Política de privacidad (mapeadores, compradores y personas que puedan aparecer en imágenes)

Versión 0.3.1, de 28 de septiembre de 2026
mercamap.com/legal/archive/privacy-policy/0.3.1

Información básica sobre protección de datos (primera capa)

Epígrafe: Responsable
Información: Iñigo Escribano Calvo, NIF 72725776Y, Portichol 83, 03670 Monforte del Cid (Alicante) · privacidad@mercamap.com

Epígrafe: Finalidad
Información: Prestar la aplicación MercaMap: (a) recibir fotogramas pixelados y telemetría de recorridos por tiendas para construir mapas de productos y calcular recompensas; (b) guiar la compra con listas y rutas; (c) con su consentimiento separado, analizar de forma seudonimizada qué se compra, dónde y con qué frecuencia para elaborar estadísticas agregadas; (d) pagos, seguridad, soporte y cumplimiento legal

Epígrafe: Legitimación
Información: Ejecución del contrato (RGPD art. 6.1.b); interés legítimo en construir un conjunto de datos de ubicación de productos para guiar a compradores y elaborar estadísticas (art. 6.1.f), con ponderación documentada; consentimiento (art. 6.1.a) para la analítica de compra y la analítica de producto; obligaciones legales (art. 6.1.c) contables, fiscales y de atención de derechos

Epígrafe: Destinatarios
Información: Encargados del tratamiento con contrato (alojamiento, base de datos, correo, analítica, errores, notificaciones, inteligencia artificial) situados en la UE o con garantías del Capítulo V (Marco de Privacidad de Datos UE-EE. UU. o cláusulas contractuales tipo). Si entra con Google o Apple, esas empresas son responsables independientes de ese inicio de sesión; en Android, Google recoge también, como responsable independiente, datos de uso y diagnóstico de ARCore, la realidad aumentada del mapeo (§8). No se venden datos individuales. Las imágenes nunca se comparten con tiendas ni marcas

Epígrafe: Derechos
Información: Acceso, rectificación, supresión, limitación, portabilidad, oposición, retirada del consentimiento y no ser objeto de decisiones automatizadas; ejercicio en la app (Ajustes -> Privacidad y datos) o en privacidad@mercamap.com; reclamación ante la AEPD

Epígrafe: Procedencia
Información: Del propio usuario (o, si entra con Google o Apple, de ese servicio: su correo y un identificador de cuenta); en el caso de terceros que aparezcan en imágenes, de los usuarios que captan las imágenes (véase el aviso de mercamap.com/personas)

Epígrafe: Información adicional
Información: El resto de esta política

1. Responsable del tratamiento

Iñigo Escribano Calvo, persona física (en adelante, "nosotros"), NIF 72725776Y, con domicilio en Portichol 83, 03670 Monforte del Cid (Alicante). Contacto para protección de datos: **privacidad@mercamap.com**. No hemos designado delegado de protección de datos porque ninguno de los supuestos del art. 34.1 de la Ley Orgánica 3/2018 (LOPDGDD) ni del art. 37.1 del RGPD nos resulta aplicable; revisamos esta decisión cada año (registro interno de decisiones).

Esta política se aplica a la aplicación móvil **MercaMap** (iOS y Android), al sitio web mercamap.com y a los

canales de soporte. La versión en español es la vinculante; la versión en inglés es una traducción de cortesía.

2. A quién se aplica

Colectivo: A. Mapeadores
Quién es: Personas mayores de 18 años que graban recorridos por estanterías con la app y reciben puntos
Secciones relevantes: 3.A, 4 (P1–P6, P11–P15), 5, 7, 10, 11

Colectivo: B. Compradores
Quién es: Personas mayores de 14 años que usan listas, mapas y rutas
Secciones relevantes: 3.B, 4 (P1, P7–P15), 7, 10, 11

Colectivo: C. Terceros y personal de tiendas
Quién es: Personas que se encuentran en una tienda mientras un mapeador, o una persona de nuestro equipo en sus pruebas, graba
Secciones relevantes: 4 (P2, P17), 6 y el aviso público de mercamap.com/personas

Colectivo: D. Visitantes web, notificantes y minoristas
Quién es: Quienes usan el sitio web, envían una notificación o solicitud, o nos contactan en nombre de una tienda
Secciones relevantes: 3.D, 4 (P13, P16), 10, 11

3. Datos que tratamos

3.A Mapeadores

- **Cuenta**: dirección de correo electrónico, idioma, declaración de mayoría de edad, fecha de creación, dispositivos y sesiones de inicio de sesión, tokens de notificación push.
- **Sesiones de mapeo**: tienda elegida, hora de inicio y fin, estado, modo de captura (realidad aumentada o sensores de movimiento), número de fotogramas y de fragmentos subidos, modelo de dispositivo y versión de la app, el resultado de la comprobación del teléfono (cifras de la cámara, de la realidad aumentada y de 3 fotos de prueba, sin imágenes), un resumen técnico de la captura (recuentos, tiempos y distancia recorrida), resultado de las comprobaciones antifraude, puntuación de calidad, motivos de rechazo, recursos.
- **Fotogramas**: imágenes fijas de estanterías (aproximadamente una por segundo) en las que **toda persona ha sido pixelada de forma irreversible en su teléfono antes de la subida**; sin audio; nunca vídeo. Cada fotograma se vincula a su sesión y, por tanto, a su cuenta mientras se conserva.
- **Telemetría de movimiento y recorrido**: aceleración y velocidad de giro del teléfono (25 Hz), rumbo magnético (5 Hz), pasos (momento de cada paso y recuento del podómetro) y la **posición y orientación del teléfono dentro de la tienda** (en metros respecto al punto de inicio de la sesión, hasta 10 veces por segundo), calculadas en el propio teléfono con realidad aumentada (ARCore, en Android) o, en teléfonos sin ella, con los sensores de movimiento. Con realidad aumentada se suben además, sin ninguna imagen: la posición corregida de los puntos de referencia que fija por el camino (uno cada 2,5 m aproximadamente); los contornos del suelo y de las estanterías que detecta; una cuadrícula de 5 cm con los obstáculos que proyecta sobre el suelo a partir de los puntos que detecta (esos puntos no se suben ni se guardan), y, para cada fotograma, dónde estaba el teléfono, a qué distancia estaba la estantería, qué punto de ella miraba la cámara y los parámetros ópticos de la cámara. Se registran también el estado del seguimiento, los giros, pasillos y zonas abiertas detectados automáticamente, cuándo la app se pausa o pasa a segundo plano, sus avisos de «Problema» y, **solo si concede el permiso de ubicación**, la posición GPS al inicio y al final de la sesión. Las imágenes de la cámara que usa la realidad aumentada se procesan en memoria y no se guardan. Nunca hay seguimiento de ubicación fuera de una sesión ni en

segundo plano. Las versiones de la app que aún no detectan los pasillos solas registran además sus pulsaciones de «Siguiente pasillo», «Media vuelta» y «Zona».

- **Registro técnico de diagnóstico (temporal, fase de pruebas)**: mientras dure la fase de pruebas, la app de las **cuentas de nuestro equipo** (hoy, solo la del responsable) envía un registro técnico de lo que hacen las sesiones de mapeo y la comprobación de realidad aumentada: estados del seguimiento, decisiones automáticas de detección, tiempos, recuentos, resultados de subida y errores, el modelo del teléfono, las versiones de la app y del sistema y, con menor frecuencia (como máximo dos veces por segundo), la posición del teléfono en la tienda respecto al punto de inicio. No contiene imágenes, coordenadas GPS, correo electrónico, nombre, teléfono ni datos bancarios: la app y el servidor descartan esos campos. Se guarda en nuestra base de datos en la UE (Fráncfort), vinculado a la cuenta, se usa solo para corregir fallos y se borra a los 30 días. Si lo activáramos para otros mapeadores, lo indicaríamos antes en esta política.
- **Datos derivados**: texto de carteles, productos avistados y su ubicación, mapa de sesión (pasillos, pasillos transversales y zonas detectados, con sus medidas), resumen de telemetría (pasos, giros) y la categoría de cada producto, sección y zona: la de cada producto la asigna el modelo de visión a partir del fotograma, y la de cada sección y zona se calcula a partir de las categorías de los productos vistos en ella y del tipo de escena. No contienen imágenes ni datos de terceros.
- **Recompensas y pagos**: libro de puntos, solicitudes de pago, IBAN y NIF (cifrados; solo se muestran los últimos cuatro dígitos del IBAN), marca de verificación de identidad y edad, declaración anual de recompensas.
- **Verificación de identidad y edad** (solo en el primer pago): imagen del DNI/NIE que una persona de nuestro equipo compara con el NIF y la fecha de nacimiento; **la imagen se suprime en el momento de la decisión**, y en todo caso a los 30 días; solo se conserva la marca "verificado", la fecha y quién verificó.

3.B Compradores

- **Cuenta**: correo electrónico, idioma, tramo de edad resultante de la pantalla de fecha de nacimiento (no se conserva la fecha completa, solo el tramo: menor de 14, 14 o más, mayor de edad), dispositivos, tokens push.
- **Uso del servicio**: tiendas consultadas, búsquedas de productos dentro de una tienda, listas (artículos, cantidades, notas, miembros del hogar con quienes comparte la lista), rutas calculadas, estado del viaje (planificado, activo, completado, abandonado) y la marca de tiempo de cada parada.
- **Ubicación**: para mostrar tiendas cercanas se envía su posición aproximada al servidor y **no se conserva** ; durante el viaje guiado, la posición en la tienda se calcula **en su teléfono** a partir del podómetro y la brújula y **nunca sale del teléfono** como trayectoria; solo un resumen por parada (llegada, tiempo en la parada) se envía, y únicamente si ha activado la analítica de compra (P8).
- **Analítica de compra seudonimizada** (solo con su consentimiento): eventos "artículo cogido", "omitido", "no encontrado", "añadido fuera de lista", "ruta recalculada", con producto, sección, tienda, semana y orden, bajo un **seudónimo** calculado a partir de una clave y una sal aleatoria propia de su cuenta; su identificador de usuario nunca figura en esas tablas.

3.C Terceros y personal de tiendas

Véase la sección 6.

3.D Visitantes web, notificantes y minoristas

- **Sitio web**: registros técnicos del servidor (dirección IP en forma de hash, agente de usuario, página solicitada, hora) durante 12 meses como máximo; las páginas públicas no usan cookies de analítica ni de publicidad; el panel de administración usa cookies de sesión estrictamente necesarias.

- **Notificaciones y solicitudes**: nombre y correo electrónico (salvo la excepción del art. 16.2.c del Reglamento (UE) 2022/2065), contenido de la notificación, tienda, fecha y hora indicadas, documentos adjuntos, nuestras decisiones y respuestas.
- **Contacto de minoristas**: identidad y cargo de la persona de contacto, cadena y establecimientos, acreditación aportada, decisiones (exclusión, correcciones) y correspondencia.

3.E Acceso con Google o Apple (mapeadores y compradores)

Además de con un código enviado a su correo, puede entrar con su cuenta de Google (en Android e iOS) o de Apple (en iOS). En ese caso:

- Google o Apple comprueban su identidad en sus propios sistemas y nos envían un **token firmado**. De él solo guardamos su **dirección de correo** (o la dirección de reenvío que Apple crea si elige «Ocultar mi correo»), que debe estar verificada, y el **identificador de su cuenta** en ese servicio.
- El nombre y la foto que Google incluye en el token **se descartan antes de guardar nada**, y a Apple solo le pedimos el correo. No conservamos el token.
- Si ya tenía una cuenta con la misma dirección de correo verificada, entrará en esa misma cuenta.
- Si entra con Apple, guardamos además, **cifrado**, un token de Apple cuya única función es pedir a Apple que retire el acceso de MercaMap a su Apple ID cuando suprima su cuenta (lo exige la directriz 5.1.1(v) de App Store).

4. Finalidades y bases jurídicas

Ref.: P1
Finalidad: Crear y gestionar su cuenta, autenticarle por código de un solo uso enviado al correo o con su cuenta de Google o Apple (§3.E), mantener sus sesiones y dispositivos, enviarle notificaciones transaccionales
Datos: Cuenta, tokens push
Base jurídica: Contrato (RGPD art. 6.1.b)
Plazo (véase §10): Hasta la supresión de la cuenta

Ref.: P2
Finalidad: Recibir, validar y procesar sus sesiones de mapeo: reconstruir el recorrido, identificar productos y su ubicación, fusionarlo con el mapa de la tienda y calcular los puntos según la tabla pública
Datos: Sesiones, fotogramas, telemetría (incluida la trayectoria en la tienda), datos derivados, libro de puntos
Base jurídica: Contrato (art. 6.1.b) respecto de sus propios datos; **interés legítimo** (art. 6.1.f) respecto de las imágenes de terceros: construir un conjunto de datos de ubicación de productos para guiar a compradores y elaborar estadísticas agregadas (evaluación interna de interés legítimo)
Plazo (véase §10): Fotogramas 14/30 días; telemetría bruta 90 días; derivados mientras el mapa sea útil

---

Ref.: P3
Finalidad: Prevenir y detectar el fraude y proteger la seguridad del servicio: límites de frecuencia, detección de duplicados, comprobación de ubicación al inicio (si dio permiso), plausibilidad de la telemetría y del recorrido, comprobación de "interior de supermercado", detección de rostros residuales, atestación del dispositivo
Datos: Sesiones, fotogramas, telemetría, dispositivo
Base jurídica: Interés legítimo (art. 6.1.f; considerandos 47 y 49): prevenir el fraude y garantizar la seguridad de la red y de la información; evaluación interna de interés legítimo
Plazo (véase §10): Como P2; marcas de fraude 6 años con el libro de puntos

---

Ref.: P4
Finalidad: Revisar sesiones por una persona, emitir motivaciones escritas y resolver recursos
Datos: Sesiones, fotogramas, decisiones
Base jurídica: Contrato (art. 6.1.b) y obligación legal (art. 6.1.c: Reglamento (UE) 2022/2065 arts. 16 y 17)
Plazo (véase §10): Tickets 3 años desde el cierre

Ref.: P5
Finalidad: Pagar las recompensas por transferencia SEPA, verificar su identidad y su mayoría de edad en el primer pago, prevenir la suplantación (periodo de espera de 72 h tras cambiar el IBAN)
Datos: IBAN, NIF, imagen del DNI/NIE (temporal), marca de verificación, pagos
Base jurídica: Contrato (art. 6.1.b); obligación legal (art. 6.1.c: conservación de la documentación mercantil, Código de Comercio art. 30; obligaciones de información tributaria, Ley 58/2003 art. 93); interés legítimo en evitar el fraude y la participación de menores (art. 6.1.f)
Plazo (véase §10): Imagen del documento: supresión al decidir (máx. 30 días); pagos y libro 6 años

---

Ref.: P6
Finalidad: Emitir cada enero la declaración anual de recompensas del año anterior y conservarla
Datos: Libro de puntos, pagos
Base jurídica: Contrato (art. 6.1.b)
Plazo (véase §10): 6 años

Ref.: P7
Finalidad: Prestar el servicio de compra: tiendas cercanas, búsqueda de productos en la tienda, listas y compartición con su hogar, cálculo de la ruta, viaje guiado, historial de viajes, señal "no encontrado" para actualizar el mapa
Datos: Uso del servicio, ubicación aproximada (no conservada), listas, viajes
Base jurídica: Contrato (art. 6.1.b)
Plazo (véase §10): Hasta la supresión de la cuenta; puede borrar listas y viajes en cualquier momento

---

Ref.: P8
Finalidad: Analítica de compra seudonimizada: registrar qué se compra, se omite o no se encuentra, dónde y con qué frecuencia, para elaborar estadísticas agregadas que mejoren los mapas y que, a partir de una versión posterior, se ofrecerán a marcas y tiendas **solo en forma agregada**
Datos: Eventos de compra bajo seudónimo, resúmenes por parada
Base jurídica: Consentimiento explícito y separado (art. 6.1.a; LOPDGDD art. 7), mediante el interruptor "compartir estadísticas anónimas de compra con marcas y tiendas", nunca condición para usar la app; la transmisión de datos de sensores requiere además su consentimiento conforme a la LSSI art. 22.2
Plazo (véase §10): Eventos 13 meses; sal de seudonimización hasta la retirada del consentimiento

---

Ref.: P9
Finalidad: Elaborar y, en su caso, comercializar **agregados** (producto × tienda × semana, etc.) en los que ninguna celda corresponde a menos de 10 compradores, con supresión complementaria
Datos: Agregados (información anónima)
Base jurídica: Los agregados no son datos personales (RGPD considerando 26); su elaboración es parte de P8 y se apoya en el mismo consentimiento; **finalidad declarada desde ahora** conforme al art. 5.1.b
Plazo (véase §10): Indefinido

Ref.: P10
Finalidad: Analítica de producto (PostHog, servidores en la UE): comprender qué pantallas se usan y dónde fallan los flujos
Datos: Identificador de instalación, eventos de uso de pantallas, modelo de dispositivo, versión; sin identificadores publicitarios
Base jurídica: Consentimiento (art. 6.1.a; LSSI art. 22.2), desactivada por defecto
Plazo (véase §10): 12 meses

Ref.: P11
Finalidad: Informes de errores (Sentry, organización en la UE): detectar fallos y caídas de la app y del servidor; y, **solo durante la fase de pruebas**, el **registro técnico de diagnóstico** de las cuentas de nuestro equipo (§3.A), para corregir fallos del mapeo
Datos: Errores: traza técnica del error, modelo de dispositivo, versión, identificador seudónimo; sin correo ni nombre. Registro técnico: los datos descritos en §3.A, vinculados a la cuenta

Base jurídica: Interés legítimo (art. 6.1.f): mantener la seguridad y el funcionamiento del servicio y corregir sus fallos; acceso al dispositivo estrictamente necesario para el servicio solicitado (LSSI art. 22.2)
Plazo (véase §10): Errores: 90 días (ventana del plan de Sentry); registro técnico: 30 días

---

Ref.: P12
Finalidad: Enviar correos y notificaciones transaccionales (código de acceso, sesión procesada, recompensa aprobada, pago enviado, respuesta a un recurso, avisos legales)
Datos: Correo, tokens push
Base jurídica: Contrato (art. 6.1.b); nunca enviamos comunicaciones comerciales sin su consentimiento previo (LSSI art. 21)
Plazo (véase §10): Hasta la supresión de la cuenta

Ref.: P13
Finalidad: Atender notificaciones, solicitudes de supresión de terceros, solicitudes de derechos, contactos de minoristas y soporte
Datos: 3.D, solicitudes
Base jurídica: Obligación legal (art. 6.1.c: RGPD arts. 12–22; Reglamento (UE) 2022/2065 arts. 16–17); interés legítimo en la defensa frente a reclamaciones (art. 6.1.f)
Plazo (véase §10): 3 años desde el cierre

Ref.: P14
Finalidad: Registros de seguridad y auditoría: registrar cada acción de administración y cada decisión automatizada, limitar tasas, detectar accesos anómalos
Datos: Registros con identificadores seudónimos y hash de IP
Base jurídica: Interés legítimo (art. 6.1.f; considerando 49); responsabilidad proactiva (art. 5.2)
Plazo (véase §10): Logs 12 meses; auditoría 6 años

Ref.: P15
Finalidad: Cumplir obligaciones contables y fiscales, y bloquear los datos tras la supresión durante los plazos de prescripción
Datos: Libro de puntos, pagos, perfil de pago
Base jurídica: Obligación legal (art. 6.1.c: Código de Comercio art. 30; Ley 58/2003 art. 66; LOPDGDD art. 32)
Plazo (véase §10): 6 años, bloqueados

Ref.: P16
Finalidad: Prestar el sitio web y la consola de administración
Datos: Registros técnicos, cookies estrictamente necesarias
Base jurídica: Interés legítimo (art. 6.1.f); LSSI art. 22.2 (estrictamente necesarias)
Plazo (véase §10): 12 meses

Ref.: P17
Finalidad: Depuración de la app durante la fase de pruebas (temporal; como tarde hasta el 31 de diciembre de 2026): vídeo de depuración grabado solo en el teléfono de una persona de nuestro equipo durante sus propias pruebas (§6)
Datos: Imágenes de la cámara sin pixelar, que pueden mostrar a personas, con las lecturas de los sensores de movimiento y datos técnicos del teléfono; sin audio ni ubicación
Base jurídica: Interés legítimo (art. 6.1.f): comprobar y corregir el seguimiento, la detección y el pixelado antes de abrir el mapeo automático a más personas (evaluación interna de interés legítimo §4.E)
Plazo (véase §10): 7 días en el teléfono; nunca se sube

No hacemos: reconocimiento facial, inferencia de edad, sexo, emociones u otras características a partir de imágenes; evaluación de su rapidez, su diligencia o su rendimiento a partir de su recorrido; publicidad personalizada; venta de datos individuales; seguimiento entre aplicaciones (no usamos el marco App Tracking Transparency porque no rastreamos); decisiones basadas únicamente en tratamiento automatizado con efectos jurídicos (véase §13).

5. Qué ocurre en su teléfono (mapeadores)

1. Mientras graba, la app muestra un **rótulo permanente de "grabando"**. En Android, si el teléfono admite realidad aumentada (ARCore), la app usa la imagen de la cámara **en memoria** para calcular la posición y los giros del teléfono en la tienda y detectar pasillos y zonas; esa imagen no se guarda ni se envía. Sin realidad aumentada, el recorrido se calcula con los sensores de movimiento.
2. La app toma fotogramas fijos de las estanterías (del orden de uno por segundo al caminar). Dos detectores en el propio teléfono buscan **personas** (cuerpo entero) y **rostros**; sus cajas se unen, se amplían un 30 % y se **pixelan** con bloques de 16 píxeles. Con realidad aumentada, para no dejar a nadie sin pixelar, la app busca también personas en hasta dos imágenes pequeñas tomadas justo antes y después de cada fotograma, que solo existen en memoria y nunca se guardan ni se envían. Solo la imagen pixelada se escribe en el almacenamiento de la app. **No se graba audio, la app no sube vídeo y ninguna imagen sin pixelar se almacena ni se envía**, con la única excepción temporal descrita en §6 (el vídeo de depuración de las pruebas de nuestro equipo, que nunca se sube).
3. El teléfono cifra localmente la cola de subida y envía fragmentos firmados a nuestro almacenamiento privado en Fráncfort.
4. El servidor vuelve a pasar un detector de rostros sobre cada fotograma ya pixelado; si encuentra un rostro residual, lo pixela de nuevo o pone el fotograma en cuarentena.
5. El pixelado es irreversible: no conservamos las imágenes originales.

Ningún sistema de detección es perfecto. Por eso le pedimos que **no enfoque a personas**, cajas, terminales de pago, mostradores de farmacia ni zonas de personal, y por eso las imágenes se suprimen en plazos cortos (§10).

6. Terceros y personal de tiendas

Las personas que se encuentren en una tienda durante una grabación no son usuarias de la app. Publicamos para ellas un **aviso público** (mercamap.com/personas) que cumple el art. 14.5.b del RGPD, porque informarles individualmente es imposible. En resumen:

- Base jurídica: interés legítimo (art. 6.1.f) en construir un conjunto de datos de ubicación de productos para guiar a compradores y elaborar estadísticas; ponderación en evaluación interna de interés legítimo; evaluación de impacto en evaluación interna de impacto.
- Las imágenes llegan a nosotros ya pixeladas; **no podemos identificar** a las personas que aparecen y no conservamos información adicional para hacerlo (RGPD art. 11.1).
- Para pedir la supresión de las imágenes de una grabación basta indicar **tienda, fecha y hora aproximada** (art. 11.2): suprimimos todos los fotogramas de esa sesión y lo confirmamos en 10 días.
- Las imágenes **nunca** se comparten con la tienda, con el empleador del personal ni con terceros, no se publican y no se usan para evaluar a nadie.
- **Excepción temporal (fase de pruebas).** Hasta que termine la fase de pruebas cerrada, y como tarde el 31 de diciembre de 2026, cuando una persona de nuestro equipo (hoy, solo el responsable) prueba la app en Android con el modo de depuración activado, su teléfono puede guardar además una grabación de ARCore: las imágenes de la cámara que ARCore usa para el seguimiento (hasta la resolución de la imagen de cámara que usa la app), **sin pixelar**, que pueden mostrar a personas, con las lecturas de los sensores de movimiento y datos técnicos del teléfono y de ARCore; **sin audio ni ubicación**. La app nunca la sube a nuestros servidores y no se envía a encargados, servicios de inteligencia artificial ni terceros; solo el responsable puede copiarla a sus propios dispositivos, y únicamente para corregir errores de la app. La app la **borra automáticamente pasados 7 días** desde la grabación (y borra todas a la vez si se desactiva la función); las copias se borran en el mismo plazo. Mientras se graba, la pantalla lo indica. Puede pedir su supresión como se indica más arriba (tienda, fecha y hora aproximada).

7. Menores de edad

- **Compradores**: pueden usar la app a partir de los **14 años** (LOPDGDD art. 7.1; Código Civil art. 1263 para los contratos "relativos a bienes y servicios de la vida corriente propios de su edad"). Una pantalla neutra de fecha de nacimiento bloquea las cuentas de menores de 14 sin insistir ni sugerir otra fecha. No hay funciones sociales ni contenido generado por usuarios visible para otros, salvo las listas compartidas dentro del propio hogar. El consentimiento de analítica de compra (P8) solo lo puede otorgar el propio usuario si tiene 14 años o más.
- **Mapeadores**: deben tener **18 años**; lo declaran al registrarse y lo verificamos con su documento de identidad antes del primer pago. Si detectamos que un mapeador es menor, cerramos la cuenta, suprimimos sus fotogramas y no realizamos ningún pago.

8. Destinatarios y encargados del tratamiento

No vendemos ni cedemos datos personales individuales. Comunicamos datos únicamente a **encargados del tratamiento** que actúan bajo nuestras instrucciones con un contrato conforme al art. 28.3 del RGPD, y a autoridades cuando una obligación legal lo exige. Además, Google y Apple, cuando entra con ellos, y Google, a través de ARCore en Android, obtienen datos directamente como **responsables independientes** (véase más abajo). La lista completa, con la versión del contrato y las garantías de transferencia, está en registro de encargados del tratamiento (https://mercamap.com/legal/dpa-register) y se publica en mercamap.com/legal/encargados.

Encargado: Vercel Inc.
Servicio: Alojamiento de la API, funciones, flujos de procesamiento, almacenamiento privado de fotogramas (Blob), registros
Datos: Todos los datos que pasan por el servidor
Ubicación del tratamiento: Funciones y Blob en Fráncfort (`fra1`); registros de plataforma no fijados a región
Garantía de transferencia: DPF y cláusulas tipo (módulo 2)

Encargado: Supabase Pte. Ltd. (Singapur)
Servicio: Base de datos PostgreSQL
Datos: Cuentas, sesiones, listas, eventos seudonimizados, libro de puntos, perfiles de pago cifrados
Ubicación del tratamiento: AWS `eu-central-1` (Fráncfort); el soporte, los registros de la plataforma y las copias de seguridad del proveedor pueden tratarse fuera de la UE
Garantía de transferencia: Cláusulas contractuales tipo (módulo 2), con las adendas del Reino Unido y Suiza; Supabase no está adherida al Marco de Privacidad de Datos; subencargado de soporte en EE. UU. (Supabase, Inc.)

Encargado: Upstash
Servicio: Límites de frecuencia y caché
Datos: Identificadores seudónimos, contadores
Ubicación del tratamiento: AWS `eu-central-1`
Garantía de transferencia: DPF (Upstash, Inc.) y cláusulas tipo (módulos 2 y 3)

Encargado: Resend
Servicio: Envío de correos (códigos de acceso, avisos)
Datos: Correo electrónico, contenido del mensaje (sin fotogramas, NIF ni IBAN)
Ubicación del tratamiento: Envío desde la UE; datos de cuenta y registros en EE. UU.
Garantía de transferencia: DPF y cláusulas tipo

Encargado: Proveedores de inteligencia artificial a través de Vercel AI Gateway: Amazon Web Services (Bedrock), Google Cloud (Vertex AI), Microsoft (Azure)
Servicio: Análisis de los fotogramas pixelados (lectura de carteles y productos) y cálculo de representaciones de nombres de producto

Datos: Fotogramas pixelados, texto de productos
Ubicación del tratamiento: Regiones de la UE (`inferenceRegion: eu`), con **retención cero de datos**: el proveedor no almacena las imágenes ni las usa para entrenar modelos
Garantía de transferencia: Subencargados listados por Vercel; DPA de AWS, Google y Microsoft; DPF / cláusulas tipo

---

Encargado: Functional Software, Inc. (Sentry)
Servicio: Informes de errores
Datos: Trazas técnicas, identificador seudónimo
Ubicación del tratamiento: Organización en la UE (Fráncfort, `de.sentry.io`)
Garantía de transferencia: DPF y cláusulas tipo para datos de cuenta

---

Encargado: PostHog, Inc.
Servicio: Analítica de producto (solo con consentimiento)
Datos: Eventos de uso, identificador de instalación
Ubicación del tratamiento: Nube UE (`eu.i.posthog.com`, Fráncfort)
Garantía de transferencia: DPF y cláusulas tipo para datos de cuenta

---

Encargado: Better Stack
Servicio: Registros, monitorización y estado
Datos: Registros con identificadores seudónimos
Ubicación del tratamiento: Centros de datos en la UE (por defecto)
Garantía de transferencia: Cláusulas tipo (anexo D del DPA; no figura en la lista del DPF)

Encargado: 650 Industries, Inc. (Expo)
Servicio: Actualizaciones de la app (EAS Update) y envío de notificaciones push
Datos: Sistema operativo y token aleatorio de actualización; token push y contenido de la notificación (en memoria, solo hasta su entrega)
Ubicación del tratamiento: EE. UU.
Garantía de transferencia: DPF y cláusulas tipo (módulo 2)

Encargado: Apple Inc. / Google LLC
Servicio: Entrega de notificaciones push (APNs / FCM)
Datos: Token push, contenido de la notificación
Ubicación del tratamiento: Servicios globales
Garantía de transferencia: Google: DPF. Apple: cláusulas contractuales tipo (Apple Distribution International Ltd., Irlanda, responde de los datos del EEE)

Encargado: Google LLC / Google Ireland Limited (Servicios de Google Play para RA, ARCore), solo Android: **responsable independiente, no encargado**
Servicio: Seguimiento de realidad aumentada en el teléfono
Datos: Datos de uso y diagnóstico de ARCore que Google recoge por su cuenta: identificadores de su cuenta de Google (si tiene sesión iniciada) o del dispositivo, rendimiento y diagnóstico, y llamadas de la app a ARCore; no las imágenes de la cámara ni la posición en la tienda
Ubicación del tratamiento: Según Google (Política de Privacidad de Google)
Garantía de transferencia: Google LLC: DPF

Encargado: Autoridades públicas
Servicio: Cuando la ley lo exige (Administración tributaria, jueces y tribunales, AEPD, Fuerzas y Cuerpos de Seguridad)
Datos: Los datos requeridos
Ubicación del tratamiento: España / UE
Garantía de transferencia: Obligación legal

Google y Apple no tratan datos por nuestra cuenta cuando entra con ellos: comprueban su identidad en su propia cuenta, bajo sus políticas de privacidad (policies.google.com/privacy y apple.com/es/legal/privacy) y

como **responsables independientes**, y nosotros solo recibimos el resultado (correo e identificador). Cuando suprime una cuenta con la que entró con Apple, enviamos a Apple el token de revocación descrito en §3.E.

ARCore. Esta aplicación se ejecuta en los Servicios de Google Play para RA (ARCore), que proporciona Google y se rige por su Política de Privacidad (policies.google.com/privacy). En Android, cuando la app usa la realidad aumentada, Google recoge a través de ARCore, como responsable independiente y no por cuenta nuestra, los datos de uso y diagnóstico indicados en la tabla. El seguimiento se calcula en el teléfono y no usamos las funciones de ARCore que envían a Google imágenes de la cámara o la ubicación (anclajes en la nube, API geoespacial). ARCore es opcional: si su teléfono no lo admite o prefiere no instalarlo, puede mapear con los sensores de movimiento.

En una versión posterior podremos usar Stripe (pagos a mapeadores) y MotherDuck (agregados anónimos); antes de activarlos actualizaremos esta política y el registro de encargados.

9. Transferencias internacionales

Nuestros sistemas principales están en la Unión Europea (Fráncfort). Algunos encargados están establecidos en Estados Unidos o en Singapur (Supabase), o pueden acceder a datos desde allí (soporte, datos de cuenta, entrega de notificaciones). Esas transferencias se amparan en el Capítulo V del RGPD:

- **Decisión de adecuación** (art. 45): Decisión de Ejecución (UE) 2023/1795 de la Comisión, de 10 de julio de 2023, sobre el Marco de Privacidad de Datos UE-EE. UU., para las entidades certificadas en dicho marco.
- **Cláusulas contractuales tipo** (art. 46.2.c): Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, incorporadas en los contratos de encargo como garantía subsidiaria, con una evaluación de impacto de la transferencia.
- El Tribunal General desestimó el 3 de septiembre de 2025 el recurso contra la Decisión 2023/1795 (asunto T-553/23, Latombe/Comisión); está pendiente el recurso de casación C-703/25 P, interpuesto el 31 de octubre de 2025. Si la Decisión fuera anulada, pasaríamos de inmediato a las cláusulas tipo con evaluación de impacto y a proveedores exclusivamente europeos donde sea necesario (calendario interno de seguimiento).

El acceso con Google o Apple lo prestan esas empresas en su relación directa con usted: en el EEE responden de su cuenta Google Ireland Limited y Apple Distribution International Ltd. (Irlanda), y cada una ampara sus propias transferencias (Google, en el Marco de Privacidad de Datos; Apple, en cláusulas contractuales tipo). Si entró con Apple, al suprimir su cuenta enviamos a Apple el token que la propia Apple emitió para ella, para que retire el acceso; en la medida en que ese envío sea una transferencia, es ocasional y necesario para ejecutar la supresión que usted pide (RGPD art. 49.1.b). Lo mismo ocurre con los datos de uso y diagnóstico de ARCore (§8): Google los trata en su relación directa con usted, según su Política de Privacidad, y ampara sus propias transferencias en el Marco de Privacidad de Datos.

Puede pedir copia de las garantías aplicables en privacidad@mercamap.com.

10. Conservación

Aplicamos el calendario de calendario interno de conservación, implementado como trabajos automáticos que registran cada supresión y la verifican al día siguiente. Resumen:

Datos: Fotogramas con una persona detectada (ya pixelada) **Plazo:** 14 días desde la extracción del mapa	
Datos: Fotogramas sin persona detectada **Plazo:** 30 días desde la subida	

Datos: Telemetría bruta (incluidas la trayectoria en la tienda y sus copias en los datos de cada fotograma y en el mapa de la sesión) y GPS de inicio/fin
Plazo: 90 días

Datos: Datos derivados (productos, ubicaciones, mapas)
Plazo: Mientras el mapa sea útil; se desvinculan de su cuenta al suprimirla

Datos: Cuenta, listas, viajes
Plazo: Hasta la supresión de la cuenta (o 36 meses de inactividad, con aviso previo)

Datos: Eventos de compra seudonimizados
Plazo: 13 meses

Datos: Sal de seudonimización
Plazo: Hasta la retirada del consentimiento o la supresión de la cuenta (supresión inmediata)

Datos: Imagen del DNI/NIE
Plazo: Al decidir la verificación; máximo 30 días

Datos: Libro de puntos, pagos, IBAN y NIF, declaraciones anuales, registro de auditoría
Plazo: 6 años (Código de Comercio art. 30), bloqueados tras la supresión de la cuenta (LOPDGDD art. 32)

Datos: Tickets, notificaciones y solicitudes de derechos
Plazo: 3 años desde el cierre

Datos: Registros técnicos
Plazo: 12 meses (Vercel: 30 días)

Datos: Informes de errores
Plazo: 90 días

Datos: Registro técnico de diagnóstico (fase de pruebas, cuentas de nuestro equipo)
Plazo: 30 días

Datos: Vídeo de depuración (fase de pruebas, solo en el teléfono de nuestro equipo; nunca se sube)
Plazo: 7 días desde la grabación; todos se borran al desactivar la función

Datos: Analítica de producto
Plazo: 12 meses

Datos: Token de Apple para revocar el acceso (solo si entró con Apple)
Plazo: Hasta la supresión de la cuenta: en ese momento se revoca ante Apple y se borra

Datos: Copias de seguridad
Plazo: Hasta 35 días; los datos suprimidos pueden persistir en ellas ese tiempo

Conjunto de mejora de modelos. En el lanzamiento no conservamos ningún fotograma más allá de los plazos anteriores para mejorar nuestros detectores. Si en el futuro creáramos un conjunto con ese fin, solo incluiría fotogramas en los que ambos detectores no encontraron a nadie, revisados por muestreo por una persona, desvinculados de la sesión y de la cuenta, con la fecha redondeada al mes y sin geolocalización, con un tamaño máximo de 5000 fotogramas y una conservación máxima de 24 meses; lo anunciaríamos en esta sección antes de crearlo.

10 bis. Dictado por voz, entrada de la tienda, tiendas que faltan y mapa

- **Dictado de la lista (compradores).** Puede decir en voz alta lo que quiere comprar. El reconocimiento de voz se ejecuta **en su teléfono** con el reconocedor del sistema operativo en modo sin conexión; el audio **no se graba, no se guarda y no se envía** a nuestros servidores ni a terceros. Solo el texto resultante

(los productos nombrados) se trata como el resto de su lista, sobre la base del contrato (art. 6.1.b RGPD). Si su teléfono no puede reconocer voz sin conexión, el dictado no está disponible y puede escribir los productos.

- **Posición de la entrada (mapeadores).** Al empezar una sesión le pedimos que se coloque en la puerta y, si ha concedido el permiso de ubicación, registramos una posición GPS de la entrada (latitud, longitud y precisión) asociada a la sesión. Con ella calculamos una **estimación agregada** de la puerta de cada tienda (mediana ponderada de varias sesiones), que se muestra a los compradores para guiarles hasta la entrada. La estimación no identifica a ningún mapeador; la posición de su sesión se conserva con los metadatos de la sesión según la tabla de conservación. El permiso de ubicación sigue siendo opcional y nunca condiciona la recompensa (base: interés legítimo, art. 6.1.f RGPD, construir un mapa de tiendas útil).
- **Tiendas que faltan (mapeadores).** Los mapeadores no crean tiendas: pueden avisarnos de una que no está en el directorio (cadena, nombre, dirección y la posición aproximada de su teléfono). El aviso se guarda como una solicitud asociada a su cuenta y a su correo para validarla y avisarle cuando la tienda esté disponible, y se conserva como el resto de avisos y consultas (apartado 10). La ficha que publicamos describe un establecimiento, no a una persona.
- **Vista de mapa.** Cuando abre el mapa de tiendas, las imágenes del mapa se descargan desde OpenFreeMap, un servicio independiente con sede en Hungría que puede usar la red de Cloudflare. Como en cualquier descarga, esos servidores reciben su dirección IP y la zona del mapa que está viendo; OpenFreeMap declara que no registra direcciones IP en funcionamiento normal y que no usa cookies. Si no abre el mapa, no se hace ninguna petición a ese servicio.
- **Directorio de tiendas.** Nombre, cadena, dirección y posición de las tiendas proceden de OpenStreetMap y del geocodificador CartoCiudad del Instituto Geográfico Nacional; describen establecimientos, no personas.

11. Sus derechos

Puede ejercer en cualquier momento los derechos de **acceso** (art. 15), **rectificación** (art. 16), **supresión** (art. 17), **limitación** (art. 18), **portabilidad** (art. 20) y **oposición** (art. 21), y a **no ser objeto de decisiones basadas únicamente en tratamiento automatizado** (art. 22):

- **En la app**: Ajustes -> Privacidad y datos -> «Descargar mis datos» (fichero descargable, disponible en un plazo máximo de 30 días, con enlace válido 7 días) y «Eliminar mi cuenta» (supresión ejecutada en un plazo máximo de un mes; los datos sujetos a obligaciones legales quedan bloqueados, §10). También puede solicitar la supresión desde el sitio web: mercamap.com/account/delete. Si entró con Apple, la supresión incluye pedir a Apple que retire el acceso de MercaMap a su Apple ID.
- **Por escrito**: privacidad@mercamap.com o Portichol 83, 03670 Monforte del Cid (Alicante). Respondemos en el plazo máximo de un mes (art. 12.3), ampliable dos meses más en casos complejos, informándole. Podemos pedirle que confirme su identidad mediante el código de acceso enviado a su correo; nunca le pediremos su documento de identidad para ejercer derechos, salvo que sea imprescindible.
- **Retirada del consentimiento** (art. 7.3): los interruptores de "analítica de compra" y "analítica de producto" en Ajustes -> Privacidad y datos -> «Consentimientos de analítica» pueden desactivarse en cualquier momento, con efecto inmediato y sin afectar a la licitud del tratamiento anterior. Al retirar el consentimiento de analítica de compra suprimimos su sal de seudonimización, de modo que los eventos ya registrados dejan de poder vincularse a usted.
- **Oposición** (art. 21.1): puede oponerse, por motivos relacionados con su situación particular, a los tratamientos basados en interés legítimo (P2 respecto de imágenes de terceros, P3, P11, P14, P16, P17); dejaremos de tratar los datos salvo que acreditemos motivos legítimos imperiosos que prevalezcan

o la formulación, ejercicio o defensa de reclamaciones. En el caso de las imágenes de terceros, aplicamos el procedimiento de la sección 6.

- **Terceros que puedan aparecer en imágenes** (art. 11): no podemos identificarle; indíquenos tienda, fecha y hora y suprimiremos los fotogramas de esa sesión.
- **Representación**: puede ejercer los derechos por medio de representante legal o voluntario (LOPDGDD art. 12.1).

Si considera que no hemos atendido correctamente sus derechos, puede presentar una **reclamación ante la Agencia Española de Protección de Datos** (art. 77): www.aepd.es · C/ Jorge Juan, 6, 28001 Madrid · sede electrónica sedeagpd.gob.es. Le agradeceremos que nos escriba antes para intentar resolverlo.

12. Seguridad

Aplicamos medidas técnicas y organizativas adecuadas al riesgo (RGPD art. 32): pixelado irreversible en el dispositivo y segunda pasada en el servidor; realidad aumentada solo con funciones que se ejecutan en el teléfono; cifrado en tránsito y en reposo; cifrado de sobre (AES-256-GCM) de IBAN y NIF con claves gestionadas por separado y rotadas trimestralmente; seudonimización de los datos de compra con claves y sales en tablas de acceso restringido; roles de base de datos con mínimo privilegio; autenticación de administradores con llave de acceso y segundo factor; principio de cuatro ojos en los pagos; registro de auditoría inalterable de toda acción administrativa; regiones de la UE para almacenamiento y base de datos; subida mediante URL firmadas de un solo uso; retención automatizada con pruebas de supresión; procedimiento de gestión de brechas con notificación a la AEPD en 72 horas (procedimiento interno de brechas); evaluación anual de seguridad. Ninguna medida elimina totalmente el riesgo; si se produjera una brecha que pudiera afectarle de forma grave, se lo comunicaríamos (art. 34).

13. Decisiones automatizadas

El cálculo de puntos y las comprobaciones antifraude son automáticos y se explican en mercamap.com/algoritmo. Toda decisión desfavorable (rechazo, reducción o marca de una sesión) se le notifica con una motivación escrita y puede recurrirse ante una persona; las tres primeras sesiones de cada persona y toda sesión marcada se revisan por una persona antes de ser definitivas; los importes están limitados por topes. Con estas garantías, entendemos que no adoptamos decisiones basadas únicamente en el tratamiento automatizado con efectos jurídicos o significativos (art. 22.1); si eso cambiara, aplicaríamos las garantías del art. 22.3 (intervención humana, derecho a expresar su punto de vista y a impugnar la decisión). No elaboramos perfiles de mapeadores ni de compradores para evaluarlos.

14. Analítica, informes de errores y dispositivos de almacenamiento

- **Analítica de producto (PostHog UE)**: desactivada por defecto; solo se activa si usted la enciende en Ajustes -> Privacidad y datos -> «Consentimientos de analítica»; no usa identificadores publicitarios ni cruza datos con otras aplicaciones o sitios; no invocamos la exención de consentimiento para medición de audiencia descrita en la guía de la AEPD "Uso de cookies para herramientas de medición de audiencia" (enero de 2024), sino que pedimos consentimiento (LSSI art. 22.2; RGPD art. 6.1.a).
- **Informes de errores (Sentry UE)**: consideramos su envío estrictamente necesario para prestar el servicio de forma segura (LSSI art. 22.2, último inciso); no incluyen su correo ni su nombre; en las sesiones de mapeo incluyen además un resumen técnico de la captura (tiempos y recuentos), sin imágenes ni posiciones; puede solicitar su supresión.
- **App Tracking Transparency / identificadores publicitarios** no rastreamos ni usamos identificadores publicitarios; la app no muestra el diálogo de seguimiento de Apple porque no realiza seguimiento.
- **Sitio web**: solo cookies estrictamente necesarias; sin analítica ni publicidad en las páginas públicas.

15. Cambios en esta política

Publicaremos las modificaciones en mercamap.com/privacidad con su fecha y un resumen de cambios, y se las comunicaremos en la app con al menos 30 días de antelación cuando afecten a finalidades, bases jurídicas, destinatarios o plazos. Si un cambio requiere un nuevo consentimiento, se lo pediremos expresamente y, hasta entonces, no aplicaremos el tratamiento afectado. Conservamos las versiones anteriores.

Versión 28 de septiembre de 2026. Texto vinculante en español.