoped to one tenant; no dealer role reaches another tenant's data.
- **Platform administration.** The platform administrator account is created once, with a single-use bootstrap token that is retired after first use.
- **Server-to-server access.** Integrations authenticate with a dedicated integration token that is rotated with an overlap period, so a rotation never interrupts a running integration and a retired token stops working on a known date.

- **Kiosks.** Kiosk tablets authenticate as devices, on a separate path from user accounts, with device tokens that can be revoked individually. A kiosk is not a signed-in person.

B • Tenant isolation

Each dealer's data is scoped by tenant in the schema, and access rules at the database level enforce that scope independently of the application code. Entry restrictions and incident records are never aggregated across tenants (Terms of Service, Section 9).

C • Encryption and key management

- **Per-dealer keys.** Each dealer's sensitive material is protected under a key issued for that dealer alone. Dealer keys are wrapped with AES-256-GCM under a master key that lives only in the runtime environment — not in the codebase and not in the database. Rotating the master key re-wraps the dealer keys and touches no data; a single dealer's key can be rotated on its own.
- **Signature envelopes.** A signed waiver is sealed at intake to the key pair of the dealer it belongs to. The intake service that receives envelopes cannot read them; the identifier of the sealing key travels with each envelope, so a compromised key exposes one dealer's envelopes, not every dealer's.
- **Card data.** Payment card details go to the payment processor directly and are never held by TacApp.

D • Access logging

- **Access to contact details is recorded:** which account, whose record, which fields (telephone, email), in what context, and when. This is the log behind the "recorded access to customer records" commitment in Section 6 and in Section 10 of the Privacy Policy.
- **Administrative actions,** changes to a person's status, merges of duplicate records, message deliveries, and discount grants each have their own log.

E • Deletion

- **Cascade at the database.** Deleting a person's record removes the records that depend on it — bookings, consents, photographs, and that person's entries in the access log — by database constraint, not by application code that might miss a table.
- **Account closure** shows the person what will be removed, sends a confirmation to the address on the account, and allows a reversal window before the deletion runs.
- **Evidentiary records** are excluded, as Section 11 states, and the closure screen says so.

F • Vulnerability management

- **Release gate.** Every release passes a sixteen-stage gate that includes **at least thirty-one defensive checks** and **at least four hundred ninety-one automated test sets**, part of which run against a real database and a live server. A further **twenty-six checks** re-run independently in the continuous-integration service on every push. A failing stage stops the release; there is no override that lets a failing gate through, and the release writes nothing when a stage fails.
- **The figures above are minimums.** They are the counts in force when this Annex was issued, and they grow: every class of defect found once gets an automated check that runs on every change thereafter. They are not reduced.

- **Tenant isolation is tested, not asserted.** Isolation between dealers is enforced in the database independently of the application, and **eighty-eight isolation checks run against a real database on every release.**
- **No third-party packages.** The application servers carry no third-party dependencies beyond the database driver, which is held in our own repository rather than fetched from a package registry. There is no dependency tree to scan, and no upstream package whose compromise reaches the Service.
- **Independent review.** The codebase is reviewed by **two independent automated reviewers using different methods**, on a cadence of at least every thirty releases or twenty-one days, whichever comes first. Each pass also re-checks the fixes made after the previous pass. Every security fix carries a regression test that fails on the code before the fix. Each review is recorded with its date and the claims it verified by running them.
- **Dynamic testing.** The Service is additionally subjected to automated dynamic penetration testing against a staging environment, never against production.

G • Incident response

A written incident plan exists. It sets out the first hour — revoke credentials, record the time, cut the path in, establish the scope from the access log — who decides, and who acts if the owner is unreachable. Its internal target for notifying affected dealers is twenty-four hours, inside the seventy-two-hour commitment in Section 7, and the clock in both runs from becoming aware, not from confirmation.

H • Personnel

Every person with access to End-Customer Data is bound as Section 5 requires.