PULSEID

Compliance whitepaper

Scanning IDs without taking on the liability.

How PulseID lets bars, nightclubs, restaurants and live-music venues check age and catch fake IDs while following each state's ID-scanning and privacy laws.

The short version. PulseID applies the law of the state where the location operates, keeps only what that state allows for as long as it allows, never builds a biometric profile, and never sells or shares a patron's data with another business.

1. A different law in every state
2. How PulseID handles it
3. What we collect, and no biometrics
4. Retention and state rules
5. Your flags stay yours
6. Patron rights and deletion
7. Security and access
8. What PulseID does not do
9. Summary

1. A different law in every state

Scanning a license at the door is no longer only an operational decision. Two kinds of law now apply:

- **ID-scanning laws.** A growing number of states limit what a business may do with data read from an ID: they cap how long it can be kept, restrict its use to age and identity checks, and in some states forbid keeping it at all.
- **Consumer-privacy laws.** States including California, Colorado, Connecticut, Minnesota and Virginia give residents the right to access, correct and delete their personal data, and to opt out of certain automated decisions.

These rules differ and sometimes conflict: a 30-day retention period that is fine in one state is unlawful in another. One nationwide policy is out of compliance somewhere. PulseID is built so that the software, not the door staff, sorts this out.

2. How PulseID handles it

The location's state decides

Compliance follows where the location operates, not which state issued the patron's ID. Each location's state sets its retention rules and permitted uses, and PulseID applies them without staff needing to know the statute.

Collect the minimum, keep it the shortest time

PulseID stores only what is needed to make and record the door decision, and deletes it on a schedule that state law caps. No marketing profile is ever built.

A person makes the call

Door staff see the result and decide. Scans that need judgment go to a manager, and every override is logged with a name and a reason. Deletion and access rights still apply to everything stored.

Your data stays yours

A location's scans and flags belong to that location. They are never sold, never used for advertising, and never pooled into a shared banned-patron list.

3. What we collect, and no biometrics

When a patron is scanned, PulseID reads the data in the PDF417 barcode (name, date of birth and age, license number, issuing state, expiration date, and the physical description on the card). When front capture is on, it also takes one compressed photo of the front of the ID. It records which location, which staff member, the time, and the door decision.

PulseID does not:

- create face templates, faceprints, fingerprints or any other biometric identifier;
- perform facial-recognition matching. The front photo is only a visual reference for staff to compare with the person in front of them, and the front check compares printed text with the barcode, never a face;
- collect anything from the patron's phone or device.

This matters legally: because PulseID never creates a biometric template, it stays outside strict biometric-privacy laws such as Illinois' BIPA.

4. Retention and state rules

Each location sets its own retention: 30 days for scans and one year for flags by default. A cleanup job runs every night. Scans older than the retention period are deleted, including the front photo, unless the scan is tied to an active flag at that location. Every deletion is written to an audit log.

On top of the location's setting, PulseID enforces stricter state rules automatically:

- **States that don't allow scan data to be kept.** PulseID does not store the name, date of birth, license number or raw barcode after the door decision. The check runs and the identifying data is discarded; only de-identified counts remain.
- **States that cap retention.** Scan data is deleted by the legal deadline even if the location set a longer period. The stricter rule always wins.

Even where scan data can't be kept, a location can keep de-identified counts, such as how many patrons fell into each age band on a given night. These carry no name, date of birth, license number or photo and

can't be linked back to anyone.

5. Your flags stay yours

A location's flags (warnings, bans and trespass orders) are visible only to that location and to other locations under the same ownership. PulseID runs no shared banned-patron network between businesses.

This is deliberate. A shared database used to refuse someone service can bring in the federal Fair Credit Reporting Act and similar state laws, turning a door tool into a regulated consumer-reporting activity. Keeping flags with the location (and its owner) keeps them the location's own business records.

6. Patron rights and deletion

PulseID is built around the Minnesota Consumer Data Privacy Act (Minn. Stat. Ch. 325M) and works with the privacy laws of California, Colorado, Connecticut, Virginia and other states. The location is the controller (it decides why and how long data is used) and PulseTech is the processor (it runs the software for the location).

A patron can use these rights by emailing **idprivacy@mypulsetech.com** with the location name, the approximate date and time of the scan, and the last four characters of the license number, so the record can be found. We honor verified requests from any state.

Requests go through a tracked deletion queue. An approved deletion removes the patron's scans, flags and patron record in one transaction, deletes the image files, and is written to the audit log. We respond within the time the patron's state requires, generally 45 days. In states where scan data isn't kept, there may be no individual record to retrieve or delete.

7. Security and access

Role	What they can do
Bouncer	One location. Scan IDs, see active flags and create flags. Editing flags is off unless the location turns it on. Cannot override a decision.
Manager	One location. Everything a bouncer can do, plus review held scans, edit and end flags, and override a deny. Every override needs a logged reason.
Location admin	One location. Everything a manager can do, plus staff, door policy, branding and billing.
PulseTech staff	All locations, for support and lawful requests only. Every access is audit-logged.

- **Servers PulseTech runs itself.** Data is hosted on PulseTech's own servers, not handed to a third-party hosting company.
- **Encrypted in transit.** All traffic between the apps and our servers uses HTTPS/TLS. The only outside provider that touches the data is Cloudflare, our network-security layer, which handles it in transit under its data-processing addendum and does not keep or sell it.
- **Locations kept apart.** Every record belongs to one location, and no location can see another business's scans or flags.
- **Audit logs.** Overrides, PulseTech staff access, retention deletions and deletion requests are all logged.

Not yet encrypted at rest. ID photos are protected by strict file permissions on access-controlled servers. Encryption at rest is planned for the next major version. We say so here rather than imply more than we ship.

8. What PulseID does not do

- No facial recognition and no biometric templates of any kind.
- No sharing of scans, flags or ban status with another business, and no shared banned-patron list.
- No selling of data, no advertising or marketing use, and no third-party analytics on patron data.
- No single nationwide policy: each location's state rules are applied automatically.

9. **Summary**

Question	How PulseID handles it
Which law applies	The law of the state where the location operates, applied automatically.
What is collected	Only what the door decision needs. Nothing from the patron's device, and no marketing profile.
Biometrics	None. No faceprints and no facial-recognition matching.
Retention	30 days for scans and one year for flags by default, deleted automatically, with stricter state caps or no-retention rules always winning.
Sharing	The location and its owner only. Never sold, and no network between businesses.
Patron rights	Access and deletion through a tracked queue, logged for audit.
Security	Role-based access, locations kept apart, TLS in transit, PulseTech-run servers, audit logs.

This whitepaper is general information about how PulseID is designed. It is not legal advice and does not guarantee compliance for any particular location. ID-scanning and privacy laws vary by state and change over time; locations should ask their own counsel about their obligations. Statutes named here are the frameworks PulseID is designed around, not a complete list.

© 2026 PulseTech · id.mypulsetech.com · idprivacy@mypulsetech.com · (208) 992-5045