VecinApp

Acuerdo de Encargo de Tratamiento (DPA)

Versión 2.4 - octubre 2026

En vigor desde el 10 de noviembre de 2026. Hasta esa fecha rige la versión firmada por cada despacho.

EL SUB-ENCARGADO DEL TRATAMIENTO: VecinApp Technologies, S.L. («VecinApp»), CIF B27593391, con domicilio en C/ Balmes 116, 2º, 08008 Barcelona (España), inscrita en el Registro Mercantil de Barcelona, Hoja B-654613, Folio 1, Inscripción 1ª (constituida mediante escritura otorgada en Barcelona el 27/03/2026 ante la Notaria Dª Lucía Rodríguez Rodríguez, protocolo 442/2026), representada por su Administrador, D. Sergi Méndez Rodríguez.

EL ENCARGADO DEL TRATAMIENTO: el despacho cliente identificado en las Condiciones Particulares.

Este documento se genera automáticamente desde el texto contractual vigente. La versión publicada en vecinapp.es/condiciones#dpa es la que rige.

Exposición

I. La Administradora presta servicios profesionales de administración de fincas a diversas Comunidades de Propietarios (las «Comunidades»), actuando como Encargado del Tratamiento conforme al Reglamento (UE) 2016/679 («RGPD») y la Ley Orgánica 3/2018 («LOPD-GDD»).

II. VecinApp es proveedora de servicios SaaS para la gestión de comunidades de propietarios. Para prestarlos, tratará datos personales de propietarios e inquilinos de las Comunidades gestionadas, actuando como Sub-Encargado del Tratamiento a instancias de la Administradora, quien a su vez actúa por cuenta de las Comunidades como Responsables del Tratamiento.

III. Las partes suscriben el presente DPA al amparo del artículo 28 del RGPD. El presente DPA forma parte integrante de las Condiciones Generales de Contratación del Servicio (disponibles en https://vecinapp.es/condiciones) y se acepta junto con ellas en el proceso de suscripción, quedando registrada dicha aceptación (versión, fecha y hora, usuario y dirección IP cuando esté disponible).

1. Objeto y ámbito de aplicación

1.1. El presente DPA regula las condiciones del tratamiento de datos personales que VecinApp realice por cuenta de la Administradora en el marco de la prestación de los servicios de la plataforma VecinApp (los «Servicios»).

1.2. La Administradora encomienda a VecinApp el tratamiento de los datos personales estrictamente necesarios para la prestación de los Servicios, conforme a las instrucciones documentadas del Anexo I.

1.3. VecinApp tratará los datos únicamente conforme a las instrucciones documentadas de la Administradora. Si considerara que alguna instrucción infringe el RGPD u otra normativa de protección de datos, lo comunicará de inmediato a la Administradora.

1.4. VecinApp reconoce que el tratamiento se realiza en última instancia por cuenta de las Comunidades de Propietarios, que ostentan la condición de Responsables del Tratamiento (art. 4.7 RGPD). La Administradora actúa como Encargado y VecinApp como Sub-Encargado (art. 28.4 RGPD). VecinApp no adquiere en ningún caso la condición de Responsable ni Corresponsable respecto de estos datos.

1.5. VecinApp no determina los fines ni los medios esenciales del tratamiento. Las decisiones sobre finalidad, base jurídica, plazos de conservación, comunicación a terceros y publicación corresponden a la Administradora y, en última instancia, a las Comunidades.

1.6. Delimitación: quedan fuera del presente DPA los datos que VecinApp trata como Responsable propio: los datos de contacto y facturación del propio Cliente y de sus usuarios (gestión de la cuenta, cobro de la suscripción mediante el proveedor de pagos, facturación, soporte y comunicaciones comerciales), que se rigen por la Política de Privacidad de VecinApp (https://vecinapp.es/privacy).

2. Identificación del tratamiento

2.1. Los Servicios no están diseñados para el tratamiento sistemático de categorías especiales de datos (art. 9 RGPD). Si la Administradora introduce voluntariamente datos de salud, discapacidad o vulnerabilidad: el tratamiento será responsabilidad exclusiva de la Administradora; VecinApp actuará solo como proveedor técnico; la Administradora garantiza disponer de base jurídica y evaluará la necesidad de una EIPD.

2.2. Síntesis del tratamiento (detalle en Anexo I):

- Naturaleza: recogida, registro, organización, almacenamiento, consulta, comunicación, conservación y supresión mediante plataforma SaaS en la nube. Incluye: tratamiento automatizado mediante agente de inteligencia artificial que procesa datos de la plataforma a través de las API de los proveedores de modelos de lenguaje del Anexo IV; agente de voz por IA para la atención de llamadas telefónicas entrantes; y firma electrónica de documentos (eIDAS).

- Finalidad: gestión integral de comunidades: comunicaciones, incidencias, documentación, cuotas y recibos, conciliación bancaria, contabilidad, convocatorias y ejercicio de derechos RGPD. El agente IA asiste a la Administradora en la gestión operativa; no elabora perfiles ni adopta decisiones automatizadas con efectos jurídicos (art. 22 RGPD no aplicable).

- Tipos de datos: identificativos (nombre, DNI/NIE), contacto (email, teléfono, dirección), vivienda (unidad, portal, piso), financieros (cuotas, deudas, IBAN, movimientos bancarios de la Comunidad), comunicaciones (mensajes, incidencias, audio/transcripción de llamadas), datos de acceso (logs).

- Interesados: propietarios e inquilinos de las Comunidades gestionadas por la Administradora.

- Duración: vigencia del Contrato de Servicios + periodos de conservación legal (Anexo III).

- Responsables: las Comunidades de Propietarios (personas jurídicas conforme a la LPH).

3. Obligaciones de VecinApp

3.1. Tratamiento conforme a instrucciones. Tratar los datos únicamente según las instrucciones documentadas de la Administradora, salvo obligación legal de la UE o de un Estado miembro (que comunicará previamente salvo prohibición por interés público). No destinar los datos a finalidades distintas de las del Anexo I.

3.2. Confidencialidad. Garantizar que las personas autorizadas se han comprometido a la confidencialidad o están sujetas a obligación estatutaria, y que solo tratan los datos siguiendo instrucciones de la Administradora.

3.3. Medidas de seguridad. Aplicar medidas técnicas y organizativas apropiadas al riesgo (art. 32 RGPD), incluyendo como mínimo: MFA obligatoria para administradores; aislamiento multi-tenant mediante Row Level Security (RLS); control de acceso por roles (seis niveles); registro de auditoría con trazabilidad de accesos; cifrado en tránsito (TLS 1.2+) y en reposo (AES-256); copias de seguridad automáticas con PITR. Detalle en Anexo II.

3.4. Sub-encargados. La Administradora autoriza de forma general la subcontratación con los proveedores del Anexo IV. VecinApp comunicará cualquier alta, sustitución o modificación sustancial de sub-encargados con siete (7) días naturales de antelación mediante un aviso en el Servicio dirigido a los administradores de cada organización, en el panel de administración y por correo electrónico, que podrá incluirse en la comunicación periódica de novedades. El aviso indicará el sub-encargado, el servicio, los datos afectados, su ubicación, la garantía de transferencia aplicable y la fecha límite de oposición. El mismo día, VecinApp publicará el cambio en vecinapp.es/subencargados, que constituye el registro permanente y actualizado de la lista. El plazo se computa desde la fecha de publicación del aviso, y VecinApp conservará el registro de su entrega. La Administradora podrá oponerse dentro de dicho plazo por razones objetivas y fundamentadas, escribiendo a dpo@vecinapp.es; en defecto de acuerdo, podrá resolver el Contrato sin penalización. La falta de oposición en plazo equivale a aceptación. La baja de un sub-encargado no requiere preaviso. VecinApp impondrá a sus sub-encargados las mismas obligaciones y responderá del incumplimiento de estos.

3.5. Asistencia para el ejercicio de derechos (arts. 15-22 RGPD). VecinApp: proporciona herramientas en la plataforma para gestionar solicitudes (módulo de ejercicio de derechos); facilita exportación en formato estructurado (Excel/CSV) para portabilidad; responderá a solicitudes de asistencia en máximo 10 días hábiles; y cuando la Administradora no pueda ejecutar técnicamente la actuación, VecinApp la ejecutará materialmente previa instrucción formal, dentro de los plazos del art. 12 RGPD, informando de inmediato. La responsabilidad frente al interesado sigue correspondiendo a la Administradora y, en última instancia, a la Comunidad.

3.6. Asistencia en seguridad y evaluaciones (arts. 32-36 RGPD). Asistencia en seguridad del tratamiento, notificación de violaciones a la autoridad y a interesados, EIPD y consulta previa.

3.7. Violaciones de seguridad. Notificación a la Administradora sin dilación indebida y en máximo 24 horas desde su conocimiento, incluyendo: naturaleza (categorías y nº aproximado de afectados), punto de contacto, posibles consecuencias y medidas adoptadas o propuestas. (La Administradora dispone de 72h para notificar a la AEPD - art. 33 RGPD; el plazo de 24h le da mayor margen.)

3.8. Registro de actividades. Mantener el registro del art. 30.2 RGPD, disponible para la autoridad de control.

3.9. Contacto de protección de datos. dpo@vecinapp.es. Si VecinApp estuviera obligada a designar DPO (art. 37 RGPD), comunicará sus datos.

3.10. Logs de seguridad. VecinApp podrá tratar datos técnicos de acceso (IP, user-agent, timestamps, sesión) con finalidad de seguridad, detección de accesos no autorizados, prevención de fraude y acreditación de cumplimiento (interés legítimo, art. 6.1.f RGPD). No se usarán para perfilado comercial.

3.11. Localización. Los datos se almacenan principalmente en AWS eu-west-2 (Londres, Reino Unido), territorio con decisión de adecuación vigente (art. 45 RGPD). Los tratamientos accesorios de los sub-encargados del Anexo IV pueden implicar transferencias a terceros países (principalmente EE. UU.) amparadas en las garantías de la Cláusula 5.

3.12. Transfer Impact Assessment. VecinApp declara haber evaluado el impacto de las transferencias internacionales conforme a las recomendaciones del CEPD. Documentación disponible bajo solicitud razonable.

3.13. Uso de inteligencia artificial agéntica.

3.13.1. Naturaleza y clasificación. VecinApp incorpora un sistema de IA agéntica (conforme a las Orientaciones de la AEPD de 18/02/2026). A efectos del Reglamento (UE) 2024/1689 (Reglamento de IA), se clasifica como de riesgo limitado (no comprendido en el Anexo III de alto riesgo).

3.13.2. Finalidad exclusiva. Asistir a la Administradora en la gestión operativa. Prohibido expresamente: perfilado de propietarios/inquilinos con efectos jurídicos; decisiones automatizadas del art. 22 RGPD (toda decisión con efectos jurídicos requiere intervención humana de la Administradora); finalidades distintas del Anexo I.4.

3.13.3. Minimización y control del contexto. El agente solo accede a los datos estrictamente necesarios por tarea (art. 5.1.c RGPD): contexto limitado a lo pertinente, sin transmisión de la base de datos completa; filtros técnicos que excluyen del contexto enviado al proveedor de modelo los campos de alta sensibilidad (DNI/NIE completos, IBAN completos, credenciales, datos del art. 9); comunicación exclusivamente cifrada (TLS 1.2+).

3.13.4. Supervisión humana y trazabilidad. El agente no ejecuta acciones irreversibles sobre datos de propietarios sin confirmación explícita del Administrador (flujo previsualizar y confirmar). Cada interacción queda registrada en el log de auditoría (usuario, tarea, timestamp, categoría de dato).

3.13.5. Transparencia. La Administradora es responsable de informar a propietarios e inquilinos del uso de herramientas de IA (art. 13 RGPD), incluida la atención telefónica mediante agente de voz. VecinApp facilitará texto informativo adecuado a su solicitud.

3.13.6. Proveedores de modelo y retención. El agente utiliza los modelos de lenguaje de los proveedores identificados en el Anexo IV: Anthropic, PBC (modelo del asistente del administrador; sin entrenamiento con datos de API y retención cero) y OpenAI, Inc. (IA del panel: lectura de facturas, transcripción de notas de voz y redacción/clasificación de textos; sin entrenamiento con datos de API). El agente de voz para llamadas entrantes se presta a través de Vocals AI (con la telefonía subyacente de Twilio). Los datos enviados vía API no se utilizan para el entrenamiento de los modelos conforme a los términos empresariales suscritos con dichos proveedores. VecinApp mantiene documentación acreditativa disponible para la Administradora y la AEPD.

3.13.7. Evaluación de impacto del módulo IA. VecinApp mantendrá actualizada la evaluación relativa al agente, revisándola ante cambios sustanciales de modelo, datos o normativa.

4. Obligaciones de la Administradora

Proporcionar solo los datos necesarios (minimización); garantizar base jurídica suficiente y que los interesados han sido informados (arts. 13-14 RGPD); impartir instrucciones conformes a la normativa (VecinApp podrá rechazar las contrarias al RGPD); informar de cambios en finalidades, categorías o interesados; gestionar con diligencia el ejercicio de derechos en los plazos del art. 12 RGPD; notificar sin dilación incidentes de seguridad que conozca; colaborar en auditorías; y mantener actualizado el listado de usuarios con acceso, revocando los que causen baja.

5. Transferencias internacionales

5.1. Los Servicios se apoyan en proveedores cuya infraestructura puede estar fuera del EEE (en particular EE. UU.). Los sub-encargados afectados constan en el Anexo IV.

5.2. Las transferencias se amparan en: Cláusulas Contractuales Tipo (Decisión de Ejecución (UE) 2021/914) y/o certificación en el EU-US Data Privacy Framework (Decisión de Ejecución (UE) 2023/1795).

5.3. VecinApp facilitará copia de las garantías aplicables a solicitud de la Administradora.

6. Auditoría y cooperación

6.1. VecinApp pondrá a disposición toda la información necesaria para demostrar el cumplimiento del art. 28 RGPD.

6.2. Auditorías e inspecciones por la Administradora o auditor autorizado: preaviso mínimo de 15 días hábiles; costes a cargo de la Administradora; máximo una por año natural salvo incidente grave; en horario laboral; sin acceso a código fuente ni a datos de otros clientes; sin comprometer la seguridad de la plataforma.

6.3. La información obtenida es confidencial.

6.4. Alternativamente, VecinApp podrá acreditar cumplimiento mediante certificados vigentes de terceros independientes (ISO 27001, SOC 2 Tipo II, ENS o equivalentes).

7. Subcontratación

7.1. El listado vigente de sub-encargados es el publicado en vecinapp.es/subencargados, que prevalece sobre la instantánea del Anexo IV. La aceptación del presente DPA constituye autorización general, con derecho de oposición conforme a la Cláusula 3.4. Los cambios comunicados antes de la entrada en vigor de la versión 2.4 de este DPA se rigen por el plazo de treinta (30) días naturales de la versión anterior.

7.2. VecinApp celebrará con cada sub-encargado contrato con las mismas obligaciones.

7.3. VecinApp responde plenamente ante la Administradora del cumplimiento de sus sub-encargados.

8. Devolución y supresión

8.1. A la finalización, a elección de la Administradora: devolución de los datos con supresión posterior, o supresión con destrucción de copias, salvo obligación legal de conservación (en cuyo caso los datos quedarán bloqueados, limitado su tratamiento a las finalidades que justifiquen la conservación). La devolución se pone a disposición en formato estructurado (Excel/CSV) y, para documentos y remesas, en PDF y ficheros SEPA, conforme a la Cláusula 7 de las Condiciones Particulares (portabilidad y devolución de datos).

8.2. En ausencia de instrucciones, VecinApp notificará con 30 días de antelación la eliminación definitiva; sin respuesta, procederá a supresión segura.

8.3. Certificado de destrucción a solicitud de la Administradora.

8.4. VecinApp podrá conservar datos estadísticos anonimizados que no permitan identificación, para mejora del servicio.

9. Confidencialidad

Secreto profesional estricto de ambas partes sobre los datos y la información de la otra parte, subsistente tras la finalización. VecinApp garantiza obligaciones equivalentes de sus empleados, colaboradores y sub-encargados.

10. Duración y extinción

10.1. Misma duración que el Contrato de Servicios; se extingue automáticamente con su terminación.

10.2. Resolución por incumplimiento grave o reiterado no subsanado en 15 días hábiles desde el requerimiento escrito.

10.3. Subsisten las obligaciones que por su naturaleza deban sobrevivir (confidencialidad, devolución/supresión, responsabilidad).

11. Responsabilidad

11.1. VecinApp responderá de los daños causados por incumplimientos que le sean directamente imputables, en los términos del art. 82 RGPD, quedando exenta si demuestra no ser en modo alguno responsable (art. 82.3).

11.2. La responsabilidad total derivada del presente DPA queda integrada en el límite general de responsabilidad del Contrato de Servicios (cl. 26.1 de las Condiciones Generales: importe abonado en los 6 meses anteriores), salvo dolo o negligencia grave.

11.3. VecinApp no responde de daños causados por instrucciones de la Administradora contrarias a la normativa ni por tratamientos fuera del alcance de los Servicios.

11.4. Nada en el presente DPA constituye corresponsabilidad (art. 26 RGPD); cada parte responde de su esfera de control.

12. Legislación aplicable y jurisdicción

Legislación española y de la UE (RGPD, LOPD-GDD). Juzgados y Tribunales legalmente competentes, salvo norma imperativa. Esta cláusula prevalece sobre la sumisión a los tribunales de Barcelona prevista en la cl. 33 de las CGC. Prevalece la versión en español.

13. Evaluación de impacto (EIPD)

La Administradora determinará si el tratamiento requiere EIPD (art. 35 RGPD); VecinApp prestará asistencia técnica.

Anexo I - Descripción del tratamiento

I.1. Actividades autorizadas: almacenamiento y organización de datos de propietarios/inquilinos; envío de comunicaciones transaccionales (incidencias, convocatorias, recibos) por email y notificación push; atención de llamadas telefónicas entrantes mediante agente de voz IA; validación de direcciones postales en el alta de comunidades; firma electrónica de documentos (eIDAS); gestión de incidencias; gestión documental comunitaria con control de acceso; gestión financiera y contable (cuotas, recibos, deudas, morosos, facturación, según roles); conciliación bancaria de las cuentas de la Comunidad mediante proveedores de información de cuentas (Anexo IV); mensajería entre propietarios y con la Administradora; gestión de solicitudes de derechos RGPD; generación de registros de auditoría; aplicación de políticas de retención.

I.2. Instrucciones de seguridad: datos de morosos accesibles solo a presidente/administrador; nóminas de empleados de la comunidad no visibles a propietarios ordinarios; mensajes privados solo accesibles a los participantes (RLS); accesos registrados en audit log con categoría de dato, base legal y usuario.

I.3. Prohibiciones expresas: ceder datos a terceros sin instrucción o base legal; usar los datos para fines propios (marketing, perfilado comercial, venta de datos); tratar fuera del EEE sin las garantías de la Cláusula 5; publicar estadísticas reidentificables.

I.4. Instrucciones específicas del agente IA: envío puntual, limitado y contextualizado de los datos estrictamente necesarios vía API segura (TLS 1.2+), sin acceso directo ni persistente del proveedor de modelo a la base de datos de producción. TIA específico documentado (art. 46 RGPD, Recomendaciones 01/2020 CEPD). Garantías: CCT (2021/914) y/o EU-US DPF (2023/1795) según proveedor; compromisos de no entrenamiento con datos de API; verificación anual de vigencia de garantías. Medidas técnicas: minimización estricta del contexto; exclusión de DNI/NIE e IBAN completos, credenciales y categorías especiales; seudonimización cuando sea viable; registro en audit log; confirmación humana previa a almacenamiento definitivo de resultados. El agente no adopta decisiones automatizadas (art. 22 RGPD no aplicable), no hace scoring ni perfilado, y toda decisión final corresponde a la Administradora.

Anexo II - Medidas de seguridad

Autenticación: MFA (TOTP) obligatoria para administradores; política de contraseñas; expiración de sesiones

Control de acceso: Roles con seis niveles de privilegio; mínimo privilegio; registro de sesiones

Aislamiento: Row Level Security (RLS): cada organización accede solo a sus datos; verificado con tests automatizados

Cifrado en tránsito: TLS 1.2+ en todas las comunicaciones; certificados gestionados y renovados automáticamente

Cifrado en reposo: AES-256 (base de datos y almacenamiento de archivos)

Copias de seguridad: Backups automáticos con PITR; retención configurable; restauración verificada periódicamente

Trazabilidad: Audit log completo: timestamp, usuario, acción, categoría de dato y base legal

Gestión de brechas: Panel de incidentes de seguridad; procedimiento de respuesta con notificación 24h a la Administradora

Retención automática: Políticas por categoría de dato con eliminación/anonimización automática

Impersonation controlada: Acceso de soporte a cuentas solo con registro completo de la sesión en audit log

Vulnerabilidades: Actualización de dependencias con revisión; análisis periódico de vulnerabilidades

Personal: Compromisos de confidencialidad; acceso a producción restringido

Agente IA: Minimización de contexto; no-entrenamiento contractual; audit log de consultas con usuario y categoría de dato

Anexo III - Plazos de conservación

Identidad del propietario (nombre, DNI, email, teléfono): Mientras sea propietario/inquilino + 5 años (art. 1964 CC)

Cuenta bancaria / domiciliación: Mientras activo + 4 años (art. 66 LGT)

Facturas y recibos de cuotas: 10 años desde emisión (art. 30 CCom)

Deuda / morosidad: Vigencia de la deuda + 5 años desde liquidación o prescripción

Actas de Junta: 10 años (Guía AEPD; relevancia probatoria)

Incidencias y comunicaciones: 3 años desde resolución

Mensajes privados entre vecinos: 1 año desde envío, salvo relevancia para incidencia en curso

Grabaciones / transcripciones de llamadas al agente de voz: 3 años desde la llamada (mismo plazo que las incidencias), salvo relevancia probatoria

Logs de auditoría: 2 años (art. 45 LOPD-GDD)

Foto de perfil: Mientras cuenta activa; eliminación en 30 días tras baja o solicitud

Datos de sesión (logs): 1 año

Solicitudes de derechos: 3 años desde resolución

DPA y registros de aceptación: 5 años tras extinción (prescripción contractual)

Anexo IV - Sub-encargados

Instantánea a la fecha de firma. La lista vigente se publica en vecinapp.es/subencargados y prevalece sobre este Anexo (Cláusula 7.1). CCT = Cláusulas Contractuales Tipo (Decisión UE 2021/914); EU-US DPF = EU-US Data Privacy Framework (Decisión UE 2023/1795).

Supabase, Inc. - Base de datos, autenticación, almacenamiento, Edge Functions, copias de seguridad Localización y garantías: AWS eu-west-2 (Londres, R.U. - adecuación art. 45). Accesorios: CCT 2021/914 + EU-US DPF Datos: Todos los datos de la plataforma

Resend, Inc. - Email transaccional (avisos, convocatorias, notificaciones) Localización y garantías: AWS eu-west-1 (Irlanda); accesorios bajo Cap. V RGPD Datos: Nombre, email, contenido del mensaje

Vercel, Inc. - Hosting y CDN de la aplicación web Localización y garantías: Regiones UE (París, Estocolmo); CCT + EU-US DPF Datos: Logs de acceso (IP, user-agent, timestamps)

Cloudflare, Inc. - Almacenamiento de objetos (R2) - copias de seguridad Localización y garantías: Europa Occidental; CCT + EU-US DPF Datos: Copias de seguridad de BD

Hetzner Online GmbH - Infraestructura de contingencia y tareas programadas de copia de seguridad Localización y garantías: UE (Alemania/Finlandia); sin transferencia internacional Datos: Copias de seguridad de BD

Anthropic, PBC - Modelo de lenguaje del asistente IA del administrador Localización y garantías: EE. UU.; CCT 2021/914 + DPA empresarial; sin entrenamiento con datos de API; Zero Data Retention (ZDR) activado a nivel de cuenta Datos: Contexto minimizado de propietarios, incidencias, comunicaciones y documentación (Anexo I.4)

OpenAI, Inc. - IA del panel: lectura de facturas (OCR), transcripción de notas de voz, redacción y clasificación de textos Localización y garantías: EE. UU.; CCT 2021/914 + EU-US DPF; sin entrenamiento con datos de API; Zero Data Retention (ZDR) activado a nivel de cuenta, incluida la transcripción de audio Datos: Ídem Anexo I.4

Wealth Reader, S.L. (CIF B44575942) - Información sobre cuentas (AIS) y agregación bancaria para la conciliación. Entidad regulada por el Banco de España, nº 6939 (art. 1.2.h RDL 19/2018) Localización y garantías: UE (Google Cloud, regiones UE); sin transferencia fuera del EEE garantizada contractualmente Datos: Movimientos, saldos y titularidad de las cuentas de la Comunidad (pueden incluir nombre e IBAN de propietarios pagadores). Credenciales de banca online cifradas y suprimidas en máx. 72 h desde la revocación o terminación

Holded, S.L. - Contabilidad y facturación, incluida la de las comunidades administradas Localización y garantías: España; sin transferencia internacional Datos: Datos contables y de facturación de las comunidades (facturas, asientos, importes)

Firma.dev - Firma electrónica de documentos (eIDAS) Localización y garantías: AWS región París (Francia); sin transferencia internacional Datos: Documentos a firmar y datos identificativos del firmante (nombre, email)

Google Ireland Limited (Firebase - Maps Platform) - Notificaciones push a los dispositivos y validación de direcciones postales en el alta de comunidades Localización y garantías: Irlanda (Dublín); el subtratamiento puede implicar a Google LLC (EE. UU.); CCT + EU-US DPF Datos: Token de dispositivo y contenido del aviso; direcciones a validar

Meta Platforms Ireland Limited (WhatsApp Business Platform) - Envío y recepción de los mensajes de WhatsApp de los despachos que conectan su número de WhatsApp Business al Buzón Localización y garantías: Irlanda; el subtratamiento puede implicar a Meta Platforms, Inc. (EE. UU.) - CCT + EU-US DPF Datos: Número de teléfono, nombre de perfil y contenido de los mensajes

Vocals AI - Agente de voz por IA para la atención de llamadas telefónicas entrantes Localización y garantías: UE; sin transferencia internacional Datos: Audio y transcripción de la llamada, número de teléfono

Twilio Inc. - Telefonía subyacente del agente de voz (provista a través de Vocals AI) Localización y garantías: EE. UU.; CCT + EU-US DPF Datos: Metadatos de la llamada, número de teléfono

Functional Software, Inc. (Sentry) - Monitorización de errores del panel de administración Localización y garantías: Región UE (Alemania); CCT; datos alojados en la UE Datos: Datos técnicos de error; posibles datos personales en pantalla (enmascarados)