VIVO CONTROL

SECURITY · 14 PAGES

The Resident Data Privacy Guide for Access Control Platforms

What data your access control platform collects, how it should be stored, who can access it, and what questions to ask any vendor before signing.

14 pages · 11 min read · PDF

INTRODUCTION

Why Privacy Matters for Access Control Specifically

An access control platform is one of the most data-intensive systems a property operates — it knows when residents come and go, who their frequent visitors are, sometimes what they look like on camera, and often personal details tied to their identity. Most property managers focus their evaluation on security features and cost, and treat data privacy as a footnote in the vendor's terms of service. That's a mistake, for both legal and practical reasons.

This guide walks through what an access control platform typically collects, how that data should be handled, who should and shouldn't have access to it, and the specific questions to ask any vendor before you sign a contract. It's written for property managers and board members, not privacy lawyers — but the topic does intersect with real legal obligations that vary by jurisdiction.

> **THIS IS NOT LEGAL ADVICE**
>
> Data privacy law — including rules on biometric data, data breach notification, and resident rights — varies significantly by jurisdiction and changes over time. This guide explains general concepts and practical due diligence steps, not what any specific law requires for your property. Confirm your specific obligations with legal counsel.

What Data Your Platform Actually Collects

Data Category	Typical Examples
Identity information	Name, unit number, email, phone number
Credential data	Mobile app account details, QR code history, fob/card numbers
Access logs	Timestamped records of every entry and exit at every access point
Video and photo data	Footage or still images from video intercoms and cameras, often tied to specific entry events
Device data	Phone type, app version, sometimes approximate location data if the app requests it
Payment data, if applicable	Billing information for any paid resident services processed through the platform

Ask any vendor for a complete list specific to their platform — this table covers common categories, but exact data collected varies by vendor and by which features a property actually uses.

A SENSITIVE CATEGORY

Biometric and Video Data Deserve Extra Attention

Video footage of a resident's face, and any biometric data such as facial recognition templates or fingerprint data, generally receives more legal protection than other categories of personal data in many jurisdictions. Some places have specific biometric privacy statutes with requirements around consent, notice, and retention that go beyond general data protection rules.

- **Confirm whether your platform uses facial recognition or simply stores video footage.** These are meaningfully different from a privacy standpoint — recognition technology that extracts a biometric template from a face is treated differently than a video clip in most frameworks.
- **Ask whether biometric data (if collected) is stored separately from other resident data,** and what specific security measures protect it.
- **Confirm consent and notice practices** — residents should generally know if biometric data is being collected, and in many jurisdictions, affirmative consent may be legally required.
- **Ask specifically about retention timelines for video and biometric data,** since these often carry different (and often shorter) retention rules than standard access logs.

If your platform uses any biometric feature, confirm the specific legal requirements that apply in your jurisdiction with counsel before deployment — this is one of the areas where general guidance is least sufficient.

How Resident Data Should Be Stored

- **Encryption in transit,** meaning data is encrypted while moving between a resident's device, the panel, and the cloud platform — ask specifically what standard is used (see our WebRTC guide for the video-call-specific version of this question).
- **Encryption at rest,** meaning stored data itself is encrypted, not just protected by account login credentials — ask whether this applies to video footage specifically, since it's often the largest and most sensitive data category.
- **Data residency,** meaning where servers physically or logically store your resident data — some properties and jurisdictions have specific requirements or preferences about data staying within a particular country or region.
- **Access controls on the vendor's side,** meaning role-based restrictions on which of the vendor's own employees can view resident data, and audit logging of when they do.
- **Backup and disaster recovery practices,** which matter both for data availability and for confirming there isn't an unsecured backup copy sitting outside the vendor's primary security controls.

Who Can Access Resident Data — Internal Roles

Resident data access should follow the same role-based principle covered in our Multifamily Operator's Playbook — access limited to what a specific role actually needs, not broad access by default.

Role	Typical Data Access Need
Property management staff	Access logs and resident contact info for their specific property
Regional/corporate staff (portfolio operators)	Aggregated or cross-property data, per your platform's role permissions
On-site guard/front desk staff	Real-time entry activity, typically without full historical export access
Vendor's support staff	Limited, audited access for troubleshooting — confirm this is logged and restricted
Vendor's engineering staff	Should generally be the most restricted internal category, given broad system-level access potential

Ask your vendor to walk through their internal access control model specifically — a platform that carefully controls resident-facing permissions but has poorly controlled internal employee access hasn't actually solved the privacy problem.

Who Can Access Resident Data — Third Parties and Legal Requests

- **Subprocessors and integration partners.** Ask which third-party services (cloud hosting, analytics, payment processing) have any access to resident data, and confirm they're bound by comparable privacy and security obligations.
- **Law enforcement and legal requests.** Ask what process the vendor follows when law enforcement or a court requests resident data — a vendor with a clear, documented policy is generally preferable to one with no stated process.
- **Data sharing with marketing or advertising partners.** Confirm resident data is not sold or shared for advertising purposes — this should be explicitly addressed in the vendor's privacy policy, not just assumed.
- **Data use for the vendor's own product improvement.** Ask whether resident data (even anonymized or aggregated) is used to train models or improve the platform, and whether you can opt out.
- **What happens in a merger, acquisition, or bankruptcy.** Confirm the privacy policy addresses what happens to resident data if the vendor company changes ownership.

Data Retention and Deletion Practices

- **Ask for specific retention periods** by data category — access logs, video footage, and account information often have different default retention windows.
- **Confirm what happens when a resident moves out.** Ask specifically whether their data is deleted, anonymized, or retained, and for how long, after their credential is deactivated.
- **Confirm what happens if you cancel the platform entirely.** This is a common gap — ask directly what happens to years of accumulated resident data if your property switches vendors (see our Switching from ButterflyMX guide for how this plays out in a real migration).
- **Ask whether deletion requests are actually honored on a specific timeline,** and whether "deleted" means removed from active systems only, or also from backups within a reasonable period.

Balance retention against the liability documentation needs covered in our Access Control and Liability guide — there's a genuine tension between minimizing data retention for privacy and retaining enough for security and legal documentation, and the right balance depends on your specific circumstances and counsel's guidance.

Resident Rights — General Concepts

Many data protection frameworks around the world grant individuals some version of the following rights over their own data, though the specifics, applicability, and enforcement mechanisms vary significantly by jurisdiction:

- **Right to access** — the ability to request a copy of what data is held about them.
- **Right to correction** — the ability to request that inaccurate data be corrected.
- **Right to deletion** — the ability to request that data be deleted, subject to legal retention exceptions.
- **Right to know how data is used and shared** — generally addressed through a privacy notice or policy.

Whether these rights apply as a legal requirement for your specific property depends on your jurisdiction and the applicable framework there — this section describes commonly recognized concepts, not a specific obligation. Confirm with legal counsel which rights, if any, are legally required for your residents, and build your resident-facing privacy notice (see page 12) accordingly.

BEFORE YOU SIGN

Vendor Due Diligence — Questions to Ask

1. What specific data does your platform collect, and can you provide a complete list broken down by category?
2. Is data encrypted both in transit and at rest? What specific encryption standards are used?
3. Where is resident data physically or logically stored, and does that meet any data residency requirements relevant to our property?
4. What is your internal employee access control model, and is employee access to resident data logged and audited?
5. Do you use facial recognition or collect any biometric data, and if so, what specific consent and retention practices apply?
6. What are your specific data retention periods by category, and what happens to our data if we cancel the contract?
7. Do you share or sell resident data to any third party, including for advertising or analytics purposes?
8. What is your data breach notification process, and what is your track record, if any, with prior incidents?
9. Can you provide your privacy policy and data processing terms in writing, ahead of a signed contract, for our legal counsel to review?

WATCH FOR THESE

Privacy Policy Red Flags

- **Vague or missing data retention periods.** "We retain data as long as necessary" without a specific timeframe makes it impossible to plan your own privacy practices around theirs.
- **Broad, undefined rights to share data with "partners."** Without a specific, limited list of what kinds of partners and for what purposes, this language can cover far more than a property manager might expect.
- **No mention of encryption standards at all,** or vague claims like "industry-standard security" without specifics.
- **No stated process for data deletion upon contract termination.** If a privacy policy doesn't address what happens to your data if you leave, ask directly before assuming the answer favors you.
- **No specific breach notification commitment or timeline.** A vendor should be able to state, in writing, how and when they'll notify you if resident data is compromised.

YOUR RESPONSIBILITY

Building Your Own Property Privacy Notice

Even with a privacy-conscious vendor, your property generally has its own responsibility to inform residents about the access control system's data practices. A short, plain-language notice — not necessarily a formal legal document — typically covers:

- [x] What data the access control system collects about residents and visitors
- [x] Why it's collected (security, access management, audit trail)
- [x] Who can access it (your property's staff, and at a high level, the vendor)
- [x] How long it's generally retained
- [x] Who to contact with questions or a data-related request

Have legal counsel review your final notice, particularly if your jurisdiction has specific disclosure requirements — but starting with this outline gives your attorney a concrete draft to refine rather than a blank page.

BRING THIS TO YOUR VENDOR EVALUATION

Checklist and Key Takeaways

- [x] Requested a complete list of data categories collected by any platform under evaluation
- [x] Confirmed encryption standards for data in transit and at rest, specifically for video footage
- [x] Asked whether biometric data or facial recognition is used, and reviewed applicable requirements with counsel
- [x] Reviewed the vendor's internal employee access control model
- [x] Confirmed data retention periods by category, and what happens at contract termination
- [x] Asked the nine due diligence questions from page 10 directly, in writing
- [x] Reviewed the vendor's privacy policy for the red flags on page 11
- [x] Drafted or updated a resident-facing privacy notice for our property

Privacy and security are related but distinct — a platform can have excellent access control security and still handle resident data poorly, or vice versa. Evaluate both explicitly, and don't assume one implies the other.

VIVO CONTROL

Ask Us These Questions Directly

We're glad to walk through our data handling, encryption, retention, and access control practices in detail — bring the checklist from this guide to your demo.

Book a Free Demo →

---

www.vivocontrol.com/en/demo/ · hello@vivocontrol.com ·