

SEGURIDAD · 14 PÁGINAS

Guía de Privacidad de Datos de Residentes para Plataformas de Control de Acceso

Qué datos recolecta tu plataforma de control de acceso, cómo debe almacenarse, quién puede acceder a ella, y qué preguntas hacer a cualquier proveedor antes de firmar.

14 páginas · 11 min de lectura · PDF

Por Qué la Privacidad Importa Específicamente para el Control de Acceso

Una plataforma de control de acceso es uno de los sistemas más intensivos en datos que opera una propiedad — sabe cuándo entran y salen los residentes, quiénes son sus visitantes frecuentes, a veces cómo se ven en cámara, y a menudo detalles personales ligados a su identidad. La mayoría de los administradores de propiedades enfocan su evaluación en funciones de seguridad y costo, y tratan la privacidad de datos como una nota al margen en los términos de servicio del proveedor. Eso es un error, tanto por razones legales como prácticas.

Esta guía recorre qué recolecta típicamente una plataforma de control de acceso, cómo deben manejarse esos datos, quién debería y no debería tener acceso a ellos, y las preguntas específicas que debes hacer a cualquier proveedor antes de firmar un contrato. Está escrita para administradores de propiedades y miembros de junta, no para abogados de privacidad — pero el tema sí se cruza con obligaciones legales reales que varían según la jurisdicción.

ESTO NO ES ASESORÍA LEGAL

La ley de privacidad de datos — incluyendo reglas sobre datos biométricos, notificación de brechas de datos, y derechos de los residentes — varía significativamente según la jurisdicción y cambia con el tiempo. Esta guía explica conceptos generales y pasos prácticos de debida diligencia, no lo que requiere alguna ley específica para tu propiedad. Confirma tus obligaciones específicas con un asesor legal.

Qué Datos Recolecta Realmente Tu Plataforma

Categoría de Datos	Ejemplos Típicos
Información de identidad	Nombre, número de unidad, correo, teléfono
Datos de credencial	Detalles de cuenta de app móvil, historial de código QR, números de fob/tarjeta
Registros de acceso	Registros con fecha/hora de cada entrada y salida en cada punto de acceso
Datos de video y foto	Grabaciones o imágenes de intercomunicadores de video y cámaras, a menudo ligadas a eventos de entrada específicos
Datos del dispositivo	Tipo de teléfono, versión de la app, a veces datos de ubicación aproximada si la app lo solicita
Datos de pago, si aplica	Información de facturación para cualquier servicio de residente pagado procesado a través de la plataforma

Pide a cualquier proveedor una lista completa específica de su plataforma — esta tabla cubre categorías comunes, pero los datos exactos recolectados varían según el proveedor y qué funciones use realmente una propiedad.

Los Datos Biométricos y de Video Merecen Atención Extra

Las grabaciones de video del rostro de un residente, y cualquier dato biométrico como plantillas de reconocimiento facial o datos de huella digital, generalmente reciben más protección legal que otras categorías de datos personales en muchas jurisdicciones. Algunos lugares tienen leyes específicas de privacidad biométrica con requisitos alrededor del consentimiento, aviso, y retención que van más allá de las reglas generales de protección de datos.

- ✓ **Confirma si tu plataforma usa reconocimiento facial o simplemente almacena grabaciones de video.** Estas son significativamente distintas desde el punto de vista de privacidad — la tecnología de reconocimiento que extrae una plantilla biométrica de un rostro se trata de forma distinta a un clip de video en la mayoría de los marcos legales.
- ✓ **Pregunta si los datos biométricos (si se recolectan) se almacenan por separado de otros datos del residente,** y qué medidas de seguridad específicas los protegen.
- ✓ **Confirma las prácticas de consentimiento y aviso** — los residentes generalmente deben saber si se están recolectando datos biométricos, y en muchas jurisdicciones, el consentimiento afirmativo puede ser un requisito legal.
- ✓ **Pregunta específicamente sobre los plazos de retención para datos de video y biométricos,** ya que a menudo tienen reglas de retención distintas (y a menudo más cortas) que los registros de acceso estándar.

Si tu plataforma usa alguna función biométrica, confirma los requisitos legales específicos que aplican en tu jurisdicción con un asesor legal antes del despliegue — esta es una de las áreas donde la orientación general es menos suficiente.

Cómo Deben Almacenarse los Datos de Residentes

- ✓ **Cifrado en tránsito**, lo que significa que los datos están cifrados mientras se mueven entre el dispositivo de un residente, el panel, y la plataforma en la nube — pregunta específicamente qué estándar se usa (consulta nuestra guía de WebRTC para la versión específica de esta pregunta aplicada a videollamadas).
- ✓ **Cifrado en reposo**, lo que significa que los datos almacenados en sí están cifrados, no solo protegidos por credenciales de inicio de sesión de cuenta — pregunta si esto aplica específicamente a las grabaciones de video, ya que a menudo es la categoría de datos más grande y sensible.
- ✓ **Residencia de datos**, lo que significa dónde almacenan física o lógicamente los servidores los datos de tus residentes — algunas propiedades y jurisdicciones tienen requisitos o preferencias específicas sobre que los datos permanezcan dentro de un país o región particular.
- ✓ **Controles de acceso del lado del proveedor**, lo que significa restricciones basadas en roles sobre cuáles empleados del propio proveedor pueden ver los datos de residentes, y el registro de auditoría de cuándo lo hacen.
- ✓ **Prácticas de respaldo y recuperación de desastres**, lo cual importa tanto para la disponibilidad de datos como para confirmar que no existe una copia de respaldo sin protección fuera de los controles de seguridad principales del proveedor.

Quién Puede Acceder a los Datos de Residentes — Roles Internos

El acceso a los datos de residentes debe seguir el mismo principio basado en roles cubierto en nuestro Playbook del Operador Multifamily — acceso limitado a lo que un rol específico realmente necesita, no acceso amplio por defecto.

Rol	Necesidad Típica de Acceso a Datos
Personal de administración de la propiedad	Registros de acceso e información de contacto de residentes para su propiedad específica
Personal regional/corporativo (operadores de portafolio)	Datos agregados o entre propiedades, según los permisos de roles de tu plataforma
Personal de guardia/recepción en sitio	Actividad de entrada en tiempo real, típicamente sin acceso completo de exportación histórica
Personal de soporte del proveedor	Acceso limitado y auditado para resolución de problemas — confirma que esto se registre y restrinja
Personal de ingeniería del proveedor	Generalmente debería ser la categoría interna más restringida, dado el amplio potencial de acceso a nivel de sistema

Pide a tu proveedor que explique específicamente su modelo interno de control de acceso — una plataforma que controla cuidadosamente los permisos orientados al residente pero tiene un acceso de empleados internos poco controlado no ha resuelto realmente el problema de privacidad.

Quién Puede Acceder a los Datos de Residentes — Terceros y Solicitudes Legales

- ✓ **Subprocesadores y socios de integración.** Pregunta qué servicios de terceros (hosting en la nube, análisis, procesamiento de pagos) tienen algún acceso a los datos de residentes, y confirma que estén sujetos a obligaciones comparables de privacidad y seguridad.
- ✓ **Solicitudes de las autoridades y legales.** Pregunta qué proceso sigue el proveedor cuando las autoridades o un tribunal solicitan datos de residentes — un proveedor con una política clara y documentada generalmente es preferible a uno sin ningún proceso declarado.
- ✓ **Compartir datos con socios de marketing o publicidad.** Confirma que los datos de residentes no se vendan ni compartan para fines publicitarios — esto debería abordarse explícitamente en la política de privacidad del proveedor, no simplemente asumirse.
- ✓ **Uso de datos para la mejora del propio producto del proveedor.** Pregunta si los datos de residentes (incluso anonimizados o agregados) se usan para entrenar modelos o mejorar la plataforma, y si puedes optar por no participar.
- ✓ **Qué pasa en una fusión, adquisición, o quiebra.** Confirma que la política de privacidad aborde qué pasa con los datos de residentes si la empresa proveedora cambia de propietario.

Prácticas de Retención y Eliminación de Datos

- ✓ **Pide plazos de retención específicos** por categoría de datos — los registros de acceso, las grabaciones de video, y la información de cuenta a menudo tienen ventanas de retención por defecto distintas.
- ✓ **Confirma qué pasa cuando un residente se muda.** Pregunta específicamente si sus datos se eliminan, anonimizan, o conservan, y por cuánto tiempo, después de que se desactive su credencial.
- ✓ **Confirma qué pasa si cancelas la plataforma por completo.** Esta es una brecha común — pregunta directamente qué pasa con años de datos de residentes acumulados si tu propiedad cambia de proveedor (consulta nuestra guía Cambiando desde ButterflyMX para ver cómo se desarrolla esto en una migración real).
- ✓ **Pregunta si las solicitudes de eliminación realmente se cumplen en un plazo específico,** y si "eliminado" significa removido solo de los sistemas activos, o también de los respaldos dentro de un período razonable.

Equilibra la retención contra las necesidades de documentación de responsabilidad cubiertas en nuestra guía de Control de Acceso y Responsabilidad — existe una tensión genuina entre minimizar la retención de datos por privacidad y conservar suficiente para documentación de seguridad y legal, y el equilibrio correcto depende de tus circunstancias específicas y la orientación de tu asesor legal.

Derechos de los Residentes — Conceptos Generales

Muchos marcos de protección de datos alrededor del mundo otorgan a los individuos alguna versión de los siguientes derechos sobre sus propios datos, aunque los detalles, aplicabilidad, y mecanismos de cumplimiento varían significativamente según la jurisdicción:

- ✓ **Derecho de acceso** — la capacidad de solicitar una copia de qué datos se tienen sobre ellos.
- ✓ **Derecho de corrección** — la capacidad de solicitar que se corrijan datos inexactos.
- ✓ **Derecho de eliminación** — la capacidad de solicitar que se eliminen los datos, sujeto a excepciones legales de retención.
- ✓ **Derecho a saber cómo se usan y comparten los datos** — generalmente abordado a través de un aviso o política de privacidad.

Si estos derechos aplican como requisito legal para tu propiedad específica depende de tu jurisdicción y el marco legal aplicable ahí — esta sección describe conceptos comúnmente reconocidos, no una obligación específica. Confirma con un asesor legal qué derechos, si alguno, son legalmente requeridos para tus residentes, y construye tu aviso de privacidad orientado al residente (ver página 12) en consecuencia.

Debida Diligencia de Proveedor — Preguntas para Hacer

1. ¿Qué datos específicos recolecta su plataforma, y pueden proporcionar una lista completa desglosada por categoría?
2. ¿Los datos están cifrados tanto en tránsito como en reposo? ¿Qué estándares de cifrado específicos se usan?
3. ¿Dónde se almacenan física o lógicamente los datos de residentes, y eso cumple con algún requisito de residencia de datos relevante para nuestra propiedad?
4. ¿Cuál es su modelo interno de control de acceso de empleados, y el acceso de empleados a datos de residentes se registra y audita?
5. ¿Usan reconocimiento facial o recolectan algún dato biométrico, y si es así, qué prácticas específicas de consentimiento y retención aplican?
6. ¿Cuáles son sus plazos específicos de retención de datos por categoría, y qué pasa con nuestros datos si cancelamos el contrato?
7. ¿Comparten o venden datos de residentes a algún tercero, incluyendo para fines de publicidad o análisis?
8. ¿Cuál es su proceso de notificación de brechas de datos, y cuál es su historial, si alguno, con incidentes previos?
9. ¿Pueden proporcionar su política de privacidad y términos de procesamiento de datos por escrito, antes de firmar un contrato, para que nuestro asesor legal los revise?

Señales de Alerta en la Política de Privacidad

- ✓ **Plazos de retención de datos vagos o inexistentes.** "Conservamos los datos tanto tiempo como sea necesario" sin un plazo específico hace imposible planificar tus propias prácticas de privacidad en función de las tuyas.
- ✓ **Derechos amplios y no definidos para compartir datos con "socios".** Sin una lista específica y limitada de qué tipos de socios y para qué propósitos, este lenguaje puede cubrir mucho más de lo que un administrador de propiedades podría esperar.
- ✓ **Ninguna mención de estándares de cifrado en absoluto,** o afirmaciones vagas como "seguridad estándar de la industria" sin especificaciones.
- ✓ **Ningún proceso declarado para la eliminación de datos al terminar el contrato.** Si una política de privacidad no aborda qué pasa con tus datos si te vas, pregunta directamente antes de asumir que la respuesta te favorece.
- ✓ **Ningún compromiso o plazo específico de notificación de brechas.** Un proveedor debería poder declarar, por escrito, cómo y cuándo te notificará si se comprometen los datos de residentes.

Construyendo Tu Propio Aviso de Privacidad para la Propiedad

Incluso con un proveedor consciente de la privacidad, tu propiedad generalmente tiene su propia responsabilidad de informar a los residentes sobre las prácticas de datos del sistema de control de acceso. Un aviso breve y en lenguaje simple — no necesariamente un documento legal formal — típicamente cubre:

- ✓ Qué datos recolecta el sistema de control de acceso sobre residentes y visitantes
- ✓ Por qué se recolectan (seguridad, administración de acceso, audit trail)
- ✓ Quién puede acceder a ellos (el personal de tu propiedad, y a un nivel general, el proveedor)
- ✓ Por cuánto tiempo generalmente se conservan
- ✓ A quién contactar con preguntas o una solicitud relacionada con datos

Haz que un asesor legal revise tu aviso final, particularmente si tu jurisdicción tiene requisitos específicos de divulgación — pero comenzar con este esquema le da a tu abogado un borrador concreto para refinar en lugar de una página en blanco.

Checklist y Puntos Clave

- ✓ Solicitada una lista completa de categorías de datos recolectados por cualquier plataforma en evaluación
- ✓ Confirmados los estándares de cifrado para datos en tránsito y en reposo, específicamente para grabaciones de video
- ✓ Preguntado si se usa reconocimiento facial o datos biométricos, y revisados los requisitos aplicables con un asesor legal
- ✓ Revisado el modelo interno de control de acceso de empleados del proveedor
- ✓ Confirmados los plazos de retención de datos por categoría, y qué pasa al terminar el contrato
- ✓ Hechas las nueve preguntas de debida diligencia de la página 10 directamente, por escrito
- ✓ Revisada la política de privacidad del proveedor en busca de las señales de alerta de la página 11
- ✓ Redactado o actualizado un aviso de privacidad orientado al residente para nuestra propiedad

Privacidad y seguridad están relacionadas pero son distintas — una plataforma puede tener excelente seguridad de control de acceso y aun así manejar mal los datos de residentes, o viceversa. Evalúa ambas explícitamente, y no asumas que una implica la otra.

VIVO CONTROL

Hazlos Directamente en Tu Demo

Con gusto recorreremos en detalle nuestras prácticas de manejo de datos, cifrado, retención, y control de acceso — lleva el checklist de esta guía a tu demo.

Reserva una Demo Gratis →

www.vivocontrol.com/es/demo/ · hello@vivocontrol.com · Esta guía tiene fines educativos generales únicamente y no constituye asesoría legal. La ley de privacidad de datos varía según la jurisdicción y cambia con el tiempo — consulta a un asesor legal calificado para orientación específica a tu propiedad.