ECOMTPV · FIDELIZACIÓN · PLAN DEFINITIVO

Fidelización con avisos de proximidad

La propuesta «Fidelización sin App», **corregida con lo que de verdad permiten Apple y Google en 2026** y con lo que permite la Agencia Española de Protección de Datos. Lo que se puede construir, lo que hay que tachar y lo que hay que tocar en el TPV.

Septiembre de 2026 · Sustituye a `otras cosas/fidelizacion-wallet.html` en todo lo relativo a proximidad

---

CONTENIDO

1. La corrección: no existe el evento de proximidad
2. Qué se tacha del plan original
3. Lo que sí se puede construir
4. Lo que está muerto, y por qué no volver a proponerlo
5. Lo legal en España, en decisiones
6. Qué hay que tocar en EcomTPV

LO PRIMERO

CORRECCIÓN DE PARTIDA

El geofence del wallet no devuelve nada al comercio

La propuesta original da por hecho que, cuando el cliente pasa cerca del local, el sistema avisa al comercio: de ahí salían el evento `cerca_del_local` hacia Brevo y la automatización «Proximidad, con

tope de frecuencia». **Eso no existe.** Ni Apple ni Google devuelven ningún *callback*, ningún registro y ninguna marca de hora al emisor del pase.

El servicio web de pases de Apple tiene exactamente cuatro extremos —registrar un dispositivo, listar los pases cambiados desde una fecha, entregar el pase actualizado y desregistrar—, más un `/v1/log` de errores. **No hay ningún «este pase se ha mostrado» ni «este usuario está cerca».** Google, igual.

Qué significa exactamente

El aviso de proximidad del wallet sirve para **que al cliente le salte la tarjeta en el móvil**. Nada más. No sirve para disparar un WhatsApp, ni para atribuir una visita, ni para medir absolutamente nada. Cuatro consecuencias directas:

- **No se puede medir.** Nunca sabrás cuántas veces se ha mostrado el pase, ni a quién, ni cuándo.
- **No se puede encadenar.** «Cerca del local → mándale un mensaje» es un flujo que no se puede construir, porque falta el disparador.
- **No se puede limitar la frecuencia desde tu lado.** No hay contador que llevar. Lo único que controlas es retirar o mover las ubicaciones del pase por *push*, o cambiar el texto que se muestra.
- **La única atribución real sigue siendo el escaneo del código del pase en caja.** Esto la propuesta original ya lo dice bien, y es lo que hay que defender: es la única fuente de verdad del sistema.

> LO QUE HAY QUE DECIRLE AL CLIENTE ANTES DE FIRMAR
>
> «El pase le aparecerá al cliente en el móvil cuando esté cerca. Usted no va a poder saber cuántas veces ha pasado eso, ni a quién le ha pasado.» Dicho al principio es una limitación razonable; descubierto en el mes tres es una reclamación.

FUENTES DE ESTE APARTADO

Apple — *Adding a Web Service to Update Passes* (los únicos extremos que existen): developer.apple.com/documentation/WalletPasses/adding-a-web-service-to-update-passes

Apple — *Showing a Pass on the Lock Screen*: developer.apple.com/documentation/walletpasses/pass/showing_a_pass_on_the_lock_screen

Google — *MerchantLocation*: developers.google.com/wallet/reference/rest/v1/MerchantLocation

CORRECCIÓN PUNTO POR PUNTO

Qué se tacha del plan original

Cinco cosas. Cuatro se tachan enteras o se reescriben; la quinta es un dato que faltaba y que cambia lo que se puede prometer.

EN EL PLAN ORIGINAL	VEREDICTO	CON QUÉ SE SUSTITUYE
Automatización n.º 6: ~~«Proximidad. Geofence del pase, con tope de frecuencia»~~	Se tacha	No hay evento, luego no hay contador ni tope que poner. Se reescribe como «Relevancia por ubicación», que no es una automatización sino una propiedad estática del pase. Las automatizaciones bajan de seis a cinco.
Evento ~~`cerca_del_local`~~ en la lista de eventos que se emiten hacia Brevo o Klaviyo	Se tacha	No se puede emitir. Los eventos que sí existen y sí se emiten son `alta`, `visita`, `compra`, `sello` e `inactivo_30d`.
Fase 3 del plan: ~~«Geofence en el pase con control de frecuencia»~~ (2 semanas)	Se tacha	El geofence se configura al emitir el pase, en la fase 1. No es un desarrollo de dos semanas: son dos campos en la configuración del local. La fase 3 se queda solo con el flujo de reseñas.

EN EL PLAN ORIGINAL	VEREDICTO	CON QUÉ SE SUSTITUYE
«~~No se pide permiso.~~ **El geofence corre en el dispositivo. Fricción: ninguna»**	**Se matiza**	Correcto en Apple. En Android el usuario tiene que haber concedido a la app Google Wallet **ubicación precisa y «siempre»**, más las notificaciones. No se lo pides tú, pero es una puerta que puede estar cerrada y que va a generar avisos del tipo «a mi cliente no le sale».
Radio del geofence: ***no aparece en el plan original***	**Se añade**	Es un límite real y hay que escribirlo: **~100 m** en Apple para una tarjeta de sellos (`storeCard`). En Google lo decide Google y no lo publica.

Lo demás del plan original se mantiene: el pase como identificador, el escaneo en caja como única fuente de verdad, la captación por NFC y QR, los consentimientos separados por canal, la prohibición de premiar reseñas y los sensores cenitales fuera del proyecto mínimo.

> LO QUE NO CAMBIA
>
> El giro conceptual sigue siendo correcto y es lo mejor de la propuesta original: **el pase no es el premio, es el identificador**. Lo que cambia es que de ese identificador cuelga menos de lo que se pensaba: cuelga la identidad en caja y el canal de mensajes, no la señal de presencia.

LO VIABLE

Lo que sí se puede construir

En orden de esfuerzo contra beneficio. Para cada vía: qué hace, qué límites exactos tiene, qué hace falta dentro y fuera del TPV, cuánto cuesta y qué riesgo legal trae.

VÍA	¿AVISA?	¿DETECTA?	¿SIN APP?	RIESGO LEGAL
1. Pase de wallet con ubicaciones	**Sí**	**No**	**Sí**	**Prácticamente nulo**
2. Captación por NFC (y QR)	**No**	**No · capta**	**Sí**	**Nulo**
3. Web Push	**Android sí, iPhone testimonial**	**No**	**Sí**	**Bajo**
4. iBeacon dentro del pase	**Solo iPhone**	**No**	**Sí, con el pase ya instalado**	**Nulo**
5. Portal cautivo del wifi	**Después, por email o SMS**	**Solo de quien se conecta**	**Sí**	**ALTO**

Las cinco vías vivas. Ninguna detecta al cliente por su cuenta: la única detección real del sistema es que alguien enseñe su pase en caja.

1 · Pase de wallet con ubicaciones incrustadas

HAZLO · ES EL PRODUCTO

Es «sin app» de verdad, porque Wallet viene de fábrica en los dos sistemas operativos. El coste marginal es cero y el riesgo legal es prácticamente nulo, porque el geofence lo evalúa el teléfono —o Google— y al comercio no le llega ningún dato de ubicación.

Apple Wallet · la clave `locations` del `pass.json`

PARÁMETRO	VALOR
Ubicaciones por pase	`10 · máximo duro de Apple`
Radio (`maxDistance`)	**~100 m** para `storeCard`, `coupon` y `generic`, que es la tarjeta de sellos. Los ~1.000 m son solo para `eventTicket` y `boardingPass`

PARÁMETRO	VALOR
Precisión efectiva	Se suma la `horizontalAccuracy` del GPS: con `maxDistance` 5 y precisión 10, es relevante hasta 15 m
Quién escribe el texto	**Tú.** El `relevantText` de cada ubicación, una línea corta
Sonido o vibración	Ninguno. Es una sugerencia pasiva en la pantalla de bloqueo
Balizas iBeacon por pase	`10 identificadores distintos`
Fecha relevante	`1 relevantDate por pase`
Tope de frecuencia	Apple no publica ninguno

Apple lo dice con estas palabras: «*Relevance information is passive […] It doesn't present alerts or post notifications*». El tope de diez ubicaciones lo justifica por consumo de batería y por tamaño del fichero del pase.

Google Wallet · `MerchantLocation`

PARÁMETRO	VALOR
Ubicaciones	`10 por clase + 10 por objeto`
Radio	Lo decide Google y no lo publica. PassKit lo estima en **~150 m**. Estimación de un tercero, no dato oficial.
Permanencia mínima	La decide Google. No publicada
Quién escribe el texto	**Google.** No es personalizable. Es la diferencia grande con Apple
Sonido	Sí. Es una notificación normal de Android, con sonido
Tope de frecuencia	Google publica 3 por 24 h para las notificaciones de *mensaje*; **para las de proximidad no publica tope**.

PARÁMETRO	VALOR
	PassKit habla de 4 al día en total. Dato en conflicto: sin confirmar.
Requisitos en el teléfono	Notificaciones activadas y permiso de ubicación **precisa y «siempre»** concedido a la app Google Wallet
Disponibilidad	Desplegado a usuarios desde **diciembre de 2025**. Probarlo con un teléfono real en España antes de venderlo.

Se activa con el campo `locations` / `MerchantLocations` de la clase y del objeto, poniendo `notifyPreference` en `notifyOnUpdate`. Google ha añadido además un interruptor por pase, en el menú de tres puntos, para que el usuario apague estos avisos.

Qué hace falta

- **En EcomTPV:** latitud y longitud por local en la configuración, un campo para el texto del aviso y la lectura del código del pase en caja. Detalle en el apartado 6.
- **Fuera:** dominio con HTTPS y certificado válido —Apple **exige** TLS en el servicio web de pases—, un servicio que firme los `.pkpass` y emita los objetos de Google Wallet, y APNs para las actualizaciones de Apple.

Coste

- **Apple Developer Program: 99 € al año.** Una sola cuenta para toda la plataforma, no una por cliente. Incluye el certificado de Pass Type ID y el de la WWDR.
- **Google Wallet: 0 €.** Cuenta de emisor gratuita, pero con **aprobación previa** para producción: proyecto de Google Cloud más cuenta de servicio. Tarda unos días, hay que planificarlo.
- **Actualización de los pases por push: 0 €**, sin límite práctico.

Riesgo legal

Prácticamente nulo, y ese es el argumento de venta. Se resuelve con **una frase en la información del alta**. Desarrollado en el apartado 5.

FUENTES

Apple — *Wallet Developer Guide: Pass Design and Creation*: developer.apple.com/library/archive/documentation/UserExperience/Conceptual/PassKit_PG/Creating.html

Apple — *Pass.Locations*: developer.apple.com/documentation/walletpasses/pass/locations-data.dictionary

Apple Developer Forums — *Apple Wallet Pass Documentation · maxDistance?*: developer.apple.com/forums/thread/666620

Passworks — *What is the maximum value for maxDistance for Apple Wallet Pass?* (100 m en `storeCard`): help.passworks.io/maximum-distance-for-apple-wallet-passes

PassKit — *How many locations will trigger a lock screen message?*: help.passkit.com/en/articles/2010114-how-many-locations-will-trigger-a-lock-screen-message

PassKit — *GPS Location Notifications: Google Wallet vs Apple Wallet*: help.passkit.com/en/articles/12441270-gps-location-notifications-google-wallet-vs-apple-wallet

Google — *Trigger push notifications* (10 por clase y 10 por objeto, `notifyPreference`, texto controlado por Google): developers.google.com/wallet/retail/loyalty-cards/use-cases/trigger-push-notifications

9to5Google — *Google Wallet rolling out nearby notifications* (4/12/2025): 9to5google.com/2025/12/04/google-wallet-nearby-notifications/

AppleToolBox — *Boarding or Wallet Pass Doesn't Appear on Lock Screen* (ajustes que tienen que estar abiertos): appletoolbox.com/wallet-pass-doesnt-appear-lock-screen/

2 · Captación por NFC en el mostrador

HAZLO · VA CON LO ANTERIOR

No avisa y no detecta: **capta**, que es el paso previo a todo lo demás. Cuesta céntimos y no tiene ningún problema legal. La propuesta original ya lo tenía bien planteado y no hay nada que corregir.

PARÁMETRO	VALOR
iPhone sin ninguna app	Desde el **iPhone XS** (2018). El 7, el 8 y el X leen NFC pero necesitan una app: para ellos el plan B es el QR

PARÁMETRO	VALOR
Android	Prácticamente todos los modelos con NFC leen una etiqueta NDEF de tipo URL sin app
Etiqueta	NTAG213 adhesiva, **0,30 – 0,80 €** por unidad
Qué se graba	Un registro NDEF URI apuntando a la página de alta, con el local en la dirección
Soporte físico	Placa o expositor de sobremesa con NFC y QR impreso, **5 – 15 €**

NFC y QR en la misma placa, nunca uno en lugar del otro. El NFC cubre a quien lo tiene activado; el QR cubre al resto y al escaparate, donde no se puede acercar el teléfono.

Riesgo legal: nulo. Es el usuario el que acerca su teléfono voluntariamente y el que decide rellenar el formulario. Ni cartelería, ni evaluación de impacto, ni base jurídica que discutir más allá de la del propio formulario de alta.

En el TPV: nada. Como mucho, un botón que muestre en pantalla el código QR de alta para que el cliente lo escanee desde el otro lado del mostrador.

FUENTES

Apple — *Adding Support for Background Tag Reading*: developer.apple.com/documentation/corenfc/adding-support-for-background-tag-reading

GoToTags — *iOS Background NFC Tag Reading on iPhone* (iPhone XS o posterior): gototags.com/help/ios/nfc/reading/background

Seritag — *How to read NFC tags with an iPhone*: seritag.com/learn/using-nfc/how-to-read-nfc-tags-with-an-iphone

3 · Web Push

OPCIONAL · FASE TARDÍA

Vale para Android. En iPhone es testimonial y lo va a seguir siendo. **No lo pongas en el argumentario de venta como si fuera un canal:** el pase del wallet hace lo mismo, mejor, y en las dos plataformas.

PLATAFORMA	SITUACIÓN EN 2026
Android · Chrome	Funciona desde hace años sin instalar nada. El usuario visita la web, se le pide permiso, acepta y recibe notificaciones. **Coste: 0 €** con claves VAPID y servidor propio
iOS / iPadOS	Existe desde **iOS 16.4** (marzo de 2023), pero **solo si el usuario añade la web a la pantalla de inicio**: Compartir → Añadir a pantalla de inicio. Tres toques que casi nadie da por una cafetería
Safari 18.4	El *Declarative Web Push* quita la necesidad de un *service worker* y simplifica el código, pero **mantiene intacto el requisito de añadir a la pantalla de inicio**
Permiso	Solo se puede pedir tras una interacción directa del usuario
Cobertura	Más del 95 % de los iPhone del mundo van con iOS 16 o superior. El problema no es la versión: es el gesto de instalar

> BULO QUE CIRCULA
>
> Se lee a menudo que «las notificaciones web no están disponibles en la Unión Europea desde iOS 17.4». **Es falso.** Apple anunció en febrero de 2024 que retiraría las aplicaciones web de la pantalla de inicio en la Unión por el Reglamento de Mercados Digitales, y **dio marcha atrás el 1 de marzo de 2024**. Siguen funcionando.

Base jurídica: el permiso del navegador es un consentimiento válido si va acompañado de información previa (art. 13 RGPD) y de una forma de revocarlo. Como el push web guarda un extremo en el terminal, encaja además en el art. 22.2 LSSI, cuya excepción es el «servicio expresamente solicitado por el usuario» —y aquí lo está, porque él ha pulsado «Permitir». **Pon la información delante del diálogo del navegador, nunca detrás.**

En el TPV: nada. Fuera: claves VAPID, manifiesto de aplicación web y un *service worker*. Coste cero.

FUENTES

WebKit — *Web Push for Web Apps on iOS and iPadOS*: webkit.org/blog/13878/web-push-for-web-apps-on-ios-and-ipados/

WebKit — *Meet Declarative Web Push* (Safari 18.4): webkit.org/blog/16535/meet-declarative-web-push/

MacRumors — *Apple Walks Back Decision to Disable Home Screen Web Apps in the EU* (1/3/2024): macrumors.com/2024/03/01/apple-walks-back-decision-to-disable-eu-web-apps/

MobiLoud — *Do Progressive Web Apps Work on iOS?*: mobiloud.com/blog/progressive-web-apps-ios/

4 · iBeacon dentro del pase

SOLO POR ENCARGO

Es la única baliza Bluetooth que sigue viva en 2026, y sigue viva justamente porque va dentro del pase. El `pass.json` de Apple admite hasta **10 balizas** con su identificador, su texto y su nombre. El iPhone hace saltar el pase a la pantalla de bloqueo al acercarse a una baliza con ese identificador **sin ninguna aplicación instalada**… pero **con el pase ya instalado**.

- **No sirve para captar a nadie.** Solo funciona con quien ya es cliente del programa.
- **Solo iPhone.** Google Wallet no tiene equivalente.
- `CLBeaconRegion` está en desuso suave desde iOS 18: sigue funcionando y hay interfaz nueva.
- **Ventaja real sobre el GPS:** precisión de metros dentro del local, funciona en un centro comercial o en un sótano donde el GPS no llega, y no consume batería de GPS.
- **Coste: 15 – 40 € por baliza**, con pilas que hay que cambiar.
- **Riesgo legal: nulo.** Es el mismo mecanismo del pase.

Cuándo: local muy grande, sótano o centro comercial, donde el geofence de 100 m del GPS cubre veinte tiendas y no distingue la tuya. Fuera del proyecto mínimo.

FUENTES

Apple — *Pass.Beacons*: developer.apple.com/documentation/walletpasses/pass/beacons-data.dictionary

Apple Developer Forums — *Are several Proximity and Beacon related libraries deprecated in iOS 18?*: developer.apple.com/forums/thread/757110

PassKit — *Using Beacons with PassKit*: passkit.com/gemtot-beacons-eddystone-ibeacon-altbeacon/

5 · Portal cautivo del wifi

RIESGO ALTO · SOLO SI LO PIDEN

Funciona, es legal si se hace bien, y es **exactamente donde la Agencia Española de Protección de Datos ya ha puesto multas de más de 40.000 €**. No es una vía fácil: es la más peligrosa de las que sí funcionan.

Lo que exige, punto por punto

- **Información previa completa** —art. 13 RGPD: quién es el responsable, para qué, base jurídica, plazo, destinatarios y cómo ejercer los derechos. En la propia pantalla, antes de pulsar nada.
- **Consentimiento expreso, separado y sin premarcar** para cada finalidad comercial —arts. 4.11 y 7 RGPD y considerando 43: un consentimiento agrupado no es válido.
- **Dar el wifi no puede condicionarse a aceptar publicidad.** Eso rompe el requisito de «libremente prestado» del art. 7.4 RGPD.
- **Art. 21 LSSI** (Ley 34/2002): para mandarle después correo o SMS comercial hace falta consentimiento previo expreso. **Conectarse al wifi no es una relación contractual previa** y por tanto no activa la excepción.
- **Notificación de brechas en 72 horas** —art. 33 RGPD— y conservación limitada y minimización —arts. 5.1.c) y 5.1.e).

> EL PROBLEMA DE PRODUCTO, QUE ES PEOR QUE EL LEGAL
>
> El portal cautivo capta a quien quiere wifi gratis, que es un perfil sesgado y muy poco solapado con el cliente fiel de una cafetería de barrio. Y la aleatorización de MAC ha roto la persistencia de sesión: en

> iOS 18 y posteriores la dirección privada **rota cada ~14 días** en redes abiertas, así que el cliente vuelve a ver la pantalla de alta una y otra vez.

Veredicto: solo si el comercio *ya tiene* wifi de invitados y quiere volumen de altas. Y aun así, que el portal sirva para **una sola cosa**: enseñar el botón «Añadir la tarjeta de sellos al wallet». Que el portal capte, y que el dato viva en el pase. Nada de acumular ahí una base de datos paralela.

En el TPV: nada. Fuera: router o controlador compatible, la pantalla del portal y el enganche con la base de altas. El responsable del tratamiento sería el comercio, no EcomTPV, pero **si tú se lo montas te salpica**.

FUENTES

Lets Law — *Primeras multas de la AEPD sobre Wi-Fi tracking* (> 40.000 €): letslaw.es/en/fines-wifi-tracking/

Autónomos y Emprendedor — *Multas de más de 40.000 euros por utilizar los datos de los clientes que usan el wifi de los negocios*: autonomosyemprendedor.es

INCIBE — *Protege tu Empresa responde: dudas legales sobre las conexiones wifi*: incibe.es/empresas/blog/protege-tu-empresa-responde-dudas-legales-las-conexiones-wifi

Legálitas — *Tengo wifi en mi negocio: cuidado con la protección de datos y las responsabilidades*: legalitas.com/actualidad/obligaciones-legales-wifi-negocio

Purple — *Apple iOS 18 and macOS 15 WiFi MAC randomisation guide* (rotación cada ~14 días): purple.ai/en-us/blogs/apples-ios-18-macos-15-the-impact-on-public-wifi-how-purple-can-help

CERRADO

Lo que está muerto, y por qué no volver a proponerlo

Dos vías que aparecen una y otra vez en las conversaciones comerciales del sector. Las dos están cerradas, y por motivos distintos: una la mató Google, la otra la mataron a la vez los fabricantes de móviles y la Agencia Española de Protección de Datos.

Bluetooth, Eddystone y Nearby Notifications

Muerto. Un móvil sin ninguna aplicación instalada **no puede** captar una baliza Bluetooth en 2026, salvo la excepción del iBeacon dentro de un pase de Wallet que ya está instalado. Cualquier proveedor que venda «balizas que notifican sin app» está vendiendo un producto de 2016.

FECHA	QUÉ PASÓ
Octubre de 2017	Google retira el soporte de Eddystone de Android y de Chrome: se acaba el «Physical Web»
25/10/2018	Google anuncia el fin de Android Nearby Notifications. Motivo declarado: **spam publicitario** — *«These notifications did not meet our standards»*
6/12/2018	Google **deja de servir** Nearby Notifications. Los usuarios dejan de ver avisos de balizas
1/4/2021	Se apaga la **Proximity Beacon API**, lo último que quedaba para asociar el identificador de una baliza a un contenido

En Apple nunca existió: iOS jamás mostró contenido de una baliza sin una app que la escuchara.

Qué queda hoy, y qué no es: las balizas dentro de tu propia app —aquí no hay app—, y Fast Pair de Google y el emparejamiento de Apple, que sirven para emparejar auriculares y accesorios y **no admiten ningún mensaje comercial**.

Y además el legal. Aunque técnicamente funcionara, escanear direcciones Bluetooth de quien pasa por delante es el mismo tratamiento que el rastreo por MAC, con los mismos problemas, y con aleatorización de la dirección Bluetooth desde Android 6 e iOS 8. Doble callejón sin salida.

FUENTES

Android Developers Blog — *Discontinuing support for Android Nearby Notifications* (25/10/2018): android-developers.googleblog.com/2018/10/discontinuing-support-for-android.html

9to5Google — *Google killing location-based Nearby Notifications on Android due to spam*: 9to5google.com/2018/10/25/google-killing-location-notifications/

BeaconZone — *Google Beacon Platform Shutting Down* (Proximity Beacon API, 1/4/2021): beaconzone.co.uk/blog/google-beacon-platform-shutting-down/

VentureBeat — *Why Android Nearby, iBeacons, and Eddystone failed to gain traction*: venturebeat.com/business/why-android-nearby-ibeacons-and-eddystone-failed-to-gain-traction

Detección pasiva por dirección MAC

Muerto por dos sitios a la vez: roto técnicamente y campo de minas jurídico. No se construye y no se le vende a nadie.

Roto técnicamente

SISTEMA	ALEATORIZACIÓN
Apple	Aleatorización de las tramas de sondeo desde **iOS 8**; dirección wifi privada por red desde **iOS 14**; y desde **iOS 18 / macOS 15 la dirección privada rota aproximadamente cada 14 días** en redes abiertas o de seguridad débil
Android	Desde **Android 10** genera una MAC aleatoria distinta **por SSID**; desde Android 12 hay aleatorización no persistente

Efecto: cualquier plataforma que cuente direcciones MAC en bruto **interpreta cada rotación como un dispositivo nuevo**. El «visitante recurrente» desaparece y lo que queda es un contador de bultos con ruido.

Y sobre todo: **a una dirección MAC no se le puede escribir.** No hay canal. Aunque la detección fuera perfecta, para avisar hace falta un canal —pase, correo, WhatsApp— y para tener canal hace falta un alta consentida. Es decir, la vía del pase.

Campo de minas jurídico

El **7 de mayo de 2024** la AEPD publicó, junto con la APDCAT (Cataluña), la AVPD (País Vasco) y el CTDPA (Andalucía), las «**Orientaciones para tratamientos que incorporen tecnologías de seguimiento Wi-Fi**». Lo que dicen:

- La MAC es un **identificador único** que permite detectar dispositivos y sacar patrones de movimiento: **es dato personal** y el tratamiento cae de

lleno en el RGPD.

- **El consentimiento (art. 6.1.a) queda descartado** como base jurídica: es materialmente imposible pedírselo a alguien cuyo teléfono estás escuchando sin que él haga nada.
- Obligación legal (6.1.c) e interés público (6.1.e) no aplican sin una ley que lo ampare; intereses vitales (6.1.d), tampoco salvo emergencia.
- Queda el **interés legítimo (6.1.f)**, y solo con un juicio de ponderación documentado. Las autoridades lo admiten para gestionar un espacio —aeropuerto, gran superficie—, **no para hacerle marketing al cliente de una cafetería**.
- **Evaluación de impacto obligatoria** —art. 35.3 RGPD, por observación sistemática a gran escala. Las autoridades recomiendan hacerla incluso cuando dudes de si es obligatoria.
- **Transparencia reforzada**: paneles visibles, señalización pública, alertas de voz o campañas informativas. La cartelería no es opcional.
- Medidas exigidas: anonimizar y agregar inmediatamente tras la captura; **no asignar el mismo identificador al mismo dispositivo en visitas distintas**; limitar el ámbito; **no cruzar los datos de geolocalización con otras fuentes**; mecanismo de exclusión efectivo; auditorías independientes.

> LA FRASE QUE CIERRA EL ASUNTO
>
> «No asignar el mismo identificador en distintas visitas» y «no cruzar con otras fuentes» hacen **imposible** reconocer a un cliente y enlazarlo con su ficha de fidelización. **La propia guía prohíbe la funcionalidad.** Lo que queda permitido es contar bultos anónimos, que es exactamente lo que hacen mejor y más barato los sensores cenitales de tiempo de vuelo o térmicos: otro producto, con instalación y otro ciclo de venta.

FUENTES

AEPD — nota de prensa de las orientaciones de seguimiento Wi-Fi (7/5/2024): aepd.es/prensa-y-comunicacion/notas-de-prensa/…-seguimiento-wifi

AEPD — *Orientaciones para tratamientos que incorporen tecnologías de seguimiento Wi-Fi* (guía en PDF): aepd.es/guias/orientaciones-wifi-tracking-seguimiento.pdf

Cuatrecasas — *Nuevas orientaciones sobre los «riesgos» del Wi-Fi Tracking*: cuatrecasas.com/es/spain/propiedad-intelectual/art/nuevas-orientaciones-sobre-riesgos-wi-fi-tracking

PwC España — *Novedades de la Guía de orientaciones para la correcta implementación de tecnologías de seguimiento WiFi*: pwc.es/es/newlaw-pulse/regulacion-digital/…-seguimiento-wifi.html

Purple — *MAC Address Randomization vs Device MAC: 2026 IT Guide*: purple.ai/en-us/blogs/mac-randomization-101

Cloud4Wi — *iOS 18 MAC randomization: key insights for IT managers*: cloud4wi.ai/resources/ios-18-mac-randomization/

CUMPLIMIENTO

Lo legal en España, en decisiones

No es un capítulo de teoría: son tres decisiones que hay que tomar antes de escribir el formulario de alta. Qué necesita consentimiento, qué cartelería hay que poner —y dónde no hace falta ninguna— y a partir de qué edad.

Decisión 1 · Qué exige consentimiento y qué no

TRATAMIENTO	BASE JURÍDICA	QUÉ IMPLICA EN LA PRÁCTICA
Alta en el programa: nombre, móvil, correo	**Art. 6.1.b) RGPD** · ejecución del contrato	Los datos **necesarios** para el programa **no necesitan consentimiento aparte**
Fecha de nacimiento	Art. 6.1.a) · consentimiento	No es necesaria para el programa, así que va con **casilla propia**. Sirve para la campaña de cumpleaños y como barrera de edad
Actualizar el saldo de sellos en el pase	Art. 6.1.b)	Es el servicio que el cliente pidió. **Sin consentimiento aparte**

TRATAMIENTO	BASE JURÍDICA	QUÉ IMPLICA EN LA PRÁCTICA
Aviso de proximidad del wallet	**No hay tratamiento por tu parte**	**Nada que pedir.** Solo una frase informativa. Explicado más abajo
Correo o SMS comercial	Art. 6.1.a) RGPD + **art. 21 LSSI**	Consentimiento previo, expreso, específico y **separado por canal**. Casillas sin premarcar, una por canal
WhatsApp	Igual, más la política de Meta	Meta exige *opt-in* explícito con independencia de lo que diga la ley
Portal cautivo del wifi	6.1.b) para dar acceso + 6.1.a) para lo comercial	El acceso **no puede condicionarse** a aceptar publicidad —art. 7.4 RGPD
Rastreo pasivo por MAC	Solo 6.1.f), con ponderación y evaluación de impacto	**No se hace.** Las restricciones de la guía vacían la funcionalidad

Un consentimiento agrupado no es válido bajo el RGPD (considerando 43). Un solo «acepto recibir comunicaciones» para correo, SMS y WhatsApp a la vez no sirve para ninguno de los tres.

Por qué el aviso del wallet es legalmente sencillo

El comercio no trata ningún dato de ubicación. Lo que ocurre es:

1. Metes unas coordenadas fijas —las de tus propios locales, que son un dato de la empresa, no de una persona— dentro de un fichero firmado.
2. Ese fichero lo instala el cliente voluntariamente en una aplicación de Apple o de Google.
3. El sistema operativo, o Google, evalúan la cercanía **en su lado**.
4. **Nada vuelve hacia ti.** Ni evento, ni registro, ni identificador, ni hora.

No hay recogida, ni registro, ni cesión de datos de localización por parte del responsable. Lo que sí tratas —nombre, móvil, correo, historial de compras — lo tratas por el alta, no por el geofence. Entre Apple o Google y el usuario

hay una relación propia, con sus propias políticas de privacidad, en la que EcomTPV no es responsable.

> LO QUE SÍ HAY QUE HACER, Y ES POCO
>
> Una frase en la información del alta (art. 13 RGPD): «*la tarjeta puede aparecer en la pantalla de bloqueo de tu móvil cuando estés cerca de uno de nuestros locales; puedes desactivarlo desde los ajustes del pase*». No fingir que es una función que el comercio puede apagar por cliente —**no puede**, se apaga desde el teléfono. Y no usar el texto del aviso para publicidad agresiva: Apple no pone tope de frecuencia, así que el abuso lo paga el cliente borrando el pase.

Decisión 2 · Qué cartelería hace falta

SITUACIÓN	¿CARTEL?	BASE
Pase de wallet con ubicaciones	**NO**	No se tratan datos en la puerta. **Es la razón para elegir esta vía**
Etiqueta NFC o QR de alta	**NO**	Basta el aviso de privacidad en la página de alta —art. 13 RGPD en el formulario
Portal cautivo	**En la pantalla**	Art. 13 RGPD. Cartel físico no exigido
Rastreo de MAC / seguimiento wifi	**SÍ, reforzado**	Paneles visibles, señalización pública, incluso avisos de voz. Orientaciones AEPD 2024 + art. 13 RGPD
Sensores cenitales de aforo	**SÍ, informativo**	Buena práctica; art. 13 si el tratamiento no es plenamente anónimo
Videovigilancia y analítica por cámara	**SÍ, obligatorio**	Cartel homologado en zona visible desde el acceso. Art. 22 LOPDGDD + guía de videovigilancia de la AEPD

Las dos primeras filas son el plan. Las cuatro últimas son las que hay que saber para decir que no con criterio cuando el cliente las pida.

Decisión 3 · Los 14 años del artículo 7 de la LOPDGDD

El **art. 7 de la Ley Orgánica 3/2018 (LOPDGDD)** establece que el tratamiento de datos de un menor basado en su consentimiento **solo es lícito a partir de los 14 años**. Por debajo hace falta el consentimiento del titular de la patria potestad o de la tutela. El RGPD (art. 8) deja la horquilla entre 13 y 16 años a cada Estado; **España fijó 14**. Y el consentimiento en protección de datos es **siempre explícito**: no vale ninguna fórmula tácita.

Traducido a producto, y esto es una tarea concreta del formulario de alta:

- El formulario ya pide la fecha de nacimiento para la campaña de cumpleaños. **Úsala como barrera**: si sale menor de 14, no se crea el pase y se muestra un aviso.
- Mínimo **14 años** en las condiciones del programa. Si el cliente es una heladería, una tienda de golosinas o una papelería junto a un colegio, hay que decírselo por escrito antes de firmar.
- **Nunca** publicidad de proximidad ni comportamental dirigida a menores. Considerando 38 del RGPD: los menores merecen protección específica en marketing y creación de perfiles.
- La campaña de cumpleaños de un menor de 14 con consentimiento paterno es posible, pero triplica el papeleo. Para un comercio pequeño la recomendación es sencilla: **el programa es para mayores de 14 y punto**.

Resumen: sencillo contra campo de minas

SE RESUELVE CON UN BUEN FORMULARIO DE ALTA	NO ENTRAR SIN ABOGADO, EVALUACIÓN DE IMPACTO Y PRESUPUESTO
– Pase de wallet con ubicaciones – Etiqueta NFC y código QR – Actualización del pase por push – Correo y WhatsApp con consentimiento separado por canal	– Rastreo pasivo por MAC o Bluetooth – Portal cautivo mal montado · multas reales por encima de 40.000 € – Cualquier cruce entre presencia física y ficha de cliente que no venga de un acto

SE RESUELVE CON UN BUEN FORMULARIO DE ALTA	NO ENTRAR SIN ABOGADO, EVALUACIÓN DE IMPACTO Y PRESUPUESTO
– Web Push · el permiso del navegador es el consentimiento	voluntario del cliente – Analítica de comportamiento por cámara – Menores de 14 sin consentimiento paterno

FUENTES

RGPD — Reglamento (UE) 2016/679. LOPDGDD — Ley Orgánica 3/2018, de 5 de diciembre. LSSI — Ley 34/2002, de 11 de julio, arts. 21 y 22.2.

AEPD — *¿Cuál es la edad para que los menores puedan prestar consentimiento?* (14 años): aepd.es/preguntas-frecuentes/10-menores-y-educacion/FAQ-1001

Iberley — *Artículo 7 LOPDGDD*: iberley.es/legislacion/articulo-7-…-lopdgdd

Alex Barbarà — *Las obligaciones legales de las cookies: el artículo 22.2 LSSI*: alexbarbara.es/cookies-articulo-22-2-lssi/

World Compliance Association — *La AEPD sanciona por tratar sin consentimiento datos personales recogidos a través de redes WiFi*: worldcomplianceassociation.com/1584/

IMPLANTACIÓN

Qué hay que tocar en EcomTPV

Menos de lo que parece. El geofence **no toca el TPV**: es un dato que viaja al generador de pases. Lo que sí toca el TPV son tres cosas.

PIEZA	DÓNDE	QUÉ ES
Coordenadas del local	Configuración de la tienda	Latitud y longitud por local
Texto del aviso	Configuración de la tienda	Una línea corta, la que verá el cliente en la pantalla de bloqueo

PIEZA	DÓNDE	QUÉ ES
Lectura del pase	Pantalla de caja	Leer el código del pase y llamar a la interfaz de actualización

1 · Latitud y longitud por local

- Dos campos numéricos en la configuración de la tienda, junto a la dirección postal que ya se guarda. Decimales con separador de punto —el formato de las dos interfaces—, no con la coma del formato español.
- Alternativa a teclearlos: **geocodificar la dirección** que ya está en la ficha del local. Es más cómodo, pero **hay que dejar el resultado editable**: con un radio de 100 metros, un portal mal geocodificado deja el aviso fuera del local.
- Un local, un par de coordenadas. **Diez como máximo por pase**: si el comercio tiene más de diez locales hay que decidir cuáles diez van en cada pase, y ese criterio es una decisión de producto, no un detalle técnico.
- **Comprobación en pantalla:** junto a los dos campos, un enlace que abra esas coordenadas en un mapa. Es la única manera barata de que el comerciante vea que ha metido el punto donde toca antes de que se emitan mil pases.

> MULTITIENDA
>
> Las coordenadas y el texto del aviso son **por local**, nunca globales. Si la configuración del TPV tiene ajustes globales y ajustes por tienda, estos van claramente en los de tienda, y hay que verificar que un comercio con varios locales no acaba con todos los pases apuntando al primero.

2 · El texto del aviso

- Un campo de texto corto por local. Es el `relevantText` de Apple: una línea, no un párrafo.

- **Poner un límite de caracteres y enseñar el contador.** Lo que no cabe se corta en el móvil, y el comerciante no lo va a ver hasta que se lo diga un cliente.
- Texto por defecto sembrado al instalar, con la ortografía correcta, para que el campo nunca quede vacío.
- **Este campo solo afecta a Apple.** En Google el texto lo escribe Google y no es personalizable: hay que decirlo en la propia pantalla, junto al campo, o el comerciante creerá que su texto se está mostrando en Android.
- El campo puede cambiarse en cualquier momento: el cambio llega a los pases ya emitidos por *push*, gratis. Eso sí es una función vendible, y es lo que sustituye a la desaparecida automatización de proximidad.

3 · Leer el código del pase en caja

- Es **la única fuente de verdad del sistema**: la única forma de saber que ese cliente ha entrado y ha comprado. Todo lo demás son señales.
- El pase lleva un código —QR o PDF417— que se lee con el lector 2D que ya usa el TPV, o con el teclado si se teclea el número. **Debe funcionar como entrada de teclado**, igual que un código de barras de producto, para no depender de hardware nuevo.
- Al leerlo: identificar al cliente, asociar el ticket, sumar el sello y llamar a la interfaz de actualización del pase. La actualización es asíncrona y gratuita: **la caja no debe esperar a que termine**. Si el servicio de pases no responde, el ticket se cobra igual y la actualización se reintenta después.
- Distinguir en la pantalla de caja los tres casos: pase leído y reconocido, pase leído y no reconocido —de otro comercio o caducado— y sin pase. El segundo caso es el que genera avisos si no se explica bien.
- **Idempotencia:** leer dos veces el mismo pase en el mismo ticket no puede sumar dos sellos. Es el mismo problema que ya está resuelto en el descuento de existencias, y se resuelve igual.

> LO QUE NO HAY QUE CONSTRUIR EN EL TPV

> Ni geofence, ni contador de proximidad, ni pantalla de «clientes cerca», ni integración con nada de ubicación. **Esa información no llega y no va a llegar.** Cualquier pantalla que la prometa es una pantalla que se quedará vacía.

Fuera del TPV, lo que hace falta montar

- Dominio con **HTTPS y certificado válido**. Apple exige TLS en el servicio web de pases; sin eso, los pases no se actualizan nunca.
- Un servicio que firme los `.pkpass` y emita los objetos de Google Wallet, con los cuatro extremos del servicio web de Apple.
- APNs para las actualizaciones de Apple.
- La página de alta con los consentimientos separados por canal y la barrera de los 14 años.
- **Cuenta de Apple Developer (99 €/año)** y cuenta de emisor de Google Wallet (0 €, con aprobación previa que tarda unos días).

Plan definitivo de fidelización con avisos de proximidad · EcomTPV · septiembre de 2026. Corrige el documento `otras cosas/fidelizacion-wallet.html` con la investigación `manuales/EcomTPV/INVESTIGACION-avisar-sin-app.md`.

Los límites de las plataformas —radios, topes de frecuencia, disponibilidad por país de las notificaciones de proximidad de Google Wallet— los cambian Apple y Google sin previo aviso. **Revalidar con un teléfono real antes de escribirlos en un contrato.** Los datos marcados como «sin confirmar» en este documento son exactamente eso: no se han verificado y no deben repetirse ante un cliente como si fueran ciertos.