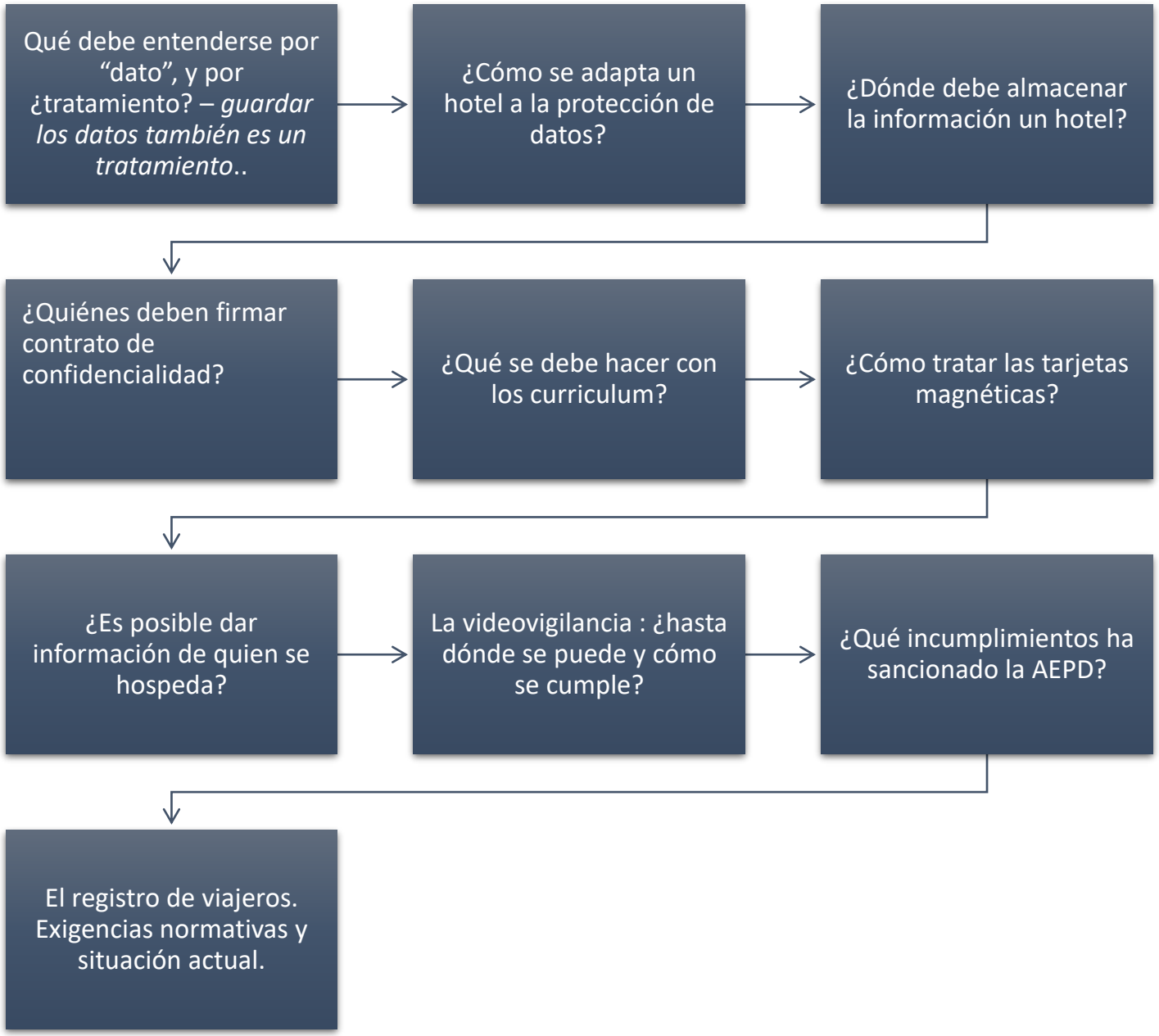
Tourism & Law
ABOGADOS

CEHAT
CONFEDERACIÓN ESPAÑOLA DE HOTELES Y ALOJAMIENTOS TURÍSTICOS

LA PROTECCIÓN DE DATOS EN LOS HOTELES, CONOCER Y ADAPTARSE A LA NORMATIVA Y DESTACARSE POR OFRECER GARANTÍAS A LOS CLIENTES

Indice


Qué debe entenderse por "dato", y por ¿tratamiento? – *guardar los datos también es un tratamiento*..
¿Cómo se adapta un hotel a la protección de datos?
¿Dónde debe almacenar la información un hotel?
¿Quiénes deben firmar contrato de confidencialidad?
¿Qué se debe hacer con los curriculum?
¿Cómo tratar las tarjetas magnéticas?
¿Es posible dar información de quien se hospeda?
La videovigilancia : ¿hasta dónde se puede y cómo se cumple?
¿Qué incumplimientos ha sancionado la AEPD?
El registro de viajeros. Exigencias normativas y situación actual.

Qué debe entenderse por “dato”, y por ¿tratamiento? – guardar los datos también es un tratamiento

- El derecho a la protección de datos de carácter personal es uno de los derechos fundamentales contenidos en la Constitución Española, por ello **TODOS** los que tratamos datos de carácter personal debemos **EVITAR** la vulneración del derecho fundamental a la protección de datos.

- La definición de dato personal se encuentra en el art.4.1 del RGPD : “Toda información sobre una persona física identificada o identificable”.

- Ejemplos de datos personales son: nombre y apellidos, numero de teléfono, DNI, fotografía, voz, huella, correo electrónico, la cuenta de una red social, la dirección de la vivienda, síntomas o información médica, número de afiliación a la Seguridad Social, imágenes de videocámaras, etc.

- Conforme a la normativa de protección de datos, consiste en cualquier operación realizadas sobre datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

2. ¿Cómo se adapta un hotel a la protección de datos?

1. Incluir textos legales en la página web.
2. El consentimiento de los interesados.
3. Registro de actividades de tratamiento.
4. Contratos de tratamiento con terceros.

5. Notificar brechas de seguridad.
6. Realizar evaluaciones de impacto y análisis de riesgos.

El Delegado de Protección de datos

2.1 ¿Cuáles son los textos legales?

- Si se tiene una página web se debe incluir en ella los textos exigidos por la ley de Protección de Datos y la LSSI (Ley de servicios de la sociedad de la información y de comercio electrónico):

- Aviso legal: es el documento donde se identifica al propietario de la página web.

- Política de privacidad: ahí se ha de informar en detalle del procesamiento de los datos, que se realiza en el establecimiento de manera informando expresa.

- Política de cookies : Cookies usadas en la página, su finalidad y duración de las mismas.

2.2 ¿Cómo debe ser el consentimiento ?

- El RGPD requiere que el consentimiento sea "inequívoco", lo que supone que se preste mediante una manifestación del interesado o mediante una clara acción afirmativa.

- Esto excluye la utilización del llamado consentimiento tácito, que permitía la anterior normativa española de protección de datos.

- Así, no se consideran formas válidas de obtener el consentimiento el uso de casillas ya marcadas o la inacción. En cambio, sí son acordes al RGPD, la utilización de una declaración por escrito, o la marcación de casillas en un sitio web de internet.

2.3 Registro de actividades de tratamiento.

- Los responsables están obligados a llevar un registro de las actividades de tratamiento bajo su propia responsabilidad.

- Aunque el Reglamento no obliga a todos los responsables o encargados a llevarlo a cabo, no siendo obligatorio para empresas con menos a 250 trabajadores, si establece otros requisitos, entre los que se encuentran el realizar tratamiento que puedan entrañar un riesgo para libertades de los interesados, que dicho tratamiento no sea ocasional, o incluyan categorías especiales de datos personales.

- En la medida en que un hotel puede recabar información de datos sobre alergias alimenticias (categoría especial), o realizar un tratamiento no ocasional, puede exigírsele este RAT.

2.4 Contratos de tratamiento con terceros.

- El sector hotelero se relaciona constantemente con terceros, como las agencias de viaje online, que también disponen de algunos de los datos de los usuarios. Por ello, aparte del registro de actividades de tratamiento, debes tener presente una lista de esas empresas externas con las que tienes contacto y asegurar que también cumplan la normativa de Protección de Datos.
- Por ejemplo: Agencias de viajes, asesorías, empresas informáticas, empresas de transporte, etc.

- Para cumplir con este requisito, es necesario la firma de un **CONTRATO DE ENCARGO DE TRATAMIENTO** con esos terceros en el que se establezcan las obligaciones de ambos para proteger los datos personales a los que accedan, en aplicación del art. 28 del RGPD.

2.5 Notificar brechas de seguridad.

- Otra de las obligaciones que establece Reglamento es en caso de producirse una brecha de seguridad, el notificarlo a la AEPD, pudiendo extenderse esa obligación, según el caso, también a los afectados.

- Una brecha de seguridad es un incidente que permite el acceso a terceros sin autorización a los datos que trata el hotel. Normalmente, se produce cuando un intruso logra sortear los mecanismos de seguridad, pero también cuando hay una perdida de ordenador, tablet o móvil que pueda permitir el acceso no autorizado de terceros.

- En el caso de que se dé una situación de ciberataque o infracción por parte del hotel, lo ideal es estar prevenidos con un plan de respuesta ante incidentes de seguridad. Además tienes un plazo de 72 horas para notificarlo a la AEPD y darle información de lo que ha ocurrido.

- Por tanto, es esencial tener implementado un plan de seguridad para garantizar que se cumple con las obligaciones en esta situación y con la comunicación en plazo.
-

2.6 Realizar evaluaciones de impacto y análisis de riesgos.

- El hotel debe también realizar **ANÁLISIS DE RIESGOS** en el que se valoren las posibles contingencias de los tratamientos que se realicen, teniendo en cuenta, entre otras cuestiones,
- el tipo de tratamiento,
- la naturaleza de los datos, o
- el número de interesados afectados;

- Además, si el riesgo resultara ser especialmente alto deberán realizar una **EVALUACIÓN DE IMPACTO** para minimizar las posibilidades de afectar a los derechos o libertados de los interesados; tras estos análisis deberán implementar unas medidas de seguridad adecuadas.

El Delegado de Protección de datos

- En principio, la LOPDGDD no incluye a los establecimientos hoteleros entre las entidades obligadas a contar con un Delegado de Protección de Datos o DPO.

- Si bien es posible su nombramiento de manera voluntaria.

- Esta figura solo es obligatoria en caso de que se traten a gran escala de categorías especiales de datos y datos relativos a condenas e infracciones penales, así como si se trata por cualquiera de las entidades determinadas en el art. 34 de la LOPDGDD, como son : las entidades bancarias, compañías aseguradoras, los centros docentes, los colegios profesionales, los centros sanitarios, empresas de seguridad…… y el resto de las entidades detalladas en el artículo.

3. ¿Dónde debe almacenar la información un hotel?

- La localización de la información también es importante con el Reglamento Europeo de Protección de datos.

- Así, si se toman datos en soportes físicos, debe asegurarse la confidencialidad, la seguridad, y proceder a la eliminación de los datos de forma segura y cumpliendo con el protocolo de conservación de datos.

- *** en ese sentido, dejar en la recepción fotocopia de documentación de clientes con acceso a terceros puede suponer una sanción, si esto es denunciado ante la AEPD.

- - si se toman datos online, entonces debe elegirse una solución o servicio informático que cifre los datos y los almacene de forma segura. En el caso de que los datos se almacenen en un servicio en la nube, se ha enseñar a los empleados a crear contraseñas fuertes. Por eso, es importante que las firmas hoteleras formen a su personal sobre los potenciales riesgos informáticos y de qué manera afrontar un posible ciberataque.

4. ¿Quiénes deben firmar contrato de confidencialidad?

- El personal del hotel con acceso a datos está sujeto a la obligación de guardar secreto y confidencialidad sobre los datos obtenidos, por ello otra de las obligaciones en materia de protección de datos en hoteles es la de FIRMAR UN ACUERDO DE CONFIDENCIALIDAD con los empleados para evitar que la información a la que tienen acceso sea revelada a personas no autorizadas. Los empleados tienen que cumplir las medidas de seguridad que la empresa establezca para asegurar la protección de los datos personales.

- En el RGPD se establece que los acuerdos de confidencialidad deben ser firmados por todas las personas que tengan acceso a la información, independientemente del tipo de relación profesional que mantengan con la empresa.

5.¿Qué se debe hacer con los curriculum?

- Para su recogida y tratamiento, es necesario el consentimiento informado y expreso del interesado, independientemente de que la persona lo haya enviado de manera voluntaria.

- Por tanto, en el caso de que una persona nos entregue su currículum debemos:

- Recabar su consentimiento para el tratamiento de sus datos.
- Informarle de que sus datos van a ser objeto de tratamiento.
- Facilitarle el ejercicio de sus derechos ARCO, en caso de que quiera cancelar o rectificar sus datos.

- Para ello debe firmar un consentimiento para tratar sus datos personales. Si no lo hacemos, nos enfrentamos a importantes sanciones en caso de denuncia.

6. ¿Cómo tratar las tarjetas magnéticas?

- Normalmente la tarjeta magnética de acceso a las habitaciones no contiene datos de carácter personal, se activan de modo automático al registrar al cliente. La información que recoge es el número de habitación y los días de uso habilitados, y se desactivan la marchar el cliente.

- Sólo el personal de administración del establecimiento puede conocer quién se aloja revisando el registro del cliente y habitación asignada.

- Por supuesto, el personal del hotel con acceso a datos está sujeto a la obligación de guardar secreto y confidencialidad sobre los datos obtenidos.

- Los establecimientos que personalicen las tarjetas magnéticas de acceso a las habitaciones, almacenando en ellas datos de carácter personal (nombre y apellidos del cliente) deben solicitar al cliente su consentimiento expreso para su cesión a terceras personas (al personal de limpieza, mantenimiento,..)

7. ¿Es posible dar información de quien se hospeda?

- Los hoteles solo podrán ceder información de sus huéspedes si han obtenido el CONSENTIMIENTO EXPRESO de éstos para ello. Por ejemplo, a proveedores de servicios o a otras empresas asociadas.

- OBLIGACION : En virtud de la ley 4/2015, de Protección de la Seguridad Ciudadana, las personas físicas o jurídicas que ejerzan actividades de hospedaje, transporte de personas, acceso comercial a servicios telefónicos o telemáticos, etc, deberán informar sobre la identidad de sus clientes a los Cuerpos y Fuerzas de Seguridad del Estado en un plazo de 24 horas. – **REGISTRO DE VIAJEROS-**

8. La videovigilancia : ¿hasta dónde se puede y cómo se cumple?

- Si se dispone de cámaras es obligatorio disponer de cartel informativo, donde se recoja la información de quien es el responsable del tratamiento de esos datos. No se puede colocar cámaras de seguridad ni en lugares que enfoquen a la vía pública, ni a viviendas o instalaciones privadas.

- Dentro de las instalaciones, tampoco se podrán colocar en lugares íntimos como los baños o aseos, o en zonas destinadas al descanso o esparcimiento de los empleados.

- Respecto a los trabajadores:

- Para que el uso de cámaras en el trabajo sea legal es necesario informar a los empleados sobre su instalación, funcionamiento y el tipo de datos que recogen. No es suficiente con colocar un cartel informativo.

- Las obligaciones legales de la empresa quedan cubiertas con la comunicación a los trabajadores, es decir, no se requiere el consentimiento de los empleados para la instalación de cámaras de vigilancia.

9. ¿Qué incumplimientos ha sancionado la AEPD?

- En lo que va del año 2022 la AEPD ha publicado más de 175 procedimientos sancionadores, con una recaudación que supera los 20 millones de euros.

- Aunque las multas más altas corresponden a incumplimientos en servicios de internet, también se han sancionado al sector hotelero, la de mayor recercusión fue la impuesta a un establecimiento hotelero por tratar datos excesivos de sus clientes sin legitimación- (caso del escaneo de pasaporte).

- Otros motivos de sanción han sido : no cumplir con la minimización de datos, tratamiento ilícito de los datos de los interesados, no facilitar información al interesado sobre el tratamiento de sus datos, la falta de confidencialidad, y las brechas de seguridad.

10. El registro de viajeros. Exigencias normativas y situación actual.

El pasado 27 de octubre de 2021 se publican en el Boletín Oficial del Estado el Real Decreto 933/2021 , 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.

Ampliar las personas obligadas a cumplir con las obligaciones, añadiendo a los ya obligados: sector hotelero en general , a los operadores turísticos, las plataformas digitales, las viviendas de uno turístico y la actividad de alquiler de vehículos.

Los obligados deben recoger los datos desde el 27 de abril de 2022

Moratoria para la comunicación de datos:

Las previsiones relativas a las obligaciones de comunicación producirán efectos a partir del 2 de enero de 2023.

OBLIGACIÓN DE REGISTRO:

En el caso de las personas menores de catorce años, sus datos serán proporcionados por la persona mayor de edad de la que vayan acompañados.

Deberán ser firmados por toda persona mayor de catorce años que haga uso de los mismos.

Los partes y hojas serán proporcionados por el establecimiento de hospedaje el cual será responsable de la exactitud de los datos.
Los sujetos obligados habrán de llevar un **REGISTRO INFORMÁTICO**.
Deberán conservarse durante un plazo de **TRES AÑOS** a contar desde la finalización del servicio o prestación contratada.

COMO SE COMUNICA:

La comunicación se realizará de manera inmediata, y en todo caso en un plazo no superior a 24 horas, respectivamente, a partir de los siguientes momentos:

a) Al realizar la reserva o la formalización del contrato o, en su caso, su anulación.

b) Al inicio de los servicios contratados.

La transmisión y conservación de los datos exigida por este real decreto a los sujetos obligados se hará conforme a los
sistemas y procedimientos que se establezcan por el Ministerio del Interior : AUN SIN DESARROLLAR.

CONCLUSION Y ESTADO ACTUAL:

Teniendo en cuenta que la mayor parte de las transacciones comerciales se realizan de manera electrónica, siendo que dichos datos son tratados por los proveedores de servicios de pago, sin que los establecimientos tengan acceso a ellos por razones de seguridad, la recogida de estos datos se antoja cuanto menos inviable, sino contraria al principio de minimización de los datos personales.

Recientemente hemos conocido **SENTENCIA TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA** C-817/2019, de 21 de junio de 2022 que responde a diez cuestiones planteadas por el Tribunal Constitucional de Bélgica sobre la ley belga que regula el sistema de recogida y tratamiento de datos de pasajeros para vuelos intracomunitarios con la finalidad de prevenir delitos de terrorismo y delitos graves, desde la que el alto organismo considera que es incompatible con el derecho de la unión la exigencia por parte del derecho interno de los estados el solicitar datos a todos los pasajeros indistintamente, cuando no existen indicios objetivos capaces de demostrar la existencia de un riesgo relacionado con delitos de terrorismo, o delitos graves.

Teniendo ello presente, al igual que ocurre con la comunicación de datos PNR, la recogida y comunicación de datos derivada del registro de viajeros también debe entenderse como una injerencia a los derecho garantizados en los artículos 7 y 8 de la Carta de la Unión Europea, y, si bien pudiera ser legítima, al perseguir otro derecho también reconocido como es el de la seguridad, la misma debe quedar sujeta a los parámetros de garantía que son :

1. El que sea recogido a través de una Ley (mientras que la obligación actual se recoge por un mero decreto).

2. respetar el principio de proporcionalidad, cuando sea necesaria y responda efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

Resultando desproporcionado que la norma exija recoger y comunicar datos sin una amenaza real, de pernoctaciones hechas en todo el territorio nacional, sin discriminar, ni someter a ámbito temporal su vigencia e imponiendo un periodo de conservación de 3 años, cuando la directiva europea de la que trae causa fija dicho plazo en seis meses, siendo por tanto dicho plazo excesivo y desproporcionado.

CONCLUSION SOBRE LA NORMATIVA DE REGISTRO DE VIAJEROS:

En resumen, dado que el sistema de registro documental de viajeros no aparece regulado en una ley, tiene un alcance general, no se limita a la persecución de la delincuencia de delitos de terrorismo y otros delitos graves, sino a la prevención de todo tipo de delitos, no regula la forma en la que los viajeros pueden conocer y dirigirse a la autoridad que trata los datos recogidos por los establecimientos hoteleros, y les obliga a conservar dichos datos por un periodo de tres años , la injerencia que ello supone al derecho a la intimidad personal y familiar de los viajeros, así como al derecho a la protección de sus datos de carácter personal resulta, a simple vista, incompatible con el Derecho de la Unión Europea.

Paloma Aguilar
paguilar@tandl.es

Gracias por vuestra atención

Tourism & Law
ABOGADOS

www.tourismandlaw.es