# Introducción

En España, los establecimientos turísticos tienen la **obligación legal de identificar a todos sus huéspedes** y comunicar determinados datos a las fuerzas de seguridad (Policía Nacional o Guardia Civil) dentro de un plazo establecido. Esto genera la duda de **si pueden guardar una copia (escaneo o fotografía) del DNI u otro documento de identidad** de los clientes para cumplir con esa obligación. A continuación, se analiza detalladamente la normativa nacional vigente (no autonómica) sobre el registro de viajeros, las exigencias del Ministerio del Interior y las Fuerzas y Cuerpos de Seguridad del Estado, **qué información debe conservarse, durante cuánto tiempo y en qué formato**, y **si la policía puede exigir la copia física del DNI** de un cliente a un alojamiento. Asimismo, se examina cómo encaja esta práctica con el Reglamento General de Protección de Datos (RGPD) de la UE y la ley española de protección de datos (LOPDGDD), incluyendo los **riesgos legales o sanciones** por conservar copias sin base jurídica suficiente. Finalmente, se proporcionan **recomendaciones prácticas** sobre si conviene o no guardar dichas copias y la forma legal de hacerlo en caso necesario (por ejemplo, eliminación automática tras enviar los partes de viajeros a la policía), así como implicaciones para **sistemas de check-in digital** como AlojaSCAN o Aloja360.

## Obligaciones legales de identificación y registro de viajeros

La **Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana**, establece en su artículo 25.1 que las personas físicas o jurídicas que ejercen actividades relevantes para la seguridad ciudadana –entre ellas **los hospedajes turísticos**– están sujetas a obligaciones de **registro documental e información** [1] [2]. Este mandato legal se ha desarrollado mediante el **Real Decreto 933/2021, de 26 de octubre**, que unifica y actualiza las obligaciones para hoteles, apartamentos, campings, casas rurales y *viviendas de uso turístico*, entre otros [3]. El RD 933/2021 sustituyó y amplió la anterior normativa (Orden INT/1922/2003) para adaptarse a las nuevas modalidades de hospedaje (por ejemplo, apartamentos de alquiler por plataformas) [3].

En virtud de estas normas, **todo establecimiento de hospedaje debe identificar a sus huéspedes mayores de 14 años** en el momento del check-in, recoger determinados datos personales en un **parte de entrada de viajeros** y **comunicar esos datos** a las autoridades policiales competentes [4] [5]. La identificación suele requerir que el cliente **muestre un documento oficial (DNI, pasaporte, NIE, etc.)** y proporcione o confirme los datos necesarios, firmando el parte de entrada. Según el RD 933/2021, la transmisión de la información de cada huésped a la policía debe hacerse de forma **telemática e inmediata (o, en todo caso, dentro de las 24 horas siguientes a la llegada)** [5] [6], mediante la plataforma digital habilitada por el Ministerio del Interior (el sistema de "hospederías" de Policía/Guardia Civil).

**¿Qué datos deben recabarse exactamente?** La normativa define de forma exhaustiva los campos obligatorios. Tradicionalmente (Orden INT/1922/2003) se exigían datos básicos como **nombre y apellidos, número y tipo de documento de identidad, fecha de expedición, nacionalidad, sexo, y fechas de entrada y salida** [7]. El nuevo RD 933/2021 amplió la lista, incluyendo datos de contacto y otros detalles, pero **el principio general es que solo deben recogerse ciertos datos identificativos esenciales del huésped**, **no una copia entera del documento** [8] [9]. En concreto, **la ley obliga a tomar únicamente información como**: nombre y apellidos, **tipo y número de documento de identidad**, fecha de nacimiento, nacionalidad, fecha de entrada (y salida) y algunos datos adicionales operativos (p. ej. código del alojamiento, medio de transporte de llegada) [10]. **En ningún caso es**

**obligatorio (ni recomendable) solicitar una fotografía del DNI, "selfies" del huésped ni datos biométricos** [11], puesto que nada de eso figura entre los campos requeridos.

Cabe destacar que el **Ministerio del Interior** ha aclarado que aunque el anexo del RD 933/2021 enumera más campos, solo son obligatorios aquellos que el alojamiento **efectivamente recabe en el ejercicio de su actividad** [12] [13]. Es decir, los establecimientos deben transmitir todos los datos especificados que **ya obtengan en su operativa normal**, pero **no están obligados a pedir información adicional al cliente más allá de los datos identificativos esenciales**. De hecho, desde el Gobierno se ha indicado que algunos campos como el sexo o la nacionalidad, que aparecían antes en los formularios, **no serán obligatorios** en la nueva plataforma [14]. En la práctica, el núcleo de información personal sigue siendo el mencionado: identidad del huésped y datos de su estancia.

**¿Cómo se deben conservar estos datos y por cuánto tiempo?** La normativa actual exige llevar un **"libro-registro" de viajeros en formato digital**. El RD 933/2021 estipula que los alojamientos **"habrán de llevar un registro informático"** con los datos recogidos y **conservarlos durante 3 años** desde la finalización del servicio de hospedaje [15] [16]. Esto supone que, por ejemplo, los datos de un cliente que se aloja hoy deberán mantenerse accesibles hasta 3 años después de su check-out, para fines de seguridad y eventuales inspecciones. Esta obligación de conservación de 3 años es de **cumplimiento obligatorio** para todos los sujetos obligados (salvo particulares que alquilan de forma ocasional, quienes están exentos de llevar registro aunque sí deben comunicar los partes) [17] [18]. En la práctica, muchas soluciones tecnológicas de gestión hotelera ya facilitan esto: por ejemplo, la aplicación **AlojaSCAN** genera automáticamente el libro de registro en PDF y lo almacena, recordando que **"es obligatorio mantener el libro de registro al menos durante 3 años"** [19].

En cuanto al **formato**, actualmente la tendencia es al soporte digital: la información se comunica por vía electrónica a la policía y el registro se lleva en sistemas informáticos [20] [5]. No obstante, nada impide que el hotel haga que el cliente **complete un parte en papel (ficha de viajero)** para recabar su firma y luego digitalizar o transcribir esos datos. De hecho, el RD 933/2021 exige que **cada huésped mayor de 14 años firme el parte de entrada** (sea en papel o mediante sistema electrónico de firma) [21]. Esos partes o su equivalente electrónico deben guardarse como respaldo. **Importante**: ni la ley antigua ni la nueva exigen que ese parte sea una *fotocopia del DNI*, solo que contenga los **datos** del DNI validados contra el documento original que se exhibe en recepción [22] [23].

## ¿Se puede (o debe) guardar una copia del DNI del cliente?

**La legislación nacional vigente *no* exige en ningún caso que el hotel o alojamiento turístico conserve una fotocopia o imagen escaneada del documento de identidad del huésped** [8]. Esta es una cuestión crucial: el cumplimiento de la obligación de registro de viajeros **se logra recopilando y comunicando los datos requeridos**, pero **en ningún momento la norma pide almacenar la imagen completa del DNI/pasaporte**. Así lo ha reiterado la Agencia Española de Protección de Datos (AEPD) en resoluciones recientes: solicitar o guardar una copia íntegra del documento **no está amparado por la normativa de seguridad ciudadana** y supone un exceso de datos [8].

En la práctica hotelera, muchos establecimientos solían escanear el DNI para agilizar el check-in. **¿Está permitido escanear el documento?** Aquí conviene distinguir: **no está prohibido usar un escáner o app para leer automáticamente los datos del DNI**, lo que *no se puede hacer* es **conservar la imagen completa o fotocopia del documento salvo que exista una justificación legal específica** [24]. Es decir, el hotel puede pasar el DNI por un lector OCR o tomarle una foto momentáneamente para extraer los datos, **siempre y cuando no guarde esa foto/escaneo una vez obtenidos los campos necesarios**

[24] [25]. Esto tiene sentido, porque almacenar la copia del DNI aportaría mucha más información (foto, dirección, firma, número de soporte, etc.) de la que la ley requiere para el registro de viajeros [26].

La propia AEPD ha sido tajante al respecto: *"ni la legislación obliga a recoger imágenes del DNI, ni está permitido recabar más datos personales de los estrictamente necesarios"* [27]. En un caso reciente, la AEPD subrayó que la normativa aplicable (LO 4/2015 y RD 933/2021) **no exige guardar copia del documento de identidad sino únicamente ciertos datos esenciales** [8]. Por tanto, un **alojamiento no tiene base legal para exigir que el cliente le entregue una fotocopia** de su DNI o pasaporte más allá de enseñarlo para apuntar los datos. Basta con la **exhibición del documento en el check-in** para comprobar su autenticidad y exactitud, sin necesidad de retener un duplicado físico o digital [28].

Algunos establecimientos podrían pensar que guardar copias les protege en caso de inspección policial o les facilita información si hubiese un incidente. Sin embargo, **ninguna norma faculta al hotel para retener el documento original del cliente ni para archivar una copia por si "la pide la policía"**. De hecho, **la policía/Guardia Civil no puede exigir al alojamiento una fotocopia del DNI que el huésped entregó**, porque se asume que el alojamiento *no* tiene tal fotocopia (ni está obligado a tenerla). Lo que las autoridades sí pueden requerir es que el hotel **haya cumplido con registrar y reportar los datos** de los huéspedes en tiempo y forma, y eventualmente pueden solicitar ver el libro-registro o los partes de entrada **con los datos consignados** [8] [19]. En otras palabras, en una inspección rutinaria o investigación, la policía puede pedir al alojamiento "muéstreme su registro de viajeros de tal fecha" (donde figuran nombre, DNI, etc. de cada cliente) o incluso preguntar por un huésped específico, pero **no van a pedir "deme la fotocopia del DNI del Sr. X"** como procedimiento estándar, porque la ley no contempla que el establecimiento deba disponer de esa copia. Si la policía necesitase verificar la identidad de un individuo concreto más allá de los datos aportados, tendría que localizar al propio huésped o consultar bases de datos oficiales, no obtenerlo del hotel.

En resumen, **la obligación legal del hotel es identificar y anotar los datos**, no coleccionar copias de documentos. **Mostrar el documento original para apuntar/verificar los datos es suficiente** y cumple la ley [28]. Cualquier política interna del alojamiento de fotocopiar o escanear el DNI "por si acaso" **carece de respaldo normativo y puede vulnerar la ley de protección de datos**, como veremos a continuación.

## Protección de datos: RGPD, LOPDGDD y principio de minimización

Cuando un alojamiento turístico trata datos personales de sus clientes (nombres, DNI, dirección, etc.), debe cumplir con el **Reglamento General de Protección de Datos (RGPD)** de la UE y la **Ley Orgánica 3/2018 (LOPDGDD)** española. Estas normas establecen varios **principios fundamentales** en el tratamiento de datos, entre ellos: **licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; limitación del plazo de conservación; integridad y confidencialidad** [29].

En este contexto, la recogida de datos de huéspedes se ampara en una **base de licitud** clara: el **cumplimiento de una obligación legal** (art. 6.1.c RGPD) impuesta por la normativa de seguridad ciudadana. Es decir, el hotel no necesita consentimiento del cliente para tomar sus datos del DNI porque una ley lo exige. **Ahora bien, esa base legal cubre únicamente los datos que la ley de seguridad ciudadana requiere**, *no más*. Por eso, **es ilícito (por desproporcionado) escanear y guardar todo el documento de identidad cuando la obligación se limita a ciertos datos** [8] [30]. Hacerlo vulnera especialmente el principio de **"minimización de datos"**, según el cual solo se deben tratar los datos **adecuados, pertinentes y limitados a lo necesario** con respecto a la finalidad legítima [31] [32].

Conservar una copia íntegra del DNI **implica tratar datos excesivos**: una fotocopia del DNI incluye la foto del titular (dato biométrico facial), su firma manuscrita, dirección completa, el ID de soporte, etc., **información que ni se necesita para el registro de viajeros ni ha sido solicitada por ninguna ley** [26]. Por tanto, carecería de base jurídica recoger esos elementos. La **AEPD** ha reiterado en guías y resoluciones que **"no es necesario escanear ni conservar una copia del DNI para cumplir con la normativa de seguridad ciudadana"**, y que hacerlo **sin una justificación específica vulnera el RGPD** [33]. En línea con ello, en la LOPDGDD (Ley 3/2018) se refuerza la idea de que el tratamiento debe ser proporcional y relacionado con fines legítimos; cualquier exceso podría considerarse una infracción.

Otro aspecto a considerar es la **limitación del plazo de conservación**. La obligación legal manda guardar los datos 3 años para fines de seguridad, pero **no más allá**. Si un hotel guardase copias del DNI "por si acaso" indefinidamente, también estaría incumpliendo el principio de no conservar datos más tiempo del necesario. Incluso dentro del plazo legal, se debe asegurar que los datos estén debidamente protegidos (principio de **integridad y confidencialidad**), dado que información como el número de DNI o la copia del mismo es sensible para posibles fraudes.

En suma, desde la óptica de protección de datos, **la práctica de escanear/fotocopiar el DNI de los huéspedes debe evaluarse con extrema cautela**. Solo sería lícita si se demuestra imprescindible para la finalidad (por ejemplo, si una autoridad lo requiriese en un caso concreto, lo cual no ocurre en el funcionamiento normal). En ausencia de tal necesidad, **prevalece el deber de minimización**: **recoger únicamente los datos estrictamente necesarios** (los campos obligatorios que pide Interior) y **evitar tratar datos adicionales (imágenes del documento, etc.)** que no aporten valor legal [9] [34].

## Sanciones y riesgos legales por guardar copias sin respaldo legal

Persistir en prácticas de fotocopiar o escanear DNI de clientes **puede conllevar sanciones significativas**. La Agencia Española de Protección de Datos, encargada de hacer cumplir el RGPD en España, **ya ha sancionado a varios alojamientos turísticos por este motivo**. Por ejemplo:

- **Caso Posada El Azufral (Cantabria)**: La AEPD impuso **1.500 euros de multa** a una posada rural que **exigió la fotocopia del DNI** a un cliente como condición indispensable para hacer check-in. El huésped se negó y el alojamiento canceló su reserva; posteriormente el viajero denunció ante la AEPD. La resolución fue clara: **pedir la fotocopia sin base legal es un tratamiento excesivo de datos** que vulnera el principio de minimización (art. 5.1.c RGPD) [35] [8]. Dado que la normativa de registro de viajeros **no exige guardar copia del DNI** sino solo ciertos datos, la posada actuó ilegalmente y fue sancionada. Este caso sentó un precedente que puso en alerta al sector hotelero sobre estas prácticas [36].

- **Caso empresa Airbnb (Barcelona)**: A principios de 2025 se conoció una sanción acumulada de **75.000 euros** a una pequeña empresa gestora de apartamentos turísticos en Barcelona. Esta obligaba a los huéspedes que reservaban vía Airbnb a **enviar fotos de su DNI (anverso y reverso) y un *selfie*** para verificar su identidad, alegando que era un requisito legal del Registro de Viajeros. La AEPD desmontó ese argumento: *"ni la legislación obliga a recoger imágenes del DNI, ni está permitido recabar más datos personales de los estrictamente necesarios"* [27]. La empresa, además, incumplió la obligación de informar claramente a los clientes (no explicaba quién era el responsable del tratamiento, con qué fin exacto se usaban esas imágenes, cuánto tiempo se conservarían, etc.), lo que agravó la situación [37]. Finalmente se le impusieron **dos multas (de 25.000 € y 50.000 €)** por sendas infracciones graves del RGPD [38] [39]. Este caso evidencia que **exigir imágenes del DNI y datos biométricos sin necesidad está considerado una infracción muy grave** en materia de protección de datos.

- **Otros casos**: La AEPD ha sancionado con **30.000 €** a un hotel que escaneaba sistemáticamente los pasaportes de sus clientes, y con **2.000 €** a un propietario de vivienda turística que mantenía copias digitales de los DNI de huéspedes sin justificación legal [33] [40]. Cada caso varía en gravedad, pero el patrón común es la recopilación o conservación de más información personal de la necesaria. Las sanciones pueden variar desde miles hasta decenas de miles de euros dependiendo de si hay reincidencia, cuántos afectados, si hay otros incumplimientos (falta de información, fallos de seguridad, etc.).

Además de las multas económicas (que bajo el RGPD podrían llegar hasta 20 millones de euros o el 4% de la facturación anual, en casos extremos), **los riesgos incluyen**: daños reputacionales, pérdida de confianza de los clientes, posibles indemnizaciones a afectados y órdenes de la AEPD de cesar en las prácticas ilícitas [41]. Un hotel expuesto públicamente por una sanción de la AEPD puede ver comprometida su imagen en un sector donde la confianza del cliente es fundamental [42] [43].

Otro riesgo real es el **ciberataque o filtración de datos**. Si un establecimiento almacena copias de DNIs (por ejemplo, en una carpeta del ordenador, en correos electrónicos o en un servidor mal protegido), esos ficheros pueden ser robados por *hackers* o empleados desleales. Los **documentos de identidad son altamente sensibles**, pues una copia fiel puede servir para suplantaciones de identidad, contrataciones fraudulentas, apertura de cuentas bancarias, etc. La **Policía Nacional** desaconseja totalmente compartir o difundir imágenes completas del DNI justamente por el riesgo de fraude que conllevan [44]. Un delincuente que acceda a un archivo con fotocopias de pasaportes/DNIs obtendría fotos, firmas y datos personales valiosos. Por tanto, al **almacenar copias innecesarias el alojamiento se hace responsable de custodiar información delicada** que, de filtrarse, podría originar sanciones adicionales por brechas de seguridad (el RGPD obliga a proteger los datos con medidas apropiadas). En resumen, **guardar copias del DNI "por si acaso" no solo es ilegal, sino que aumenta la exposición a incidentes de seguridad** [45].

## Recomendaciones de autoridades y expertos en protección de datos

Dada la postura clara de la normativa y de la AEPD, las recomendaciones de organismos oficiales y expertos confluyen en un mensaje: **los alojamientos turísticos NO deben conservar copias del DNI u documentos de identidad de los huéspedes, salvo que exista una excepción legal muy concreta que lo justifique**. A continuación, se detallan **buenas prácticas** para cumplir la ley de forma eficaz y respetuosa con la privacidad:

- **Limitarse a los datos necesarios:** Revise sus procesos de check-in y **solicite únicamente los datos estrictamente requeridos por la normativa vigente**, nada más [46]. Esto significa recoger solo los campos obligatorios (identificación y datos de la estancia) y **eliminar de sus formularios cualquier petición de información adicional** que no esté prevista en la ley. Por ejemplo, **eliminar la petición de fotocopias del DNI** o de datos como la dirección postal completa (si no se requiere), etc. **La exhibición del documento en persona es suficiente** para comprobar la identidad, no hace falta obtener una copia [28].

- **No fotocopiar ni escanear para guardar: Suprima la práctica de exigir o archivar fotocopias del DNI/Pasaporte**. Si hasta ahora su personal lo hacía por rutina, deje claro que **no está permitido conservar copias físicas ni digitales del documento de identidad** de los clientes [47]. En un check-in presencial, el recepcionista debe verificar el documento y anotar los datos, pero **no debería quedarse con una copia** (ni siquiera "por seguridad"). En caso de check-in online, **no pida al huésped que envíe una foto/escáner de su DNI por email o WhatsApp**

antes de llegar; en su lugar, opte por soluciones más seguras (como formularios encriptados o mejor aún, verificación al llegar). **Si por alguna razón excepcional obtiene una copia**, asegúrese de **borrarla inmediatamente** tras usarla para el fin puntual.

- **Uso responsable de herramientas digitales:** Emplear **sistemas de check-in automáticos o escáneres OCR** es totalmente compatible con el RGPD **si se hace bien**. Es decir, **se puede escanear el DNI con herramientas que extraigan los datos requeridos y aceleren el registro**, **pero** dichas herramientas **no deben almacenar la imagen completa** ni recopilar más datos de los necesarios [24] [25]. Verifique con su proveedor de software cómo maneja las imágenes: lo ideal es que la foto del DNI se procese solo en memoria para leer el MRZ (zona de lectura mecánica) o la info relevante, y **no se guarde en la base de datos**. Muchos sistemas (como apps móviles) ya funcionan así, eliminando automáticamente la foto una vez leído el texto. Este enfoque **está respaldado por expertos legales** porque cumple el principio de minimización y mejora la eficiencia sin aumentar riesgos [25].

- **Eliminar datos residuales:** Implante políticas de **borrado periódico** de datos que no deban conservarse. Por ejemplo, si su escáner o fotocopiadora almacena imágenes temporalmente, cerciórese de que esas imágenes se eliminan. Si en algún momento imprimió o fotocopió un DNI, **destrúyalo** (trituradora de papel en el caso físico, borrado seguro en el caso digital). Asimismo, una vez que el huésped ha salido y pasado el plazo legal de conservación, depure esos registros según establezca la ley o su evaluación interna.

- **Formación y concienciación del personal:** Es fundamental **capacitar a los empleados** (recepcionistas, encargados de check-in, etc.) en materia de protección de datos [48]. Deben entender por qué no se pueden pedir fotocopias del DNI alegremente, cómo cumplir la normativa correctamente y cómo responder si un cliente tiene dudas. Un personal formado sabrá, por ejemplo, explicar al huésped *"Le solicito su DNI solo para tomar los datos obligatorios por ley; no nos quedamos con ninguna copia de su documento"*. Esto no solo evita infracciones, sino que transmite profesionalidad y transparencia al cliente.

- **Transparencia con el cliente:** Proporcione a los huéspedes la **información básica de privacidad** cuando recoja sus datos. Según el RGPD, hay que informar de la identidad del responsable (el hotel), la finalidad (cumplir obligación de registro policial), el plazo de conservación (3 años por ley), destinatarios (Fuerzas de Seguridad) y los derechos del interesado. Esta información puede estar en la ficha de check-in o en cartelería en recepción. **Aclare también que NO se guardarán copias de sus documentos** y que los datos se tratan con seguridad. La **transparencia** genera confianza y reduce potenciales reclamaciones [49].

- **Medidas de seguridad:** Asegúrese de proteger adecuadamente los datos que sí almacena (los partes de viajero con los campos obligatorios). Use contraseñas fuertes en los sistemas, cifrado si es posible, y controle el acceso a esos ficheros. Recuerde que aunque no guarde copias de DNI, los datos personales en sí mismos (nombre, número de documento, etc.) también deben resguardarse para evitar accesos no autorizados.

- **Asesoramiento experto:** Si tiene cualquier duda sobre cómo ajustar sus procedimientos, consulte con especialistas en protección de datos o con las guías oficiales de la AEPD. Por ejemplo, la AEPD ha publicado guías sobre verificación de identidad y sobre tratamientos de datos en el sector turístico. Un auditor externo puede revisar si su software de check-in cumple con RGPD o si sus cláusulas informativas están correctas [50].

En esencia, la **recomendación unánime** es **no conservar copias de DNI** y enfocarse en **cumplir la ley recogiendo solo los datos necesarios**, garantizando al mismo tiempo la seguridad de esa información. Así se evitan multas y, además, se ofrece una mejor experiencia al cliente (menos intrusiva). Como bien señala un artículo especializado, **pedir datos innecesarios no solo arriesga sanciones de la AEPD sino también supone un riesgo de seguridad** en sí mismo, ya que almacenar copias de documentos crea un "botín" atractivo para ciberdelincuentes [51]. Cumplir la ley de forma estricta es también una manera de cuidar al cliente y la reputación del negocio [52].

## Sistemas como *AlojaSCAN* o *Aloja360*: implicaciones y buenas prácticas

Herramientas digitales como **AlojaSCAN** o **Aloja360** se han popularizado para facilitar el registro de viajeros. Estas aplicaciones permiten, por ejemplo, **escáner el DNI con el móvil o que el propio huésped introduzca sus datos online**, integrándose luego con la plataforma policial para enviar automáticamente los partes en plazo. La cuestión es: ¿es esto compatible con no guardar copias? La respuesta es **sí**, siempre que se configuren correctamente.

De hecho, **el uso de apps tipo AlojaSCAN puede mejorar el cumplimiento legal** si se emplean adecuadamente. Por ejemplo, AlojaSCAN funciona así: el anfitrión crea una reserva en la app y envía un enlace al cliente principal; **el cliente rellena sus datos y los de sus acompañantes desde ese enlace, pudiendo incluso escanear su DNI con la cámara del móvil** (la app le pide tomar una foto del **dorso del DNI**, donde está la zona de lectura mecánica, para **extraer automáticamente los datos**) [53] [54]. Cuando el cliente llega al alojamiento, el propietario solo tiene que **validar que los datos coinciden con el documento original mostrado** y, con un clic, **enviar el registro de entrada a la policía** [55]. **Todo el proceso se completa en menos de 24 horas**, cumpliendo la exigencia legal [55].

Las ventajas de estos sistemas son varias: eliminan errores de transcripción (al leer automáticamente del DNI), agilizan el trámite y generan un **registro informático unificado**. AlojaSCAN, por ejemplo, **crea el libro de registro en PDF y lo conserva por el tiempo reglamentario** [19], liberando al propietario de llevar archivos en papel. Además, envía la información directamente a la policía sin que el hospedero tenga que entrar manualmente en la web oficial cada vez [56].

**Ahora bien, es importante verificar que estas herramientas respeten los principios de minimización y seguridad**. Según Monlex (asesoría legal que colabora en Hosteltur), **es perfectamente legal que los hoteles usen sistemas tecnológicos de check-in (OCR, escáneres digitales)** siempre que **extraigan únicamente los datos requeridos y no conserven la imagen completa del documento** una vez obtenidos [57] [25]. Las recomendaciones específicas para el uso de estas apps incluyen:

- **Configurar la app para no guardar imágenes:** La aplicación debe estar diseñada para **no almacenar la foto del DNI** tras procesarla. En el caso de AlojaSCAN, la foto del dorso del DNI se usa solo para leer automáticamente los campos (nombre, número, etc.) y luego esos datos se guardan estructurados, **pero la imagen no se almacena permanentemente** (según las pautas generales indicadas por los expertos) [25]. Conviene confirmarlo leyendo la política de privacidad o documentación de la app; por ejemplo, Aloja360 en su web de privacidad se compromete al cumplimiento del RGPD, lo que implica no conservar datos más de lo necesario [58].

- **Almacenar solo datos obligatorios:** Asegúrese de que el sistema **solo pida los campos obligatorios** del viajero. Si la herramienta solicita, por ejemplo, la dirección completa o el correo electrónico del huésped **y** esa información no es requerida por la ley (en el nuevo RD 933/2021 sí

se menciona el domicilio habitual y contacto del viajero en el anexo I, aunque no está claro si es obligatorio comunicarla siempre), valore si realmente necesita recogerla. Lo ideal es que la app permita marcar qué campos son opcionales. En todo caso, ninguna aplicación debe forzar al cliente a subir *selfies* o documentos adicionales más allá del DNI/Pasaporte para completar el registro legal, ya que eso sería excesivo. AlojaSCAN, de hecho, **se limita al escaneo del DNI y a pedir al cliente que complete teléfono y email manualmente** (datos que sí pueden ser útiles para el anfitrión pero que habría que tratar conforme a RGPD con su debida información) [59].

- **Seguridad de la información:** Verifique que el proveedor maneje los datos de forma segura. Por ejemplo, **AlojaSCAN indica que guarda los datos en servidores certificados en España con medidas de seguridad elevadas** [60]. Esto es importante porque está alojando datos personales de sus huéspedes en la nube de ese proveedor. Asegúrese también de tener un contrato o acuerdo de tratamiento de datos con el proveedor, como exige el RGPD para encargados del tratamiento.

- **No relajarse en la verificación:** Aunque la tecnología ayuda, **siga comprobando personalmente la identidad** cuando el cliente llegue. La app le facilitará que los datos ya estén escritos, pero un empleado debe contrastar que el nombre y número de DNI que aparecen coinciden con el documento físico que presenta el cliente. Así se cumple con la responsabilidad de garantizar la **exactitud de los datos** frente al documento original [22] [61]. Una vez validado, se procede al envío telemático. Esto cierra el círculo cumpliendo tanto la normativa de Interior (envío del parte en <24h) como la de protección de datos (solo se ha tratado lo imprescindible y con seguridad).

En cuanto a **Aloja360/AlojaSCAN y la funcionalidad de guardar copias**: por la información disponible, su enfoque es más bien el contrario, es decir, facilitar el **no tener que guardar copias**. Permiten que el cliente introduzca datos y use el escáner integrado, con lo que el propietario no necesita hacer fotocopias; y luego almacenan en la plataforma únicamente los datos estructurados necesarios para el registro y el histórico de reservas [62] [63]. Si alguna herramienta ofreciera la opción de **descargar o almacenar la imagen del documento**, sería aconsejable **no utilizar esa función**, ya que, como hemos reiterado, no está justificada legalmente. En su lugar, confiar en que la herramienta ha capturado correctamente los datos y mantener solo esos campos.

En definitiva, **los sistemas como AlojaSCAN son compatibles con la protección de datos siempre que se usen de forma acorde a la ley**. Los expertos señalan que el miedo inicial de algunos hoteleros a usar OCR tras la entrada en vigor del RD 933/2021 es infundado: lo que está prohibido es guardar imágenes completas, **pero usar tecnología para extraer los datos de forma eficiente es "totalmente válido" y recomendable, siempre cumpliendo los principios del RGPD** [25] [64]. Por tanto, se puede abrazar la digitalización del check-in sin vulnerar la privacidad: **la clave es configurar y proceder bien, de modo que ni un byte de información extra quede almacenado**. Esto permitirá al alojamiento beneficiarse de la automatización (menos errores, menos trabajo manual, experiencia más rápida para el cliente) **sin incurrir en los vicios de antes (fotocopias archivadas, etc.)**.

## Conclusiones

**¿Está legalmente autorizado un alojamiento turístico a guardar una copia del DNI de los huéspedes?** En términos generales, **no: la legislación nacional (Ley 4/2015 y RD 933/2021) no contempla ni autoriza que los hoteles, apartamentos o casas rurales almacenen fotocopias o escaneos del documento de identidad de los viajeros como parte del registro obligatorio** [8]. Lo exigido es únicamente **recoger ciertos datos** del documento e informar de ellos a las Fuerzas de

Seguridad, manteniéndolos en un registro durante 3 años [65] [16]. **Conservar una copia física o digital del documento va más allá de lo requerido** y, salvo situaciones excepcionales, **colisiona con la normativa de protección de datos** por exceder la finalidad autorizada [8] [30].

Desde el punto de vista práctico, **no se recomienda a los alojamientos conservar copias del DNI** de sus clientes. **No hace falta** para cumplir la ley, **supone un riesgo** (de sanción y de seguridad) y puede erosionar la confianza del cliente. Las autoridades de protección de datos han demostrado que sancionarán estas prácticas: ya hay precedentes de multas a hoteles y anfitriones que insistieron en fotocopias sin base legal [35] [27]. También la policía ha alertado de los peligros de que circulen copias de documentos de identidad [44]. Por tanto, la directriz para el sector es clara: **identificar al viajero sí, pero almacenar su documento no**.

En caso de que un alojamiento, por desconocimiento o precaución excesiva, hubiese estado guardando tales copias, debería **rectificar de inmediato**: destruir las copias acumuladas (salvo quizás las de huéspedes actualmente alojados, que deberían eliminarse al hacer check-in efectivo) y ajustar su procedimiento. En su lugar, debe implementar las **buenas prácticas** mencionadas: pedir solo los datos obligatorios, informar adecuadamente, asegurar los sistemas y usar herramientas digitales conforme a RGPD. Por ejemplo, puede adoptar soluciones donde se escanea el DNI solo para rellenar automáticamente el formulario, **sin almacenarlo**, y donde tras el envío a la policía los datos quedan registrados en la base de datos segura, cumpliendo los 3 años de custodia legal.

**¿Y si la policía o la Guardia Civil "piden" algo al alojamiento?** Lo que pueden exigir es ver el **libro-registro de viajeros** o comprobar que se han enviado los partes de determinado día (y sancionar si no se hizo). **No pueden exigir legalmente unas fotocopias de DNI que la normativa no prevé**. Un alojamiento diligente tendrá sus libros-registro al día (sea en papel firmado o en PDF exportable) y podrá mostrarlos a la autoridad en una inspección [19]. En cambio, tener o no tener fotocopias carece de relevancia para la inspección, puesto que **no es un requerimiento normativo**. Incluso ante investigaciones específicas (por ejemplo, la policía busca a una persona y consulta si estuvo hospedada), el alojamiento proporcionará los datos registrados (nombre, DNI, etc.) pero **la identificación final la hará la policía por sus medios**, no necesita que el hotel le entregue un documento que, de hecho, legalmente no debería conservar.

Finalmente, cabe mencionar que **esta postura estricta no va en contra del negocio, sino a su favor**. Proteger los datos de los clientes y evitar recolectar información de más es parte de la **responsabilidad social y legal** de cualquier empresa moderna. En el sector turístico, donde la experiencia y la confianza del viajero son vitales, demostrar respeto por la privacidad es un plus. Un establecimiento que **cumple la normativa a rajatabla (sin extralimitaciones)** evita sanciones y ofrece garantías a sus huéspedes de que sus datos personales serán tratados con seriedad y prudencia [42] [43].

En conclusión, **no conviene ni es legal guardar copias del DNI de los viajeros salvo que exista una orden o base jurídica específica para ello**. Lo aconsejable es **ceñirse a la ley**: pedir el documento para identificar al huésped, extraer los datos necesarios, reportarlos a la policía en tiempo y forma, y guardar esos datos (y solo esos) el plazo establecido. Cualquier copia adicional debe eliminarse. Siguiendo estas pautas, los alojamientos encontrarán un equilibrio entre la **seguridad pública** (cumpliendo con sus obligaciones ante Interior) y la **protección de datos personales** de sus clientes, evitando riesgos tanto legales como reputacionales en el camino. **La normativa está para quedarse y adaptarse a ella es invertir en el futuro del negocio**, tal como destacan los expertos [43]. En definitiva: **identificar sí, copiar no**.

**Fuentes:** Normativa oficial (LO 4/2015; RD 933/2021) y opiniones de la AEPD y expertos en protección de datos [8] [10] [24] [27], entre otros. Las referencias citadas incluyen declaraciones de la AEPD,

Boletines Oficiales del Estado y guías especializadas para asegurar la fidelidad de la información proporcionada.

---


1 2 5 6 15 16 17 18 20 21 22 23 61 BOE-A-2021-17461 Real Decreto 933/2021, de 26 de octubre, por el que se establecen las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor.
https://www.boe.es/buscar/doc.php?id=BOE-A-2021-17461

3 4 10 11 27 37 38 39 44 52 Pedir fotocopia del DNI en hoteles y alojamientos turísticos: un error legal que puede salir muy caro - CINC
https://www.cinc.com/es/pedir-fotocopia-del-dni-en-hoteles-y-alojamientos-turisticos-un-error-legal-que-puede-salir-muy-caro/

7 26 29 30 32 33 34 40 41 ¿Es legal escanear DNI en hotel?⚖ | NoHayDerecho© ⚖
https://nohayderecho.com/es-legal-que-un-hotel-escanee-mi-dni-o-pasaporte-al-hacer-el-check-in/

8 9 28 31 35 36 42 43 45 46 48 49 50 51 65 Registro de viajeros: ¿Puede un hotel exigir una copia del DNI? La AEPD responde
https://www.hosteltur.com/comunidad/005947_registro-de-viajeros-puede-un-hotel-exigir-una-copia-del-dni-la-aepd-responde.html

12 13 14 Qué datos piden los hoteles con el nuevo registro de viajeros
https://www.newtral.es/datos-registro-viajeros-hoteles/20241216/

19 53 54 55 56 59 60 62 63 AlojaSCAN como funciona | Aloja360
https://aloja360.com/alojascan/alojascan-como-funciona/

24 25 47 57 64 ¿Puedo escanear el DNI de mis huéspedes? Así debes hacerlo legalmente
https://www.hosteltur.com/comunidad/006016_puedo-escanear-el-dni-de-mis-huespedes-asi-debes-hacerlo-legalmente.html

58 Política de Privacidad Aloja360 y AlojaSCAN
https://aloja360.com/aviso-legal/politica-de-privacidad-aloja360/