

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

PRIVACY POLICY

How TacApp Technologies LLC collects, uses, discloses, and retains personal information in connection with our websites, the dealer admin panel, branded customer applications, kiosk software, and related support and billing operations (together, the "Service").

Roles in plain terms. When a dealer uses TacApp, that dealer is our business customer. The dealer's own customers use the dealer's branded application. For those end-customer records the dealer is the controller (or "business") and TacApp is the processor (or "service provider") — except where we act as a controller for our own B2B accounts, billing, websites, and security operations. The Data Processing Addendum is what makes this binding rather than descriptive. This policy does not replace the privacy notice a dealer gives its own customers.

1 · WHO WE ARE

TacApp Technologies LLC operates a white-label loyalty, messaging, booking, training, and check-in platform for firearms retailers, shooting ranges, and training businesses.

Contact: privacy@tacapp.io · legal@tacapp.io · security@tacapp.io

2 · INFORMATION WE COLLECT

A. From dealers and their staff

- Account and profile data: name, business name, email, phone, role
- Billing and subscription data. Payment credentials are handled by our payment processors, not by us
- Business configuration: branding, locations, hours, offers, automations, content
- **Support communications**, including calls to our support line. **Where a call is recorded or transcribed, we say so in an announcement at the start of the call, before anyone speaks.** Several states require the consent of every party to a recording; the announcement is how we ask for it. If you would rather not be recorded, say so at the start and we will turn it off for that call. Recordings and call notes are used to handle the issue you called about and to keep a record of what was agreed, and for nothing else. **The support line is for dealers and their staff; we do not record calls with a dealer's own customers**

B. From end customers, processed on the dealer's behalf

- **Identifiers:** name, email, phone, loyalty or membership identifiers
- **Date of birth**, where a waiver, acknowledgment, or age-restricted activity depends on the signer's age. See "Why we hold a date of birth" below
- **Visit and engagement data** used for loyalty and messaging — check-in, class attendance, points balances, and limited application activity signals
- **Booking, waitlist, and event registration data**

- **In-app messages and offers**
- **Signed waivers and acknowledgments:** the document text, the version signed, the signature, and the supporting audit details described in Section 9
- **Range incident records:** a staff-written account of what occurred, the people involved or present — which may include individuals who hold no account with the dealer — and evidence photographs. Where photographs are attached, embedded technical metadata such as time and location is deliberately preserved, because it forms part of the record's evidentiary value. Incident records are append-only: entries may be added or corrected, never removed or overwritten. Incident records are not available in any tenant that has a location in Washington — see Section 14
- **Entry restrictions:** where a dealer maintains a list of individuals not permitted on its premises, we store the identifying details the dealer enters. **There is no field for the reason.** See Section 13
- Where a dealer runs youth or family activities, a parent or guardian may record a minor's name and date of birth as part of a guardian-signed waiver — see Section 12
- Optional training progress, certificates, and instructor notes the dealer chooses to use
- Device and technical data needed for sessions, security, and notification delivery: network (IP) address, browser and operating-system type, request logs, and the push notification token issued to a device by Apple or Google. Request logs follow the 90-day retention in Section 9. A notification token is deleted when you turn notifications off or remove the application. Data the customer application keeps on your own device is under your control: clearing site data or removing the application removes it, as the Cookie Policy describes
- **Loyalty passes in Apple Wallet or Google Wallet,** where a dealer issues them. A pass carries the customer's name and membership code and nothing else — no photograph, no date of birth

C. Identity document reading at the kiosk

Where a dealer enables it, the kiosk reads the barcode on a driver's license or state identification card to fill in a check-in or waiver.

The barcode contains far more than we take. The raw string never leaves the device: it is parsed on the tablet and discarded. We take three fields — **last name, first name, and date of birth** — and we read the expiration date only to warn staff that a document has expired, without storing it.

We do not take, transmit, or store the document number, the address, the physical description, the photograph, the license class, or any endorsement or restriction. **There is no field for them in the Service.** This is an architectural limit, not a setting.

Reading a driver's license electronically is regulated differently from state to state, and some states restrict which businesses may do it. **The feature is switched on or off per location, not per tenant,** because the law that applies is the law of the state where the kiosk stands: a dealer with locations in two states does not get one setting for both. It is off by default wherever our per-state list says reading is restricted, and in some states it can be enabled only where the visitor has been shown what is read and has been offered typing the information in instead. Whether to use it is the dealer's decision and the dealer's responsibility.

D. Why we hold a date of birth

Where a waiver or acknowledgment depends on the signer's age, we record the date of birth as part of that record, because **the age is part of what is being attested**. We do not use date of birth for marketing, for segmentation, or for any purpose outside the record it belongs to, and we do not keep it in a customer profile independent of that record.

E. What we do not collect from point-of-sale systems

Where a register is connected, we receive only what loyalty requires — typically transaction total, timestamp, and location context. **We do not collect or store itemized purchase contents, firearm serial numbers, ATF Form 4473 data, or bound-book / A&D entries.** This is an architectural limit, not a setting.

F. Websites and diagnostics

Standard server logs, security telemetry, and limited diagnostics required to operate and protect the Service.

3 · SOURCES OF INFORMATION

- Directly from dealers, staff, and end customers using forms or applications
- Automatically from devices and browsers
- From service providers supporting hosting, delivery, payments, and security
- From integrations the dealer enables, limited as described above

4 · HOW WE USE INFORMATION

- To provide, maintain, and secure the Service
- To run the loyalty, messaging, booking, training, kiosk, and waiver features the dealer configures
- To establish a record of safety-related events at a venue, and to help resolve or defend claims arising from them
- To bill subscriptions and prevent fraud or abuse
- To provide support, monitor reliability and security, comply with law, and enforce our agreements

We do not sell personal information, we do not share it for cross-context behavioral advertising, and we do not use end-customer data for a third-party advertising network.

5 · SENSITIVE PERSONAL INFORMATION

Some of what a dealer records can be sensitive personal information under California law and comparable state laws — in particular, an incident record that describes an injury.

We use sensitive personal information only for the purposes permitted by Cal. Civ. Code §1798.121: to perform the services the dealer has configured, to secure the Service and prevent fraud, and to maintain the quality and safety of the Service. **We do not use or disclose it to infer characteristics about anyone.** Because our use is limited to those permitted purposes, the right to limit the use of sensitive personal information does not apply to it; we will honor such a request if that ever changes.

Health-related information is also governed by Section 14 and by our Consumer Health Data Policy.

6 • ARTIFICIAL INTELLIGENCE

The Service does not include a generative artificial-intelligence feature that produces content for users inside the application. Customer data is not used to train AI models. If that ever changes, this section changes with it, before the feature is enabled.

7 • HOW WE DISCLOSE INFORMATION

- To the dealer that owns the relevant tenant, and to that dealer's authorized staff according to role permissions
- To service providers processing on our behalf (Section 8)
- Where required by law or valid legal process
- In connection with a business transfer, subject to appropriate protections
- With consent, where applicable

We do not disclose end-customer lists to manufacturers for the manufacturer's own marketing. Where a dealer enables sponsored knowledge-base materials inside its application, manufacturers receive no identifiable end-customer database from TacApp — only aggregate delivery counts. Sponsored materials are labeled as sponsored wherever they appear.

8 • SERVICE PROVIDERS AND SUBPROCESSORS

We disclose personal information to service providers — and to "contractors" under the CPRA, where applicable — under written contracts limiting use of the data to providing services to us. Categories include cloud hosting and infrastructure; database and file storage; the edge service that receives signed waivers before they reach evidentiary storage; evidentiary storage itself; content and media delivery; email and transactional messaging; mobile notification and wallet delivery; voice and support telephony; email infrastructure; payment processing; backup and disaster-recovery storage; and security, CDN, and network protection.

These disclosures are for business purposes. **They are not a "sale" or "share" of personal information for cross-context behavioral advertising under the CCPA or CPRA.**

Categories are public; the names are available on request. The categories above are the disclosure that privacy law requires, and they are public because they should be. The list of the specific providers behind them is our own operational and security information: we provide it in full to any dealer on request, and to a prospective dealer under a confidentiality agreement. **Every subprocessor stores production data in the United States.**

Changes. We give dealers at least **thirty (30) days' notice**, by email and in the panel, before a new subprocessor begins processing customer data. A dealer may object on reasonable grounds relating to data protection; if we cannot resolve the objection, the dealer may terminate the affected subscription and receive a pro-rata refund of prepaid fees. Subprocessors are bound by obligations at least as protective as those in our Data Processing Addendum, and we remain responsible for their performance.

United States storage. Production data is stored with providers in the United States, encrypted in transit and with appropriate encryption and access controls at rest. Storage used for customer content is private, never public. **No subprocessor stores production data**

outside the United States, and we will not move production storage of dealer data outside the United States without at least thirty (30) days' prior notice. Delivery networks are a different matter, and we would rather say so than let you discover it: the edge that serves a page and the services that carry a push notification to a phone operate worldwide, so a request from someone traveling abroad, or a notification on its way to a device, may pass through infrastructure outside the United States. **It is not stored there.**

9 • RETENTION

Category	Retention	Deletable on request
Dealer account and billing records	Life of the account, plus what tax, accounting and legal obligations require	Partly
Operational activity and behavioral logs	Deleted or anonymized on a rolling basis after 90 days, except where needed longer for security, dispute resolution, or legal hold	Yes
Loyalty balances, membership status, booking history	As needed for the dealer's operations, until deletion is requested or the account closes	Yes
Evidentiary records — signed waivers, acknowledgments, incident reports and their photographs	At least ten (10) years from the creation of the record, and longer where the record concerns a minor, in write-once storage	No — see below
Tenant data after a subscription ends	Available for export for at least 30 days, then deleted on the normal cycle	Yes
Encrypted backups	Rolling cycle; deleted data expires with the backup	By expiry

Two regimes, on purpose. Marketing and activity data is deleted because the less we hold, the less anyone can ask us for. Evidence works the other way: its value is that it outlives the period in which a claim can be brought.

Evidentiary records cannot be deleted or altered during their retention period, including by TacApp, except where deletion is compelled by a court order, by binding legal process, or by applicable law. Where that occurs, we will notify the affected dealer unless we are prohibited from doing so, and the deletion itself will be recorded. A deletion request does not otherwise extend to evidentiary records; all other personal information about the same individual is handled normally.

Where a record concerns a minor, we keep it until that person's twenty-sixth birthday, or ten years from the record, whichever is later. In most states the period in which an injured child may bring a claim does not begin to run until they reach the age of majority, so a record created when a child is eight can still be the only account of what happened eighteen years later. The period is set when the record is written, it can be extended, and it is not shortened.

Legal hold. Where a record is the subject of a claim, an investigation, or a preservation request, we place 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.

What deletion means elsewhere: when data is deleted, it is removed from active systems immediately, and from encrypted backups within thirty (30) days as those backups expire.

10 • SECURITY

We use administrative, technical, and organizational measures appropriate to the Service, including encryption in transit, access controls, tenant isolation, recorded access to customer records, and restore testing of backups on a schedule. Evidentiary storage is held separately from operational data, and the application's key to that storage can add records but cannot read or delete them.

If something goes wrong. We will notify the affected dealer promptly, and in any event **within seventy-two (72) hours** after becoming aware of a security incident — actual or reasonably suspected unauthorized access, disclosure, alteration, loss, or destruction of that dealer's customer data. We do not wait for the investigation to finish before the clock starts. The notice will describe what is known at the time, what we are doing, and what the dealer may need to do. We will provide updates as the investigation progresses and will assist the dealer with any notification the dealer is required to make.

No method of transmission or storage is completely secure.

11 • YOUR PRIVACY RIGHTS

Dealers and their staff

California ended the business-to-business exemption in 2023. If you are a dealer, an owner, or a member of a dealer's staff, and you are a California resident, you have the full set of consumer rights in relation to the information we hold about you as a controller — your account, billing, support, and website data.

Depending on where you live, you may have the right to:

- **know** what personal information we have collected, used, and disclosed about you
- **access** a copy of it, in a portable format
- **correct** it if it is inaccurate
- **delete** it, subject to the exceptions described in this policy and in law
- **opt out** of sale or sharing — we do neither
- **limit** the use of sensitive personal information — see Section 5
- **not be discriminated against** for exercising any of these rights

How to exercise them

Two ways, either is enough: email privacy@tacapp.io, or use the privacy request form in the dealer admin panel.

What happens next. We acknowledge a request **within 10 business days** and respond substantively **within 45 calendar days**. Where a request is complex we may extend once by a further 45 days, and we will tell you why before we do.

Verification. We verify that the request comes from you, using information we already hold. We ask for no more than we need, and we do not create an account to answer a request.

Authorized agents. You may use an authorized agent. We will ask the agent for proof of authorization and, unless the agent holds a power of attorney, we will confirm the request with you directly.

If we say no. We tell you which exception we relied on. **You may appeal** by replying to our decision or writing to privacy@tacapp.io with "Appeal" in the subject line. We respond to appeals within 45 days, and if we deny the appeal we will tell you how to contact your state attorney general.

End customers of a dealer

If you are a customer of a range, store, or training business that uses TacApp, **the dealer is the controller of your records** — contact the dealer that operates the application you use. We assist dealers with verified requests as required by contract and law.

Rights of deletion are subject to the evidentiary retention described in Section 9, which exists to preserve a record for the defense of legal claims. Health-related information is governed by Section 14, where different rules apply.

12 • MINORS

The Service is directed to businesses and to adult customers of firearms-related businesses.

TacApp does not permit accounts for children, and no part of the Service is directed to children.

Where a dealer's activity involves a minor — a youth class, or a range visit with a parent or guardian — the dealer may record the minor's name and date of birth as part of a guardian-signed waiver or an incident record. **That information is supplied by the adult signing on the minor's behalf, not collected from the child**, is used only for that record, and is subject to the retention in Section 9.

We do not knowingly collect personal information directly from children, and we do not use any information about a minor for marketing, profiling, or targeted content. If you believe a child has provided information to us directly, write to privacy@tacapp.io and we will delete it.

13 • ENTRY RESTRICTIONS

Where a dealer maintains a list of individuals not permitted on its premises, we store the identifying details the dealer enters. **We do not store why.** There is no field for a reason, and that is an architectural limit, not a setting: a free-text reason is where a health condition, a criminal allegation, or a protected characteristic would end up, and the safest place for that information is nowhere. The decision, its basis, and its lawfulness are the dealer's; TacApp neither makes nor reviews those decisions, and the kiosk never displays a restriction to the visitor — it alerts staff.

Entry restrictions never leave the dealer's tenant. A restriction a dealer records is visible only to that dealer's own authorized staff at that dealer's own locations. **TacApp does not aggregate restrictions across dealers, does not operate a shared or industry-**

wide list, and does not make restriction data available to any other dealer, to any third party, or to any product feature outside the tenant that created it. This is an architectural limit, not a setting.

14 · HEALTH-RELATED INFORMATION

An incident record can describe an injury. Washington and Nevada regulate that kind of information separately from general privacy law.

Washington. Incident records are **not available** in any tenant that has a location in Washington — in every location of that tenant, not only the Washington one. Washington's My Health My Data Act gives individuals a right to delete health-related information with no exception for the defense of legal claims, which cannot be reconciled with write-once evidentiary storage. Rather than weaken that storage, we do not offer the feature there.

Our **Consumer Health Data Policy** describes how health-related information is handled everywhere else, and what rights attach to it.

15 · OUTSIDE THE UNITED STATES

Primary processing and storage are in the United States. Accessing the Service from elsewhere means information is processed in the United States.

The Service is offered to businesses located in the United States and is not directed to individuals in the European Economic Area, the United Kingdom, or Switzerland. We do not target those markets, price in their currencies, or offer the Service in their languages. If we begin offering the Service in those markets, this policy will change before we do, and the additional rights and terms that apply there will be set out here.

16 · CHANGES

We may update this policy. The "Last updated" date will change, and where required we will give additional notice. Material changes affecting dealers are notified under Section 22 of the Terms of Service.

17 · CONTACT

TacApp Technologies LLC · 8735 Dunwoody Place, STE N, Atlanta, GA 30350, United States · (770) 268-8830

contact@tacapp.io is the main address. If none of the others obviously fits, use it — we will pass it to whoever should answer, and nothing is lost by starting there.

Write to	About
contact@tacapp.io	Anything not listed below, and anything you would otherwise have to guess about
support@tacapp.io	Something is broken, or you need help using the Service
billing@tacapp.io	Invoices, payments, refunds, plan changes, and renewals
legal@tacapp.io	This agreement, contracts, and formal notices

Write to	About
privacy@tacapp.io	Privacy requests, and questions about the information we hold
security@tacapp.io	Vulnerability reports and suspected unauthorized access
dmca@tacapp.io	Copyright notices and counter-notices under 17 U.S.C. §512
accessibility@tacapp.io	Something on TacApp blocks you. We answer within two business days

Writing to the wrong one is not a problem. These are routing conveniences, not a filter — a notice that has to reach us reaches us whichever address it arrives at.