

**CONFEDERACION ESPAÑOLA DE
ORGANIZACIONES**

INFORMATICA@CEOE.ES

Registro de Entrada: REGAGE26e00042669773

CONSULTA PRESENTADA

Se solicita se resuelva la consulta adjunta que formula CEOE, como representante del sector empresarial, en relación con la aplicación del Real Decreto 933/2021.

En concreto, sobre los tratamientos realizados por los sujetos obligados por el 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 y, respecto de la identificación de los viajeros, el empleo de sistemas automatizados de lectura de documentos, la conservación de datos, la trazabilidad, la seguridad y la intervención de terceros.

La consulta señala expresamente que no pretende cuestionar la obligación material establecida por el Real Decreto 933/2021, sino obtener criterios operativos sobre su aplicación desde la perspectiva de la normativa de protección de datos.

Sobre las cuestiones planteadas debe partirse de la regulación aplicable en materia de protección de datos de carácter personal: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos. RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Como indica la Exposición de motivos de la LOPDGDD “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”.

En términos prácticos, este principio requiere que las organizaciones analicen *qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo*. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

Respecto a la función consultiva de la AEPD dirigida a los Delegados de Protección de Datos, la Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, el CAPÍTULO III, apartado cinco a), señala lo siguiente:

“5. No serán objeto de respuesta las consultas:

(.....)

c) Que pretendan la validación de actuaciones o documentos en materia de protección de datos elaborados por responsable o encargados.”

En consecuencia, le indicamos que esta AEPD no tiene entre sus competencias el análisis y la validación de aplicaciones informáticas más allá de señalar que en su diseño deberán cumplir con la normativa de protección de datos. Los responsables del tratamiento y, en su caso, los responsables de la aplicación informática deberán conocer bien el contexto en el que ha de aplicar el RGPD y la conformidad final dependerá de cómo se implementen y documenten ciertos aspectos clave en su funcionamiento y los tratamientos de datos asociados. También deberá determinar las medidas más adecuadas en atención al análisis de riesgos para cada tratamiento.

Como orientación general a las cuestiones que se plantean, el Real Decreto 933/2021, tiene por objeto regular las obligaciones de registro documental e información previstas en la normativa de protección de la seguridad ciudadana.

El propio preámbulo de la norma señala que estas obligaciones se establecen en desarrollo del artículo 25.1 de la Ley Orgánica 4/2015, de protección de la seguridad ciudadana, y que responden a la necesidad de disponer de herramientas de control sobre actividades relevantes para la seguridad ciudadana, en particular ante las amenazas derivadas del terrorismo y del crimen organizado.

El artículo 4 del Real Decreto establece la obligación de los sujetos obligados de recoger los datos de las personas usuarias de establecimientos de hospedaje y de alquiler de servicios necesarios para su registro y comunicación, mientras que el artículo 5 determina los datos que deben constar en el correspondiente registro y su periodo de conservación. El artículo 6 regula su comunicación a las autoridades competentes.

Por su parte, el artículo 7 establece un régimen específico respecto del tratamiento de los datos personales generados en ejecución del Real Decreto. En particular, dispone que dichos datos se conservarán en ficheros radicados en la Secretaría de Estado de Seguridad y que su tratamiento podrá ser realizado por las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus competencias de prevención, detección e

investigación del delito, estableciendo expresamente su apartado 3 que el tratamiento de los datos de carácter personal derivados de la ejecución del Real Decreto se llevará a cabo conforme a la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Esta regulación debe tenerse en cuenta al analizar los tratamientos efectuados por los distintos intervinientes, diferenciando las operaciones de recogida y registro que corresponden a los sujetos obligados de los tratamientos posteriores efectuados por las autoridades competentes. En todo caso, la existencia de una finalidad de seguridad ciudadana y la remisión a la Ley Orgánica 7/2021 no permiten entender que los sujetos obligados puedan recoger o conservar indiscriminadamente todos los datos contenidos en los documentos utilizados para acreditar la identidad. Las operaciones realizadas para cumplir las obligaciones del Real Decreto deberán respetar los principios de protección de datos que resulten aplicables, en particular el principio de minimización, y deberán limitarse a la información necesaria para cumplir las obligaciones legalmente establecidas.

Esta AEPD, en la [“NOTA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS CON RELACIÓN A LA SOLICITUD DE COPIAS DE DOCUMENTOS DE IDENTIDAD EN HOSPEDAJES PARA DAR CUMPLIMIENTO AL REAL DECRETO 933/2021”](#), señala que solicitar o conservar una copia íntegra del documento de identidad (DNI o pasaporte), vulnera el principio de minimización de datos, establecido en el artículo 5.1.c) del RGPD, y supone un tratamiento excesivo de datos al contener más datos que los obligados a aportar en virtud de la normativa aplicable, como la fotografía, la fecha de caducidad del documento, el CAN o el nombre de los padres de su titular. También se considera que el hecho de entregar una copia de la documentación personal implica, entre otros, un riesgo innecesario de suplantación de la identidad, que debe ser evitado o, por lo menos, mitigado de manera efectiva.

Por otro lado, el DNI no contiene toda la información requerida por el Anexo I del Real Decreto (como el correo electrónico o el teléfono), por lo que el escaneo por sí solo no basta para cumplir la norma.

El hecho de que el documento de identidad contenga información adicional a la exigida por el Real Decreto 933/2021 no significa que toda exposición visual inevitable de esos datos constituya, por sí misma, un tratamiento ilícito.

Debe diferenciarse entre lo que puede ser la mera visualización incidental y momentánea de información que aparece en el documento utilizado para verificar la identidad, de la consulta deliberada o utilización de datos que no sean necesarios para la finalidad de identificación y la captación, reproducción o conservación de esos datos.

En el primer supuesto, cuando la visualización sea estrictamente instrumental para comprobar la identidad, y no exista registro o utilización posterior de los datos adicionales, puede considerarse comprendida en la operación de verificación de identidad amparada por la obligación legal en los términos establecidos en el artículo 6.1.c) del RGPD: *“el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento,”*

No obstante, el citado artículo no constituye una habilitación general para acceder a cualquier dato contenido en el documento que deberá limitarse a los necesarios para cumplir la obligación legal.

El responsable debe configurar el procedimiento de manera que la exposición de información adicional sea la mínima posible y que esos datos no sean capturados, registrados, incorporados a sistemas ni utilizados para finalidades distintas.

En consecuencia, la utilización de un sistema de escaneo de documentos de identidad para cumplir con el Real Decreto 933/2021 sería viable únicamente si se garantiza técnicamente que el proceso respeta el principio de minimización de datos.

En este sentido se podría plantear la posibilidad de implantar un sistema de Escaneo Selectivo que funcione mediante tecnología de reconocimiento óptico de caracteres (OCR) que solo extrae y registra los campos de texto exigidos en el Anexo I del Real Decreto 933/2021, sin capturar ni almacenar la imagen del documento ni los datos no requeridos. Si el sistema extrae solo el nombre, número de identidad, nacionalidad y fecha de nacimiento (según el Anexo I), se cumpliría con la obligación de registro.

En todo caso, la AEPD propone métodos de cumplimiento que considera suficientes y menos intrusivos que el tratamiento de imágenes de documentos.

En el hospedaje presencial se considera más idóneo completar un formulario con los datos del Anexo I y realizar una comprobación visual para verificar que los datos coinciden con el documento que el huésped exhibe, sin necesidad de escanearlo. Y en el hospedaje en línea (sin presencia), para la autenticación remota, la AEPD sugiere el uso de certificados digitales, la verificación mediante el medio de pago utilizado, o el envío de códigos de seguridad (OTP) al teléfono o correo electrónico del huésped.

Respecto a la posibilidad de implantar un sistema de Escaneo Selectivo que únicamente extraiga y registre la información exigida por Anexo I del Real Decreto 933/2021, sin capturar ni almacenar datos no requeridos, el responsable del tratamiento (el establecimiento de hospedaje en estos casos), puede responder mejor al principio de minimización que un sistema que conserve una reproducción íntegra del documento, pero la valoración de si una solución concreta cumple efectivamente estas condiciones corresponde al responsable del tratamiento.

Como responsable del tratamiento debe evaluar la compatibilidad del sistema con el RGPD y asegurarse de mitigar el riesgo de suplantación de identidad asociado al manejo de copias digitales.

No corresponde a la AEPD homologar, o certificar una tecnología OCR, ni declarar, con carácter general, que un determinado producto o arquitectura informática cumple el RGPD.

La AEPD ha publicado una [Guía de Protección de Datos por Defecto](#) en la que señala que el responsable debe configurar los tratamientos de manera que, por defecto, únicamente sean objeto de tratamiento los datos necesarios para cada finalidad, incluyendo la cantidad de datos, la extensión del tratamiento, el plazo de conservación y la accesibilidad.

Como antecedente, la [Resolución PS/00078/2021](#) examinó un sistema utilizado por un establecimiento hotelero que escaneaba el pasaporte y utilizaba tecnología OCR para

convertir la imagen en texto e incorporar los campos correspondientes al programa de gestión hotelera. La propia AEPD requirió información sobre el programa empleado y sobre el tratamiento efectuado y la infracción apreciada se vinculó al tratamiento de la fotografía del cliente para finalidades propias del establecimiento, en particular para facilitar la identificación del cliente en los consumos y controlar el acceso, y no a la mera utilización de OCR para transformar los datos del documento en texto. La resolución puso de manifiesto, entre otros extremos, que la fotografía continuaba conservándose en los sistemas del establecimiento pese a que este había afirmado que se eliminaba al finalizar la estancia.

Esta resolución no constituye una validación general del OCR ni de la solución tecnológica utilizada.

Sobre la verificación de identidad sin conservación del documento en la citada nota técnica, la AEPD considera que, en el ámbito presencial, resulta adecuado que el interesado facilite los datos exigidos y que el establecimiento compruebe visualmente que coinciden con el documento exhibido.

En los procedimientos realizados a distancia, la AEPD ha señalado como posibles mecanismos de autenticación los certificados digitales, la comprobación de los datos asociados al medio de pago utilizado o el envío de códigos de seguridad al teléfono o correo electrónico del interesado. La propia Agencia advierte que cualquier otro procedimiento deberá ser evaluado por el responsable del tratamiento. No existe, por tanto, una obligación general de conservar el documento como prueba de que se ha realizado la verificación.

Respecto a los datos del registro, datos internos y evidencias de cumplimiento, el artículo 5.3 del Real Decreto 933/2021 establece expresamente que los datos del registro informático deberán conservarse durante tres años desde la finalización del servicio.

Este plazo se refiere a los datos del registro que deben conservarse conforme al artículo 5 y no puede interpretarse como una habilitación general para conservar durante tres años cualquier otra información generada durante el proceso de identificación.

Cada categoría de datos debe disponer de una finalidad y un plazo de conservación justificados. Si una imagen se genera únicamente como elemento instrumental para obtener determinados datos y deja de ser necesaria una vez realizada esa operación, el responsable deberá valorar su supresión. El hecho de que los datos del registro deban conservarse tres años no permite extender automáticamente ese plazo a la imagen utilizada para obtenerlos.

Del mismo modo, los logs no tienen que conservarse necesariamente durante tres años por el solo hecho de que el registro de viajeros tenga ese periodo de conservación.

Respecto a la necesidad de acreditación del cumplimiento y trazabilidad, el artículo 5.2 RGPD exige al responsable poder demostrar el cumplimiento de los principios del Reglamento.

Los logs, metadatos y registros de transmisión pueden constituir elementos de evidencia adecuados para demostrar determinados aspectos del funcionamiento del tratamiento, pero, no puede afirmarse que constituyan por sí solos un mecanismo suficiente para acreditar el cumplimiento del RGPD en todos los casos.

Además, los propios logs constituyen un tratamiento de datos personales cuando contienen información relativa a personas identificadas o identificables. En consecuencia, su generación, conservación y consulta deberán estar amparadas por una de las bases de legitimación previstas en el artículo 6.1 del RGPD, que deberá determinarse atendiendo a la finalidad concreta perseguida con dichos registros y respetar los principios de minimización y limitación del plazo de conservación.

Sobre la seguridad y delimitación de responsabilidades, el propio Real Decreto establece que las comunicaciones se realizan por procedimientos telemáticos y que la disposición adicional segunda atribuye al Ministerio del Interior el establecimiento de los sistemas y procedimientos de transmisión y conservación (artículo 6).

Por tanto, el sujeto obligado no puede ser considerado responsable de decisiones técnicas sobre una infraestructura que no diseña ni controla.

No obstante, mantiene las obligaciones que corresponden a las operaciones que se encuentran bajo su ámbito de decisión, entre ellas la adecuada recogida de los datos, la configuración de sus propios sistemas, la gestión de accesos, la seguridad de los dispositivos utilizados, la selección de proveedores y la protección de los datos antes de su transmisión.

La responsabilidad deberá delimitarse atendiendo a la capacidad efectiva de decisión y control de cada interviniente.

El artículo 32 RGPD exige al responsable y al encargado adoptar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. La AEPD ha reiterado que las medidas deben determinarse atendiendo al riesgo concreto y que deben ser objeto de revisión y evaluación de su eficacia.

En este sentido, cuando el responsable utilice una solución tecnológica proporcionada por un tercero, deberá ejercer la diligencia exigible conforme a los artículos 24, 25, 28 y 32 RGPD.

El artículo 28.1 RGPD exige seleccionar únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas. La selección del encargado debe realizarse atendiendo a las garantías efectivamente ofrecidas y no limitarse a incorporar cláusulas generales de cumplimiento.

El responsable podrá valorar la utilización de medios automatizados para facilitar la obtención de los datos exigidos por el Real Decreto 933/2021 y le corresponde determinar, mediante el correspondiente análisis de riesgos y en aplicación de los principios de protección de datos desde el diseño y por defecto, si la solución concreta resulta necesaria y proporcionada y si garantiza que únicamente se tratan los datos necesarios para cumplir la obligación legal. El responsable deberá asimismo comprobar y poder acreditar el funcionamiento efectivo de la solución, incluida la eventual generación, conservación y eliminación de imágenes o datos adicionales.

Este tipo de tratamiento de datos personales implica la utilización de nuevas tecnologías y cuando del análisis de riesgos resulte que el tratamiento probablemente entrañe un alto riesgo, deberá realizarse la correspondiente evaluación de impacto en protección de datos (EIPD) conforme al artículo 35 RGPD. La AEPD dispone de herramientas específicas para apoyar esta valoración, pero advierte expresamente que esas herramientas no sustituyen las decisiones que corresponden al responsable sobre los fines y medios del tratamiento.

Por tanto, la existencia de una EIPD, un análisis de riesgos o unos logs no constituye por sí sola una certificación de cumplimiento. Lo relevante es el conjunto de medidas y evidencias y su correspondencia con el tratamiento efectivamente realizado.

Una EIPD es una herramienta preventiva que el responsable del tratamiento debe realizar para identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento y debe realizarse antes de que se ejecute el tratamiento efectivo de los datos o cuando cambien las condiciones del tratamiento o varíen los riesgos asociados.

Se pueden consultar los recursos de ayuda publicados por la AEPD para realizar la evaluación del riesgo y la EIPD en el [área de actuación de innovación y tecnología de la web](#)

No existe un documento o mecanismo único que determine el cumplimiento del principio de responsabilidad proactiva. Lo relevante es que el responsable pueda demostrar que ha identificado y legitimado el tratamiento, evaluado sus riesgos, aplicado los principios de protección de datos desde el diseño y por defecto y adoptado medidas adecuadas y eficaces

También puede resultar de interés la consulta de los siguientes enlaces:

<https://www.aepd.es/preguntas-frecuentes/2-rgpd/10-evaluacion-de-impacto>

<https://www.aepd.es/preguntas-frecuentes/1-tus-derechos/3-identificacion-con-dni>

<https://www.aepd.es/documento/listas-dpia-es-35-4.pdf>

<https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>

<https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-informa-de-que-no-esta-permitido-solicitar-copia-dni-o-pasaporte-en-hospedajes>

<https://www.aepd.es/guias/nota-aepd-registro-hospedajes.pdf>

<https://www.aepd.es/documento/ai-00413-2024.pdf>

Esta respuesta constituye una actividad meramente informativa de la AEPD; no tiene efectos vinculantes, no modifica la situación jurídica del solicitante y no constituye un acto recurrible.

Atentamente.