AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

PLAN DE INSPECCIÓN DE OFICIO A CADENAS HOTELERAS

CONCLUSIONES Y RECOMENDACIONES

Junio de 2004

Los artículos 27 y 40 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 y 28 del Real Decreto 428/1993, de 26 de marzo por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos habilitan a su Director para realizar auditorias de los sistemas informáticos con miras a determinar su conformidad con las disposiciones de la citada Ley Orgánica.

Al amparo de dichos preceptos se acordó la realización de un Plan de Inspección de Oficio a Cadenas Hoteleras, cuyo resultado se recoge en las conclusiones de la inspección, en las que se ponen de manifiesto ciertas deficiencias respecto del cumplimiento de las previsiones de la Ley Orgánica mencionada y de las normas que la desarrollan.

El documento de conclusiones fue remitido a la Confederación de Hoteles y Alojamientos Turísticos así como a las entidades auditadas para que formulasen observaciones , sin haberse emitido ninguna por parte de aquellas.

Con el fin de posibilitar la subsanación de aquellas deficiencias, así como un correcto cumplimiento del citado marco normativo y, en virtud de las potestades previstas en el artículo 5 c y d) del Real Decreto antes citado, se dictan, con fundamento en las conclusiones que se recogen en el documento adjunto, las recomendaciones incorporadas en el mismo, las cuales deberán ser observadas por las entidades pertenecientes a este sector al objeto de adecuar los tratamientos de datos a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y a sus normas de desarrollo.

Madrid, 25 de junio de 2004

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: José Luis Piñar Mañas

c. Sagasta 22 28004 Madrid www.agpd.es

PLAN DE INSPECCIÓN DE OFICIO A CADENAS HOTELERAS

INDICE

1. INTRODUCCIÓN

Durante los últimos meses del año 2002 y el año 2003, por acuerdo del Director de la Agencia de Protección de Datos (APD), se procedió a realizar un Plan de Inspección de oficio al sector hotelero con objeto de comprobar el grado de adecuación de los ficheros automatizados utilizados para gestionar los datos personales de sus clientes a las prescripciones de la Ley Orgánica 15/1999, de 13 de diciembre (LOPD) y normativa que la desarrolla.

La primera cuestión que se planteó en la Agencia antes de abordar el citado Plan de oficio fue la selección de los establecimientos a los que se debería auditar. Para tener conocimiento del volumen aproximado de hoteles ubicados en el territorio nacional se acudió a la "*Guía Oficial de Hoteles"* en su versión profesional, editada por TURESPAÑA (Secretaría de Estado de Comercio y Turismo del Ministerio de Economía) en el año 2002.

Esta guía contiene un listado de hoteles y hostales de todas las categorías, pensiones de dos estrellas y "*ciudades de vacaciones"* dispersos por toda la geografía española incluidas las islas. Analizados todos los datos publicados se conoció que la oferta hotelera está compuesta por aproximadamente 10.000 establecimientos de los cuales, 86 son paradores de turismo con una oferta de 9.978 plazas hoteleras, 1.220 hoteles integrados en 132 cadenas hoteleras con 439.977 plazas hoteleras ofertadas, 131 son hoteles balnearios, y el resto de establecimientos corresponden a entidades independientes.

El principal objetivo de la inspección era auditar los distintos tratamientos que realizan los hoteles con los datos personales de los clientes que se hospedan en ellos o que contratan la celebración de eventos en sus salones, con la idea de exponer las conclusiones obtenidas de forma anónima y elaborar recomendaciones que sirvan para que cualquier establecimiento del sector pueda adecuar su funcionamiento a la normativa de protección de datos. Se ha prescindido, por tanto, de otros tratamientos como los relativos a la gestión de recursos humanos proveedores u otros distintos de los relacionados con la clientela.

Ante tal oferta de establecimientos y plazas hoteleras y teniendo en cuenta el objetivo de la Agencia, se estimó que el número de plazas ofertadas podría ser el criterio más significativo respecto del volumen de datos personales tratados. En consecuencia, el Plan se circunscribió a las cadenas hoteleras, dado que una misma cadena aglutina muchos hoteles dispersos por toda la geografía española y la tipología de sus clientes abarca desde profesionales con estancias cortas a familias en periodo vacacional con estancias medianas o largas. Así, se han inspeccionado 4 cadenas hoteleras en las que se han visitado tanto los servicios centrales como los hoteles más representativos de las mismas (en total 15 hoteles), además de centrales de reserva y empresas que prestaban algún servicio a los mismos. A partir de todas las inspecciones citadas y de los resultados obtenidos, se han confeccionado las conclusiones que se recogen en el presente documento.

c. Sagasta 22 28004 Madrid www.agpd.es

Por último debe puntualizarse que el presente informe recoge fundamentalmente aquellos aspectos concretos que son susceptibles de mejoras y que han sido obtenidos de entre todas las entidades auditadas, sin que pueda deducirse ni que alguna de ellas, ni tampoco el sector hotelero inspeccionado en su conjunto, presente un funcionamiento deficiente.

2. DESCRIPCIÓN DEL SECTOR

2.1 Organización de las cadenas hoteleras

Las cadenas hoteleras auditadas se ofertan en el mercado bajo una o varias marcas comerciales cuya titularidad la suele ostentar una sociedad mercantil que, a su vez, suele tener sociedades participadas, configurándose como un grupo integrado de empresas que se dedican a actividades turísticas en general y, más concretamente, a la gestión y explotación de hoteles propios, alquilados, en régimen de gestión o franquicia. De lo anterior se desprende que un hotel perteneciente a una marca hotelera, según la terminología empleada en el sector, se encuentra en alguna de las siguientes situaciones respecto de la sociedad propietaria de la marca comercial:

- *Propiedad o arrendamiento*: son hoteles dirigidos y gestionados en su totalidad por la sociedad titular de la marca comercial.
- *Gestión*: se trata de hoteles en los cuales son dos las sociedades participantes en el negocio. Por una parte la sociedad propietaria de la marca comercial y, por otra, la mercantil propietaria del negocio hotelero con la que se vincula el personal que trabaja en el establecimiento. En este caso se suscribe un contrato entre ambas empresas mediante el cual la mercantil propietaria del negocio contrata con la propietaria de la marca comercial, además de la utilización de su marca y los valores añadidos de publicidad que ello implica, la gestión del negocio. Se ha comprobado que, en algunos casos, la gestión incluye la implantación y utilización del sistema informático y de los ficheros informáticos en los que se tratan los datos personales de los clientes y en otros, el sistema informático y los ficheros automatizados son responsabilidad de la sociedad titular del negocio del hotel, sin que exista vinculación entre los datos de los clientes del hotel y los datos de los clientes de la cadena hotelera.
- *Franquicia:* Este régimen de explotación implica la firma de un contrato de franquicia mediante el cual la sociedad titular de la marca comercial permite o habilita a la sociedad propietaria del negocio del hotel para que utilice su marca. En la mayoría de los casos, la sociedad propietaria del hotel es la que dirige y gestiona el negocio en su totalidad y únicamente se beneficia de los estándares implícitos en la marca comercial así como de los beneficios publicitarios de la cadena hotelera en su conjunto, como miembro de la misma.

2.2 Información tratada por las cadenas hoteleras

Respecto del origen de la información que tratan las distintas entidades, se ha podido comprobar que se recaban datos personales relativos a las personas para las que se reserva una habitación en algún hotel de la cadena. Estos datos personales los puede facilitar una agencia de viajes, una empresa, un organismo oficial o el propio interesado.

Las agencias de viajes, habitualmente, solicitan a la cadena hotelera disponer de un número de habitaciones para ofrecérselas a sus clientes directos. En este caso las agencias no suelen facilitar al hotel datos personales de sus clientes sino que simplemente, reservan una habitación entre las adjudicadas por el hotel y es la agencia de viajes la que recaba los datos de su cliente para formalizar la reserva. En este caso, el cliente facilita sus datos personales a su llegada al hotel.

No ocurre lo mismo cuando la reserva de habitación se realiza por una empresa u organismo oficial desde los que una persona se dirige a la central de reservas de la cadena hotelera o directamente al hotel, para reservar la habitación que ocupará una persona distinta de la solicitante o cuando una agencia reserva directamente la habitación en un hotel. Habitualmente, la central de reservas o el hotel solicitan datos personales tanto de quien reserva la habitación como de la persona que posteriormente se va a alojar en la misma.

Por último, las reservas puede realizarlas directamente el cliente utilizando cualquiera de las vías que las cadenas hoteleras ponen a su disposición y que, en la casi totalidad de los casos son: personándose el cliente directamente en el hotel, a través de las páginas web que publicitan las cadenas hoteleras, por teléfono, e-mail o fax. En todos los casos el cliente debe facilitar, como mínimo, su nombre y apellidos, teléfono de contacto, la duración de la estancia y un número de tarjeta de crédito si el cliente desea garantizar la habitación reservada.

Todas las cadenas hoteleras auditadas cuentan con una central de reservas donde se gestiona la disponibilidad de cada uno de los hoteles de su cadena y se reciben y tramitan las reservas que llegan por cualquiera de los medios disponibles; sin olvidar que todas ellas suelen estar conectadas con sistemas GDS (Global Distribution System) de terceras entidades como Amadeus, Sabre, Galileo y Wordspan de tal forma que permiten a estas últimas realizar transacciones de consulta sobre disponibilidad de habitaciones en los hoteles de la cadena y sus tarifas, además de permitir confirmar, modificar o cancelar reservas, no tratándose en estos casos datos personales.

Los datos personales recabados durante el proceso de gestión de la reserva de habitaciones quedan almacenados en un fichero informático y cuando el cliente acude al hotel en la fecha indicada, durante el proceso de recepción o *check in*, son ampliados con los datos incluidos en el documento nacional de identidad o pasaporte y con la información que se va generando durante la estancia del cliente en el hotel como puede ser el consumo telefónico, restaurante, visionado de películas de pago u otros servicios añadidos. En algunos casos, además de los ficheros informáticos donde almacenan los datos personales relativos a las reservas y a las estancias de los clientes, los hoteles disponen de ficheros automatizados que permiten obtener información

relativa a las llamadas telefónicas realizadas por los clientes desde el número de habitación en la cual se han hospedado, así como información del tipo de películas visualizadas.

Otro servicio que suelen prestar los hoteles pertenecientes a las cadenas hoteleras visitadas es la contratación de sus salones para la celebración de eventos de todo tipo. En estos casos, los datos personales que habitualmente almacenan los hoteles son los relativos a las personas solicitantes de los eventos, no constando información relativa a los asistentes a los mismos.

Una práctica muy extendida en el sector, que permite aumentar la información relativa a sus clientes, es el desarrollo de programas de fidelización propios destinados a sus clientes habituales. Cada uno de los hoteles pertenecientes a una misma cadena hotelera distribuye, en recepción y en cada una de las habitaciones de sus hoteles, folletos informativos del programa incluyendo un formulario de recogida de datos personales que puede cumplimentar el cliente interesado en pertenecer al mismo. Además, todas las cadenas hoteleras suelen incluir la información y el formulario en su página web.

El cliente que desea adherirse al programa y que ha cumplimentado el formulario, posteriormente recibe una tarjeta de fidelización que le identifica ante cada uno de los hoteles de la cadena como cliente fidelizado y le permite acumular puntos por cada estancia en los hoteles, además de obtener ventajas y servicios preferenciales dentro de los hoteles de la cadena o canjear los puntos por estancias gratuitas.

Las cadenas hoteleras, además de los programas de fidelización propios, suelen participar en programas de fidelización patrocinados por otras compañías de transporte aéreo o terrestre. En otros casos, las cadenas hoteleras promocionan junto con una entidad bancaria, la utilización de una tarjeta de crédito de marca compartida. No obstante, el intercambio de información que se realiza como consecuencia de la participación en los programas de fidelización de terceras empresas se traduce, exclusivamente, en la acumulación/utilización de puntos asociados a un número de tarjeta.

Por último, todos los hoteles pertenecientes a la misma cadena hotelera suelen disponer de la misma aplicación informática para gestionar los datos personales de los clientes que se hospedan en su establecimiento, siempre bajo la dirección y coordinación de los servicios centrales que son los que marcan las directrices a seguir por todos. En los servicios centrales de todas ellas reciben información relativa a la facturación realizada por cada uno de sus establecimientos, encontrándose diferencias respecto de la información recibida que, en algunos casos se refiere únicamente a la facturación global sin detallar por clientes, y en otros, la información incluye los datos personales del cliente concreto.

3. CONCLUSIONES RESPECTO DE LA LEY ORGANICA 15/1999 Y NORMATIVA DE DESARROLLO

A continuación, se analiza, desde el punto de vista de la protección de datos, el cumplimiento de cada uno de los principios legales respecto de los tratamientos que realizan las entidades inspeccionadas con los datos personales de sus clientes.

3.1 Calidad de los datos (artículo 4)

El artículo 4 de la LOPD establece que "*los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido"*. A este respecto, de la información recabada de los ficheros informáticos que gestionan los datos personales de los clientes se desprende que los datos tratados son, en general, adecuados, pertinentes y no excesivos en relación con las correspondientes finalidades.

Se ha constatado que la mayoría de las cadenas hoteleras pretenden mantener sistemas de información del tipo *Datawarehouse* especializados en tratamientos complejos y masivos de la información recabada de todos los clientes que se hospedan en cada uno de sus hoteles, lo que permitiría, además de una única identificación del cliente en todos los hoteles de la cadena, la definición de perfiles personales individuales, así como la obtención de datos agregados sobre el comportamiento de sus clientes y sobre las preferencias por determinados servicios disfrutados en los hoteles al objeto de adecuar los servicios y atenciones a dichas preferencias.

Durante las visitas realizadas a los hoteles se ha comprobado que alguna entidad almacena en sus ficheros automatizados información relativa a clientes que no abonaron su factura y que fueron clasificados como morosos, información que persiste en los ficheros sin actualizar en algunos casos y en otros, aunque la tipificación del cliente esta actualizada cuando salda su deuda, los datos del cliente siguen figurando en el fichero como moroso. Esta información es utilizada únicamente por una cadena hotelera que utiliza el modelo denominado como de propiedad no produciéndose cesiones de datos a terceros.

Tras analizar toda la información disponible se ha podido constatar que los datos personales que recaban las cadenas hoteleras relativos a sus clientes desde el momento en que se realiza una reserva de habitación para alojarse en un hotel hasta que el cliente lo abandona, se mantienen tanto en los ficheros a los que accede cada uno de los hoteles como en los servicios centrales.

Se ha comprobado que todas las entidades mantienen en sus ficheros, por tiempo indefinido, información relativa a las personas que han realizado una reserva de habitación en un hotel incluso en aquellos casos en los cuales las reservas se han cancelado.

Por otra parte, todos los datos personales relativos a los clientes que se han hospedado en un hotel, incluyendo los que se recogen durante el *check-in* y los que se generan durante toda la estancia del cliente, se suelen mantener activos en el fichero que habitualmente utiliza el hotel para gestionar su actividad, incluso en el caso de clientes que únicamente se han hospedado en una ocasión en el hotel hace varios años.

Se ha detectado que algunos hoteles disponen de centralitas de teléfonos que automáticamente administran y mantienen un fichero que contiene todas las llamadas telefónicas realizadas por el cliente (nombre y apellidos del cliente, número de teléfono al que ha llamado, día y hora de la llamada así como duración de la misma) comprobándose que se mantiene la información sin cancelar una vez que se ha facturado al cliente por dichas llamadas en el proceso de *check out*. También se ha detectado que algunos hoteles almacenan información relativa al tipo de películas que han visualizado sus clientes, incluyendo día, hora y tipo de película, la cual se sigue manteniendo en el fichero con posterioridad a la facturación que se le realiza al cliente por este servicio. No obstante, se ha constatado que la información detallada a la que se hace referencia en el presente párrafo no se incorpora a la base de datos que gestiona los datos personales de los clientes.

Asimismo, se ha detectado que algunas cadenas hoteleras mantienen información de clientes que han solicitado la baja en los programas de fidelización desarrollados por aquélla. También se ha comprobado que alguna cadena hotelera dispone de información relativa a los solicitantes de tarjetas de crédito de marca compartida que la entidad bancaria participante ha denegado.

Por último, en algunos hoteles que disponen de salones destinados a la celebración de eventos, con aplicaciones informáticas sencillas que les permite gestionar este tipo de actividad, se ha comprobado que suelen mantener información relativa al cliente que ha celebrado el evento durante amplios períodos de tiempo, cuando ha dejado de ser necesaria puesto que el evento se ha celebrado, el cliente ha pagado la factura satisfactoriamente, y ya no mantiene ningún tipo de relación con el hotel.

3.2 Derecho de información en la recogida de los datos (artículo 5)

Según se ha descrito anteriormente, la recogida de datos personales de los clientes que se van a hospedar en una habitación de un hotel se produce principalmente en dos ocasiones: en el momento de realizar una reserva de habitación y en el propio hotel cuando se persona el cliente en el mostrador de recepción para alojarse en la habitación reservada. En el caso de las reservas, teniendo en cuenta los distintos sistemas disponibles para realizarlas, se han constatado las siguientes situaciones:

- Si la reserva se realiza vía internet, a través de los formularios incluidos en las distintas páginas web que publicitan las cadenas hoteleras, la información facilitada suele incorporar el nombre y dirección de la sociedad responsable del fichero en el cual se van a incluir los datos facilitados y la posibilidad de ejercer los derechos de acceso,

rectificación, cancelación u oposición. Sin embargo, no siempre se informa de la finalidad para la que se recaban los datos que se recogen, aspecto especialmente relevante ya que en todos los casos se recaba un número de tarjeta de crédito así como la caducidad de la misma. Asimismo, se ha detectado una entidad perteneciente a un grupo empresarial cuya matriz se encuentra establecida en Estados Unidos, el cual dispone de una página web que permite realizar reservas en el hotel ubicado en territorio nacional y que, aunque tiene información relativa a su política de privacidad, en ningún momento informa al cliente de la identidad y dirección del responsable del fichero donde constan los datos facilitados en el proceso de reserva, ni de la posibilidad de ejercer los derechos que le asisten, así como tampoco de las posibles cesiones a la empresa matriz ubicada en el extranjero. Finalmente, no se suele diferenciar entre campos obligatorios y voluntarios para el suministro de información, considerándose a todos los efectos como obligatorios al no permitir realizar la reserva cuando alguno de ellos queda sin contenido.

- Cuando la reserva se realiza utilizando la vía telefónica, directamente al hotel o a la central de reservas correspondiente, ninguna de las entidades informa a los clientes del destino de los datos personales que se le solicitan y aunque en la mayoría de las ocasiones por ésta vía únicamente se recaba el nombre, apellidos y número de teléfono de contacto así como los datos relativos a las fechas de la reserva, cada vez es más habitual solicitar un número de tarjeta de crédito con su fecha de caducidad.
- Si la vía utilizada es el envío de un e-mail, el destinatario del mismo suele utilizar la misma vía para confirmar o denegar la reserva solicitada. En ambos casos, los datos personales suelen incorporarse a ficheros informáticos de la entidad y, sin embargo, en la mayoría de las ocasiones, cuando el hotel o la central de reservas contesta al solicitante, la respuesta no suele llevar incorporada la correspondiente cláusula informativa que se recoge en el artículo 5 de la LOPD.
- Por último, algunos hoteles disponen de formularios en papel que deben cumplimentar los clientes que solicitan reservar directamente una habitación en el hotel. Estos formularios tampoco suelen llevar incorporada ningún tipo de información relativa al citado artículo de la LOPD.

Otra vía a través de la que se obtienen datos personales es directamente en el mostrador del hotel cuando se produce el *check in* del cliente. En este momento es cuando se solicita del cliente el documento nacional de identidad o pasaporte para completar los datos exigidos en el libro de registro de pasajeros (apellidos y nombre, hijo/a de, y de, nacionalidad, número de DNI o pasaporte, fecha de nacimiento, lugar, domicilio habitual, población, estancia prevista) así como otros complementarios (tarjeta de crédito si el hotel todavía no dispone del número y su caducidad; esta petición del número de tarjeta de crédito y fecha de caducidad suele producirse en algunos casos cuando la reserva de habitación ha sido realizada por un tercero distinto del cliente). En este caso, para poder obtener conclusiones respecto de las exigencias del artículo 5 de la LOPD, resulta necesario analizar cada una de las tipologías de hoteles según el sistema de explotación aplicado a cada uno de ellos en los términos descritos en el

apartado correspondiente a organización de las cadenas hoteleras. Debe destacarse que en los casos en los cuales se facilita información relativa al citado artículo, ésta se realiza en dos idiomas: castellano e inglés.

- *Propiedad incluyendo arrendamiento del inmueble o gestión que comprende los sistemas informáticos:* Si los hoteles son propiedad de la compañía titular de la marca comercial bajo la que se ofertan en el mercado o si han firmado un contrato de gestión que incluye la utilización del sistema informático que trata los datos personales de los clientes alojados en el hotel, se ha comprobado que se producen distintas situaciones: Hoteles que ofrecen al cliente el documento de bienvenida cuando éste se persona en recepción y que no contiene ningún tipo de información que haga referencia al artículo 5 de la LOPD; hoteles que ofrecen un documento conocido en el sector como "*bienvenido"* o contrato de hospedaje que incluye información completa y hoteles que, aunque ofrecen información, ésta resulta insuficiente o incompleta.

  Analizando toda la casuística podemos afirmar que las deficiencias detectadas en el conjunto de las cadenas inspeccionadas consisten bien en recoger como titular del fichero una denominación que no se corresponde con la sociedad que realmente es la responsable del fichero automatizado donde se tratan los datos personales; bien en ofrecer la posibilidad de ejercer los derechos reconocidos en aquél artículo sin informar de la dirección donde ha de dirigirse.

  A lo anterior hay que añadir que respecto de la cesión o envío de publicidad, no se informa sobre la finalidad para la que se van a tratar los datos personales, ni sobre si van a ser cedidos a terceras empresas y para qué finalidades, o si será la que recaba los datos la que enviará publicidad de terceros Por otra parte, en ninguno de los folletos se ha encontrado la opción que permita al cliente marcar una casilla que impida o permita el envío de publicidad o la cesión de sus datos a terceras empresas.

- *Franquicia o gestión excluyendo los sistemas informáticos:* En ambos casos, se ha comprobado que los hoteles facilitan al cliente un documento estándar denominado "*bienvenido"* que utilizan todos los hoteles de la misma cadena hotelera obviando el régimen bajo el que funciona cada uno de ellos. Teniendo en cuenta que este tipo de hoteles únicamente se benefician de las facilidades que les proporciona la utilización de la marca comercial, la información facilitada en el documento está recogiendo como responsable del fichero a una sociedad que no es la que realmente trata los datos personales.

Ya se ha comentado anteriormente que algunos hoteles disponen de ficheros automatizados que les permiten gestionar datos personales de clientes que celebran eventos en sus salones. El hotel suele utilizar formularios de solicitud de información que debe cumplimentar el cliente, siendo posteriormente informatizados los datos del mismo. Estos formularios no suelen incluir ningún tipo de información relativa al artículo 5 de la LOPD aunque en alguno de ellos se incluye una casilla a cumplimentar por el cliente sobre si desea recibir publicidad.

Además de la información citada anteriormente, las cadenas hoteleras recaban datos adicionales de aquellos clientes que solicitan adherirse a los programas de fidelización. Estos datos se recaban a través de formularios en papel o en la propia web de la cadena. A este respecto, se ha comprobado que se suele incorporar una cláusula informativa relativa al artículo 5 de la LOPD con algunas deficiencias como no informar claramente de la finalidad del tratamiento, ni de la dirección del responsable del fichero o de la posibilidad de ejercitar los derechos que le asisten.

Finalmente, los hoteles disponen en sus instalaciones de cuestionarios de calidad que permiten evaluar el nivel de satisfacción de sus clientes respecto de los distintos servicios ofrecidos por el hotel durante su estancia. Todos ellos, además de los ítem relativos a los distintos servicios del hotel, suelen incorporar apartados para recoger los datos personales de los clientes que lo han cumplimentado. No obstante, se ha detectado que las cadenas hoteleras suelen tratar únicamente los datos relativos a la valoración de los servicios a efectos estadísticos, extrayendo conclusiones sobre nivel de calidad ofrecido por cada uno de sus hoteles y excluyendo el tratamiento de los datos relativos a las personas que los han cumplimentado. En algunos casos puntuales, cuando el apartado de observaciones refleja alguna queja o agradecimiento hacía un hotel concreto, los datos personales del clientes son automatizados para emitir una respuesta personalizada al cliente.

La mayoría de las cadenas hoteleras están estudiando la posibilidad de tratar conjuntamente, en un futuro próximo, los datos personales obtenidos de sus clientes durante su estancia en los hoteles de la cadena y todos los datos del cuestionario relativos a la valoración en los distintos ítem realizada por los clientes, al objeto de ofrecerle un mejor servicio y poder realizar estudios con fines de marketing. En este sentido la mayoría de las encuestas, aunque suelen hacer referencia a la confidencialidad de los datos recogidos, no recogen una información acorde al artículo 5 de la LOPD.

Finalmente se ha constatado que una misma entidad utiliza diferentes textos informativos en los distintos documentos donde debe incluirse la información exigida por el artículo 5 de la LOPD.

3.3 Consentimiento del afectado (artículo 6)

El artículo 6 de la ley en su apartado 1 señala textualmente "*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa*".

Además en los siguientes apartados se recoge lo siguiente:

"*2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en*

fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".

En la mayor parte de los casos el tratamiento de los datos de los clientes para la prestación de los servicios se funda en la existencia de una relación negocial amparada por el artículo 6.2 de la LOPD.

Respecto del tratamiento para otras finalidades, dado que utilizan formularios sin incluir la cláusula exigida por el artículo 5 de la LOPD, o si la incluyen ésta resulta ser deficiente, el consentimiento que se obtiene no es un consentimiento informado. Así, se han detectado tratamientos que exceden de la relación contractual como es el caso de los que realizan para extraer relaciones de personas que cumplen años con el fin de remitirles una felicitación los cuales, al no haberse informado previamente, se realizan sin el consentimiento de los afectados.

Además, se ha detectado la realización de perfiles de clientes con fines comerciales a partir de la información personal facilitada por el propio cliente y de la que consta en los ficheros producto de su permanencia en los hoteles de la entidad, sin que se informe de ello a los clientes y, por tanto, sin su consentimiento.

3.4 Datos especialmente protegidos (artículo 7 y 8)

No se ha encontrado evidencia de que en los ficheros automatizados que almacenan datos personales de los clientes de los hoteles auditados en el presente Plan, se traten datos considerados como especialmente protegidos según el artículo 7 de la LOPD (ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual). No obstante, en algunos casos sí se ha detectado que los ficheros utilizados disponen de un campo de observaciones en el que recoge información relativa al cliente que puede ser relevante y que permite una mejor atención por parte del personal del hotel, como facilitar una habitación especial en el caso de personas con alguna minusvalía.

3.5 Seguridad de los datos (artículo 9 y Real Decreto 994/1999 , de 11 de Junio. Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal)

En general, de conformidad con lo que establece el RD 994/1999, todas las cadenas hoteleras inspeccionadas han adoptado medidas de índole técnica y organizativa para garantizar la seguridad de los datos de carácter personal que tratan durante el desarrollo de sus actividades. Las medidas de seguridad adoptadas han sido plasmadas en documentos de seguridad que son de obligado cumplimiento para el personal que necesita acceder a los datos automatizados de carácter personal.

Ahora bien, respecto de los hoteles en régimen de franquicia, se ha detectado que las empresas responsables de los ficheros con datos de carácter personal de sus clientes así como de los tratamientos realizados, aunque hayan implantado algunas medidas de seguridad de las de obligado cumplimiento según el nivel correspondiente, no las recogen en un documento de seguridad.

Asimismo, en relación con los hoteles en régimen de *gestión* que tienen sistemas informáticos propios también se ha detectado que las medidas de seguridad implantadas en los mismos no están recogidas en un documento de seguridad.

En las visitas de inspección realizadas a los hoteles a que se refieren los dos apartados anteriores, se ha podido comprobar que han implantado algunas medida de seguridad como la definición de usuario y contraseña para acceder a los datos personales como mecanismo de autenticación así como la realización de copias de seguridad o definición de distintos perfiles de acceso. No obstante, con carácter general se pueden afirmar que no se encuentran implantadas todas las medidas de seguridad exigidas para el nivel básico.

En cuanto a las cadenas hoteleras que han elaborado el correspondiente documento de seguridad y tienen implantadas medidas de seguridad en todos sus hoteles y servicios centrales, así como en los hoteles en régimen de gestión o franquicia que, aunque no han elaborado el documento de seguridad sí tienen implantadas algunas medidas de seguridad, se ha comprobado la existencia de algunas deficiencias que se expresan a continuación:

1. Respecto de las funciones y obligaciones del personal, habitualmente los responsables de las cadenas hoteleras auditadas suelen redactar decálogos generales que deben cumplir todas las personas que trabajan en la compañía. Sin embargo, no queda reflejada en un documento la función asignada a cada trabajador dentro de la empresa.

   En otras ocasiones, la empresa responsable del fichero ha definido las funciones y obligaciones a cumplir por el personal que trabaja en los departamentos de tecnología y sin embargo, las funciones asignadas a los demás trabajadores no están documentadas.

2. En relación con el registro de incidencias, se ha comprobado que la mayoría de las cadenas hoteleras han definido procedimientos de notificación y gestión de incidencias que incluyen un registro de incidencias. No obstante se ha detectado alguna empresa que no dispone del

citado procedimiento aunque en la práctica utilizan un registro de incidencias que suele carecer de alguno de los apartados relacionados en artículo 10 del Reglamento.

3. Respecto de la identificación y autenticación, se ha constatado que en casi todas las cadenas hoteleras y en particular todos los hoteles, han confeccionado una relación detallada de usuarios que tienen acceso autorizado al sistema de gestión que trata los datos personales de los clientes. Sin embargo se ha comprobado que esta medida no se encuentra implantada en todos los casos.

   En algunos hoteles se he comprobado que es posible acceder a los sistemas informáticos que tratan los datos personales de los clientes sin necesidad de utilizar ningún mecanismo de autenticación.

   Además, en aquellos casos en los cuales el mecanismo de autenticación utilizado se basa en la existencia de contraseñas, se ha podido comprobar que en la mayoría de los hoteles una misma contraseña es compartida por varias personas que además se identifican ante el sistema con el mismo usuario.

   Se ha comprobado que la mayoría de las cadenas hoteleras han definido procedimientos de asignación, distribución y almacenamiento de contraseñas. No obstante en la práctica se ha constatado que algunos establecimientos concretos almacenan las contraseñas sin cifrar, lo cual permite el acceso a las mismas por terceros si no se establece una adecuada política de accesos a la información y, por tanto, no está garantizada su confidencialidad e integridad.

   Finalmente, se ha constatado que en algunos hoteles el responsable de la gestión de contraseñas distribuye éstas a los interesados sin que conste ningún procedimiento estándar en el documento de seguridad que lo prevea.

4. En cuanto al control de acceso, en aquellos casos en los cuales se puede acceder a la información contenida en los ficheros sin utilizar ningún mecanismo de identificación y autenticación, se permite que cualquier usuario acceda a todos los recursos y no únicamente a los datos necesarios para el desarrollo de sus funciones.

5. Respecto de la gestión de soportes, se ha comprobado que algunos hoteles almacenan las copias de seguridad en armarios abiertos ubicados además, en despachos abiertos.

6. En fin, en lo que se refiere a las copias de respaldo y recuperación, aunque la mayoría de los hoteles realizan las mismas con la periodicidad marcada desde los servicios centrales y controlada desde éstos, no en todos los casos se realiza el citado control, detectándose que los dispositivos utilizados para realizar las copias no permiten identificar el tipo de información que contienen.

Con independencia de lo expuesto anteriormente, también se ha detectado que en algunos hoteles los servidores donde residen los ficheros informáticos que contienen los datos personales de los clientes se ubican en espacios abiertos sin ninguna medida de seguridad.

Por último debe mencionarse que el intercambio de información relativa a reservas a través de internet se realiza sin cifrar y, aunque según la tipología de datos personales utilizada el nivel de seguridad aplicado sería acorde con lo dispuesto en el artículo 4 del Reglamento, es preciso insistir en los riesgos que conlleva que se comuniquen a través de un medio como internet datos tales como el número de tarjeta de crédito y su fecha de caducidad, lo que podría permitir el uso de los mismos por terceros no autorizados.

3.6 Deber de secreto (artículo 10)

El artículo 10 de la LOPD hace referencia a la obligación de guardar secreto profesional por parte del responsable del fichero y de todas las personas que intervengan en cualquier fase del tratamiento de los datos personales. Se ha comprobado que las cadenas hoteleras, a la firma del correspondiente contrato de empleo con sus trabajadores, suelen incluir cláusulas de confidencialidad por la que éstos se obligan a guardar el deber de secreto respecto de los datos personales a los que tengan acceso como consecuencia de su trabajo en la entidad. No obstante, esto no se cumple en todos los casos ya que, en algunas ocasiones, únicamente firman las citadas cláusulas aquellos empleados que desempeñan su trabajo directamente en los departamentos de tecnología, sin que se haga extensivo al resto de los empleados que, por las funciones que desempeñan, también acceden a los ficheros informáticos que tratan datos de carácter personal.

3.7 Cesiones de datos y acceso a los datos por cuenta de terceros (artículos 11 y 12)

En el presente apartado se abordan las conclusiones de la inspección en relación con las cesiones de datos y la prestación de servicios por terceros.

El artículo 3. i) de la LOPD establece el concepto de cesión o comunicación de datos definiéndola como “toda revelación de datos a una persona distinta del afectado”.

El régimen jurídico de las cesiones de datos se contempla, básicamente, en los artículos 11 y 12 de la Ley. El primero porque delimita en qué términos son lícitas las cesiones y, el segundo por cuanto que exceptúa jurídicamente que exista una cesión cuando en la prestación de servicios que implican el acceso a la información, se prestan las garantías previstas en dicho precepto.

El artículo 3. d) y g) de la LOPD define las figuras de responsable del fichero o tratamiento y encargado del tratamiento.

El primero de los apartados califica como responsable del fichero o tratamiento a “*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento”*.

El segundo define al encargado del tratamiento como “*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento”*.

La relación entre ambos se configura, esencialmente, en el citado artículo 12 de la LOPD que, bajo la rubrica "*Acceso a los datos por cuenta de terceros"*, establece que "*no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento"*.

A tal efecto, los apartados 1, 2 y 3 del mismo precepto establecen el sistema de garantías cuyo cumplimiento permite considerar que no existe cesión o comunicación de datos en la prestación de servicios y el apartado 4 regula la responsabilidad específica del encargado del tratamiento.

Señalado lo anterior, en la inspección se han constatado las siguientes situaciones:

- Los hoteles de la mayoría de las cadenas hoteleras, forman parte de ellas, si bien a través de la titularidad que ostenta una sociedad independiente participada por la matriz titular de la marca comercial, que es la que realiza la explotación del hotel.

  En este caso no existe un contrato firmado entre ambas sociedades en relación con el tratamiento de datos personales de los clientes.

- En otros hoteles, su propietario suscribe un contrato de gestión con la sociedad titular de la marca comercial que no siempre incluye referencia expresa a la gestión de los datos personales de los clientes. A su vez, en este supuesto la gestión de datos personales de los clientes presenta dos modalidades. Por una parte, los casos en los que la titular del hotel es responsable de los tratamientos facilitando la titular de la marca comercial servicios informáticos y asesoramiento para la gestión de los ficheros y, por otra, los supuestos en los que la encargada de la explotación del hotel pacta que los datos personales de los clientes serán de su exclusiva propiedad.

  En este caso suele existir un contrato firmado entre las sociedades intervinientes. Sin embargo, en ocasiones, dada la antigüedad de los contratos, no se incluyen estipulaciones sobre si los servicios contratados comprenden o no, ni en qué términos, la utilización de ficheros informáticos y datos personales de los clientes.

- Finalmente, en otros hoteles, la relación contractual se articula bajo la modalidad de un contrato de franquicia entre personas jurídicas independientes.

Como se ha señalado en el apartado 4.3, el tratamiento de los datos personales de los clientes se funda, en la mayor parte de los casos, en la existencia de un relación negocial amparada por el artículo 6.2 de la LOPD.

De ello se desprende que, conforme a la definición antes transcrita de responsable del fichero o tratamiento, tendrán esta condición, al menos en lo relativo al alojamiento y la facturación de servicios complementarios, las entidades que sean parte de la relación negocial; es decir, habitualmente, las que ostenten la titularidad del hotel.

Así, en los casos de hoteles de sociedades independientes, aunque estén participadas por la matriz titular de la marca comercial, aquéllas son las que deben ser consideradas como

responsables conforme a la normativa de protección de datos y, si la matriz titular de la marca comercial presta servicios relacionados con la explotación, ha de ser considerada como encargada del tratamiento.

Lo mismo sucederá en los casos en que, siendo una empresa la titular del negocio, su explotación se lleve a cabo a través del régimen que se han denominado como de gestión. Por su parte, las entidades que, en virtud de la relación contractual con el titular del hotel, llevan a cabo la explotación del negocio ostentaran la condición de encargados del tratamiento.

En los casos en que se haya celebrado un contrato de franquicia entre entidades independientes, será responsable del tratamiento la entidad franquiciada, con la que el cliente establece la relación negocial.

En todo caso, en los supuestos a que se refieren los tres párrafos anteriores, el acceso a los datos de los clientes, si se produce en el marco de una prestación de servicios por una tercera entidad, aunque sea la matriz, deberá, para ser lícita, contemplar las garantías exigidas en el artículo 12 de la LOPD.

Por otra parte, se ha constatado que las cadenas hoteleras realizan tratamientos de datos de los clientes con la finalidad de llevar a cabo estudios de mercado, perfiles sobre las preferencias de los clientes, promociones comerciales u otros similares. A tal efecto, se comunican los datos de clientes a las entidades titulares de la marca comercial que son las que efectúan, bajo su propia responsabilidad, los tratamientos descritos. Así sucede tanto cuando esta entidad es propietaria de las sociedades participadas, como en los casos en que la titular de la marca comercial realiza la explotación del negocio a través del régimen conocido como de gestión y, en algunos casos, cuando se suscribe un contrato de franquicia.

En estos supuestos existe una cesión de datos que exige el consentimiento previo e informado del cliente. Según se ha constatado en la inspección, las cláusulas informativas que se facilitan a los clientes no informan con claridad de la cesión ni de las finalidades determinadas para las que tratarán los datos.

Asimismo se producirá una cesión de datos cuando la prestación de servicios no incorpora las garantías del artículo 12 de la LOPD.

Para completar el análisis, a continuación se hace referencia a otras situaciones que se han detectado, principalmente, en los servicios centrales de las cadenas hoteleras:

- En lo que se refiere a las centrales de reservas, en alguna ocasión esta actividad se realiza por una tercera empresa participada por la sociedad titular de la marca comercial. Aunque existe, en algunos casos, un contrato firmado entre ambas empresas, este suele omitir las garantías previstas en el artículo 12 de la LOPD.
- Por otra parte se ha constatado que determinados servicios relacionados con el alojamiento (hosting) de bases de datos o la instalación y mantenimiento de infraestructura informática o tecnológica, entre otras, bien no están formalizadas en contratos escritos, y si lo están, no

recogen las garantías antes citadas. Lo mismo suele suceder en los casos en que las cadenas hoteleras disponen de servicios de consultoría con terceros que permiten el acceso a la información contenida en los sistemas informáticos.

- Respecto de los programas de fidelización vinculados a las cadenas hoteleras, se ha comprobado que suelen intervenir terceras empresas incurriendo en las deficiencias antes descritas. Así, en los programas de fidelización propios o en los que participan las cadenas hoteleras, intervienen terceras empresas en la gestión de las tarjetas emitidas o en la grabación de los datos incorporados en los formularios de adhesión a los programas de fidelización sin adecuarse a las exigencias del artículo 12 de la LOPD.

Finalmente, se ha constatado que todos los hoteles facilitan diariamente a la Comisaría de Policía Nacional o Autonómica a la que pertenecen por su ubicación física, información relativa a los clientes que se han hospedado en sus habitaciones. En la mayoría de las ocasiones los hoteles suelen remitir los listados que extraen de sus sistemas informáticos o bien, un Policía Nacional se persona en el hotel a recoger el listado aunque, también se da el caso de hoteles que no facilitan el citado listado a la Policía y simplemente informan de las estancias cuando personal del Cuerpo solicita información puntual sobre algún cliente del hotel.

Esta cesión trae causa de lo establecido en el artículo 45.1 del Convenio de Schengen, ratificado por España en fecha 23 de julio de 1993. Según este precepto:

"*Las Partes contratantes se comprometen a adoptar las medidas necesarias para garantizar que:*

a) El director de un establecimiento de hospedaje o su encargado procuren que los extranjeros alojados, incluidos los nacionales de las demás Partes contratantes y de otros Estados miembros de las Comunidades Europeas, con excepción de los cónyuges o menores que les acompañen o de los miembros de grupos de viaje, cumplimenten y firmen personalmente las ficha de declaración y que justifiquen su identidad mediante la presentación de un documento de identidad vigente.

b) Las fichas de declaración así cumplimentadas serán conservadas por las autoridades competentes o transmitidas a éstas, siempre que dichas autoridades lo estimen necesario para prevenir peligros, para perseguir delitos o para dilucidar el paradero de personas desaparecidas o víctimas de accidentes, excepto si el Derecho nacional dispusiera otra cosa".

También se encuentra habilitada por el artículo 12 de la Ley Orgánica 1/1992, de 21 de febrero que dispone que "*Las personas naturales o jurídicas que desarrollen actividades relevantes para la seguridad ciudadana, como las de hospedaje, el comercio o la reparación de objetos usados, el alquiler o el desguace de vehículos de motor, o la compraventa de joyas y metales precioso, deberán llevar a cabo las actuaciones de registro documental e información previstas en la normativa vigente".* El desarrollo más reciente de esta previsión legal se encuentra en la Orden INT/1922/2003, de 3 de julio.

3.8 Derecho de las personas: acceso, rectificación, cancelación y oposición (artículos 15 y 16)

Las cadenas hoteleras, en general, informan a los usuarios de la posibilidad de ejercer los derechos recogidos en los artículos 15 y 16 de la LOPD y suelen disponer de procedimientos que permitan cursar las solicitudes recibidas. En este apartado hay que destacar que la mayoría de los procedimientos se limitan a transcribir los artículos 15 y 16 de la LOPD así como la Instrucción 1/1998 de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

Se ha constatado en la mayoría de las cadenas hoteleras que, debido a los distintos tipos de explotación de los hoteles que ostentan una misma marca comercial (propiedad, gestión en sus dos vertientes o franquicia) y dados los términos de la cláusula informativa incluida en los distintos formularios utilizados para recabar datos personales en los hoteles, resulta difícil atender estos derechos ya que el escrito que remite el ciudadano ejerciendo sus derechos se recibe siempre en la sede central de la sociedad propietaria de la marca comercial y los datos se encuentran dispersos en los ficheros de distintos hoteles.

Matizando lo anterior, en el caso de hoteles cuyo responsable es una tercera empresa que no forma parte del grupo empresarial al que pertenece la sociedad titular de la marca comercial (gestión sin incluir el sistema informático o franquicia), la respuesta al ejercicio del derecho de acceso es inviable dado que es imposible acceder a los datos personales incluidos en los ficheros informáticos de estos hoteles.

Cabe destacar que, según manifiestan las entidades visitadas, habitualmente no reciben peticiones ejerciendo los derechos analizados. Por otra parte, ninguna de ellas, en los formularios empleados para la recogida de datos, ha incluido un recuadro que permita a sus clientes manifestarse respecto del derecho de oposición.

3.9 Creación, notificación e inscripción en el Registro General de Protección de Datos (artículos 25 y 26)

A lo largo del plan de inspección sectorial, se han realizado consultas al Registro General de Protección de Datos al objeto de conocer las inscripciones que figuraban de las entidades visitadas comprobándose que, con carácter general, todas ellas habían procedido a la inscripción de sus ficheros de clientes. No obstante en el transcurso de las visitas se conoció la existencia de hoteles en régimen de gestión o franquiciados que disponen de ficheros automatizados de clientes cuyo responsable es una sociedad diferente de la sociedad propietaria de la marca comercial bajo la que operan, comprobándose que existen casos en los que las sociedades responsables de ficheros no habían notificado los mismos en el Registro General de Protección de Datos.

Estas circunstancias dificultan que el Registro General de Protección de Datos pueda cumplir su principal función, que es la de facilitar a los ciudadanos información sobre quien es el responsable del tratamiento de sus datos y dónde poder ejercer sus derechos.

3.10 Movimiento internacional de datos (artículos 33 y 34)

Se ha detectado el caso de un hotel vinculado a una destacada marca comercial de ámbito internacional, propiedad de una sociedad residente en los Estados Unidos de América, que recibe periódicamente los datos personales de todos los clientes hospedados en el hotel ubicado en España.

La sociedad propietaria de la marca comercial bajo la que se conoce el hotel ha firmado un contrato con una sociedad cuya sede se encuentra en un país miembro de la Unión Europea. En base a este contrato, el hotel remite a esta sociedad, vía electrónica, los datos personales de todos los clientes que se han hospedado en el hotel y, posteriormente, esta sociedad remite un cuestionario de calidad al domicilio particular del cliente que fue facilitado por el mismo al hotel durante el proceso de "*check in*", al objeto de valorar los servicios prestados por el hotel.

Se ha constatado que se informa a los clientes de que los datos recogidos en el formulario que se cumplimenta al registrarse en el hotel, será tratados automatizadamente por la sociedad ubicada en USA. Sin embargo, no se informa de que la misma esté ubicada en dicho país.

4. RECOMENDACIONES RESPECTO DE LA LEY ORGANICA 15/1999 Y NORMATIVA DE DESARROLLO

A la vista de las anteriores conclusiones deben formularse las siguientes recomendaciones:

PRIMERA: *CALIDAD DE DATOS*

El artículo 4 de la LOPD establece que "*los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido*".

Según se ha constatado, la información recabada y tratada en los ficheros informáticos que gestionan los datos personales de los clientes es, en general, adecuada, pertinente y no excesiva en relación con las finalidades para las cuales se recaban, que son las de ofrecer servicios relacionados con el alojamiento del cliente en el hotel.

También se ha constatado que algunas cadenas hoteleras pretenden tratar, de forma simultánea y centralizada, todos los datos personales recabados de los clientes durante su estancia en los

distintos hoteles de la cadena mediante la implantación de sistemas de información denominados *datawarehouse*. Dada la potencialidad y eficacia de estos sistemas para poder combinar gran cantidad de información y obtener resultados en poco tiempo, los responsables de las cadenas hoteleras pueden tener una identificación única de cada cliente y elaborar perfiles de los mismos en base a sus gustos, preferencias y servicios solicitados durante su estancia en cada uno de los hoteles con la finalidad de ofrecerles una atención más personalizada en cada hotel de la cadena, atendiendo a sus gustos y preferencias ya conocidas. Por tanto, se recomienda a las cadenas hoteleras que pretendan implantar estos sistemas que sólo realicen este tipo de tratamientos cuando dispongan del consentimiento del titular de los datos.

Algunas entidades almacenan en sus ficheros información sobre el impago de deudas por parte de sus clientes. Dicha información debe ser exacta y puesta al día de forma que responda con veracidad a la situación actual del afectado y refleje con precisión si la deuda ha sido o no saldada. Además tal información será accesible únicamente por los hoteles cuya titularidad se corresponda con el responsable del fichero y no se cederá a terceros aunque utilicen la misma marca comercial salvo que dispongan del consentimiento del interesado.

El artículo 4.5 de la LOPD establece que "*los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados*".

Por otra parte, el artículo 16.3 establece lo siguiente "*la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión*".

Se ha constatado que los datos personales relativos a las reservas canceladas así como los relativos a las reservas que han concluido con la estancia del cliente se mantienen en los ficheros de las entidades. Tales datos deberán cancelarse procediendo, conforme al artículo 16 de la LOPD, a su bloqueo durante el plazo necesario para atender las posibles responsabilidades nacidas del tratamiento, transcurrido el cual deberá procederse a la supresión definitiva.

En este sentido, cuando las entidades mantienen información relativa a clientes, que durante largos períodos de tiempo no han vuelto a solicitar los servicios del hotel o incluso se han hospedado sólo una vez hace varios años, se recomienda la definición de procedimientos internos que permitan determinar los siguientes aspectos:

- Qué datos personales de sus clientes es necesario mantener activos en el fichero de gestión de clientes.
- Los datos personales que se deben almacenar en ficheros históricos a efectos legales como puede ser el caso de datos de facturación o los correspondientes al libro de registro de entrada de viajeros.
- El período de tiempo que debe transcurrir desde la última actualización de los datos personales del cliente antes de proceder a su bloqueo conforme al artículo 16.3 de la

LOPD, debiendo procederse a su supresión una vez que hayan desaparecido las circunstancias que justifiquen el bloqueo de los datos.

En particular, la información de clientes generada con la finalidad de facturar determinados servicios como son los ficheros que contienen datos generados en las centralitas telefónicas o los que contienen información relativa a las películas de video visualizadas por los clientes, sólo podrán utilizarse para la citada finalidad.

Finalmente, deben bloquearse y, en su caso, suprimirse en los mismos términos señalados en el apartado de reservas, los datos personales recabados en las siguientes situaciones:

- Los datos personales de clientes que, perteneciendo a los programas de fidelización patrocinados por las cadenas hoteleras, en un momento determinado solicitan la baja en dichos programas.
- Los datos personales de clientes que celebraron eventos en los salones de los hoteles y que una vez celebrado el evento no mantienen ningún tipo de relación con el hotel.
- Los datos personales que almacenan las cadenas hoteleras relativos a clientes que han solicitado una tarjeta de crédito de marca compartida entre la cadena hotelera y una entidad bancaria y ésta última ha denegado la tarjeta al interesado.

SEGUNDA: *DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS*

El artículo 5.1 de la LOPD establece que "*los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información: b) del carácter obligatorio o facultativo de su respuesta a las preguntas que les son planteadas; c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante*".

Asimismo, el punto 4 del mismo artículo establece que: "*cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del artículo 5.1.*"

Por tanto se deberá informar de lo establecido en el artículo 5.1 a todos los clientes con carácter previo a la recogida de sus datos, con independencia del procedimiento utilizado para recabarlos, ya sea a través de llamada telefónica, e-mail, formularios, Internet o cualquier otra. No obstante, se dan circunstancias en las que el medio utilizado pudiera hacer imposible o exigir

esfuerzos desproporcionados para facilitar la información previamente a la obtención de los datos. En tales casos, y según lo establecido en el artículo 5.5, la empresa responsable podría solicitar a la Agencia Española de Protección de Datos la exención de la obligación de información, adoptando otras medidas compensatorias.

En todos los casos en los cuales se utiliza un formulario para recabar datos de los clientes, en soporte papel o electrónico, además de información relativa al responsable real del fichero y a su dirección, debe incluirse información relativa a la finalidad para la cual se recaban los datos, al destinatario de los mismos, a las consecuencias de la negativa a suministrar determinados datos, a la posibilidad de ejercitar los derechos de acceso, cancelación, rectificación y oposición y a las cesiones a terceras empresas incluyendo la cesión a los Cuerpos y Fuerzas de Seguridad del Estado, así como diferenciar los campos obligatorios de los voluntarios incluyendo una casilla que permita al usuario manifestarse sobre la cesión de sus datos, sobre la recepción de publicidad u oponerse a la realización de tratamientos destinados a elaborar perfiles en base a sus preferencias.

También se recomienda la revisión de todos los formularios de recogida de datos personales (solicitudes de celebración de eventos, formularios de adhesión a programas de fidelización, cuestionarios de calidad, etc.), con independencia de la finalidad para la cual se recaban, y adecuen las cláusulas impresas al objeto de adaptarlas a lo estipulado en el mencionado artículo.

Asimismo, durante las actuaciones de inspección desarrolladas en las cadenas hoteleras se ha comprobado que en los formularios utilizados para recabar datos personales que incluyen información relativa al artículo 5 de la LOPD, la misma esta escrita tanto en castellano como en inglés. En esta línea, se considera una buena práctica que, con carácter general, toda la información facilitada a los clientes a través de los distintos medios utilizados para recoger datos personales fuese redactada, al menos, en los citados idiomas.

Finalmente, deberá establecerse un sistema que permita homogeneizar la información facilitada por las entidades a sus clientes a través de los distintos medios de recogida utilizados ya que la información relativa al artículo 5 de la LOPD debe ser la misma en todos ellos.

TERCERA: *CONSENTIMIENTO DEL AFECTADO*

El artículo 6 de la LOPD dice textualmente "*el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".*

Las empresas deberán adoptar las medidas necesarias para recabar el consentimiento de sus clientes y evitar los tratamientos o cesiones de datos de los que no se hubiese informado a cada afectado. En aquellos casos en los que los hoteles han recabado datos facilitando información deficiente o los mismos sean utilizados para finalidades diferentes a las que han sido consentidas por el cliente o legalmente autorizadas, se deberá cesar en dichos tratamientos hasta que no se disponga del correspondiente consentimiento.

En particular, el tratamiento de los datos para la realización de segmentaciones o perfiles personales con fines comerciales constituye un tratamiento ajeno a la relación negocial con el cliente. Por ello será preciso suministrar una información sobre esta finalidad y obtener un consentimiento específico al efecto. Asimismo, debe tener la posibilidad de oponerse a tales tratamientos en el momento de recogida de la información, por ejemplo, mediante la marcación de una casilla.

CUARTA: *DATOS ESPECIALMENTE PROTEGIDOS*

El artículo 7 dispone lo siguiente en sus distintos apartados:

> "*1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.*
>
> *Cuando en relación con estos datos se proceda a recabar el consentimiento a que hace referencia el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.*
>
> *2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias...*
>
> *3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.*
>
> *4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual".*

Por tanto, en aquellos casos en los cuales se trate este tipo de información en los ficheros de los hoteles, como puede ser el caso de datos relativos a minusvalías, deberá solicitarse el consentimiento expreso del cliente al que haga referencia.

Finalmente, aunque durante las actuaciones inspectoras realizadas en los hoteles no se ha constatado que los mismos recaben datos considerados especialmente protegidos sobre ideología, afiliación sindical, religión y creencias se advierte que, en el caso de que se celebren eventos o se utilicen servicios que permitan asociar información de aquella naturaleza a personas físicas, el hotel debería recabar el consentimiento expreso y por escrito del cliente cuyos datos van a ser tratados.

QUINTA: *SEGURIDAD DE LOS DATOS*

El artículo 9 de la LOPD textualmente recoge en sus distintos apartados lo siguiente:

> *"1. El responsable del fichero y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*
>
> *2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas."*.

El artículo 8 del Reglamento de Medidas de Seguridad de los ficheros que contengan datos de carácter personal hace referencia al Documento de Seguridad estableciendo, en su apartado 1 que "*el responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información"*.

Durante las actuaciones inspectoras se ha comprobado que todas las cadenas hoteleras inspeccionadas han adoptado medidas de seguridad de índole técnica y organizativa, tanto para los servicios centrales como en los hoteles que tienen implantados los sistemas informáticos proporcionados por dichos servicios, las cuales han sido plasmadas en documentos de seguridad. No obstante, las empresas responsables de hoteles en régimen de franquicia o gestión con sistemas de información propios, aunque hayan implantado algunas medidas de seguridad, no disponen del documento de seguridad por lo que, deberán elaborarlo e implantarlo en su organización, teniendo el cuenta que el mismo deberá contener como mínimo lo siguiente:

1. Ambito de aplicación.
2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
3. Funciones y obligaciones del personal.
4. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
5. Procedimientos de notificación, gestión y respuesta ante las incidencias.
6. Procedimientos de realización de copias de respaldo y de recuperación de los datos.

Los sistemas *Datawarehouse* permiten aglutinar y tratar de un modo sencillo una amplia y completa información relativa a los clientes de las cadenas hoteleras la cual ha sido recogida previamente mediante el empleo de diferentes sistemas de información. Uno de los tratamientos que estos sistemas permiten realizar de un modo relativamente sencillo es la elaboración de perfiles de sus clientes. El artículo 4 del Reglamento de Medidas de Seguridad establece que cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que

permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de seguridad de nivel medio.

Por tanto, las cadenas hoteleras que dispongan, a fecha de dictarse las presentes recomendaciones, de un sistema *Datawarehouse* o que tengan prevista su inmediata creación, deberán implantar, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, a menos que tuviesen que implantar medidas de nivel alto.

Ya se ha comentado que los hoteles franquiciados o en régimen de gestión con sistemas de información propios, aunque no disponen de documento de seguridad, sí han implantado algunas medidas de seguridad. Por su parte, las cadenas hoteleras que han elaborado el correspondiente documento de seguridad, también las han implantado en sus establecimientos.

Ahora bien, en estos casos, se ha comprobado la existencia de algunas deficiencias por lo que, se recomienda a todas las cadenas hoteleras y a los hoteles, en particular, la revisión del documento de seguridad y de las medidas de seguridad implantadas, al objeto de que se adecuen a los distintos artículos del Reglamento debiendo, específicamente, considerar los siguientes aspectos:

1. Definir claramente las funciones y obligaciones de las personas con acceso a los datos de carácter personal y a los sistemas de información, incluyendo las que acceden desde los puestos de trabajo ubicados en cada uno de los hoteles de la compañía, de tal forma que cada usuario acceda únicamente a aquellos datos y recursos que precise para realizar la función encomendada.

2. Confeccionar una relación actualizada de usuarios que tengan acceso autorizado al sistema de información, la cual debe corresponder con la situación real. Asimismo deberán establecerse procedimientos de identificación y autenticación para cada acceso que se realice al sistema de información.

   Por otra parte, cuando el mecanismo de autenticación se base en la existencia de contraseñas, el procedimiento de asignación, distribución y almacenamiento debe garantizar su confidencialidad e integridad, de tal forma que cada usuario y contraseña sean únicos por persona.

3. Establecer mecanismos que impidan a los usuarios acceder a información no necesaria.

4. Definir por escrito procedimientos de notificación y gestión de incidencias así como adecuar el registro de incidencias incluyendo en todo caso el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

5. Establecer un procedimiento que verifique la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos, especialmente, en los casos en los que las copias de seguridad son realizadas en los hoteles

por personal no cualificado técnicamente de forma que se garantice, en caso de pérdida o destrucción de información, la reconstrucción de la misma al estado anterior.

6. Los soportes informáticos que contengan datos personales deberán almacenarse en un lugar con acceso restringido al personal autorizado a tal efecto en el documento de seguridad.

Por su parte, las cadenas hoteleras que dispongan o tengan previsto utilizar un sistema *Datawarehouse,* al ser exigibles adicionalmente medidas de seguridad de nivel medio, deberán tener en cuenta lo siguiente:

1. La cadena hotelera deberá nombrar uno o varios responsables de seguridad.
2. Los sistemas de información e instalaciones de tratamiento de datos deberán someterse a una auditoria, interna o externa, que verifique el cumplimiento del Reglamento de Medidas de Seguridad y de los procedimientos e instrucciones vigentes en materia de seguridad de datos. Esta auditoria deberá realizarse al menos cada dos años.
3. Las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.
4. Se deberán tomar medidas respecto de los soportes que vayan a desecharse o reutilizarse.

Además, sería recomendable la adopción de medidas que eviten que el intercambio de información relativa a las reservas que se comunican a través de Internet se realice de forma ininteligible de tal forma que impida la captura o manipulación por terceros.

En lo que se refiere a la aplicación de las medidas de seguridad exigidas por el Reglamento ciado debe formularse una aclaración adicional, de carácter general.

El artículo 1 del Reglamento delimita su ámbito de aplicación estableciendo que será aplicable únicamente a los ficheros automatizados. Esta delimitación resultaba congruente con el sistema de garantías contemplado en la Ley Orgánica 5/1992, de 29 de octubre (LORTAD), en cuyo desarrollo fue aprobado, y que sólo era de aplicación a ficheros automatizados.

La vigente LOPD presenta como una de sus principales novedades la ampliación de su ámbito de aplicación que ahora alcanza “los datos de carácter personal registrados en soporte físico que los hace susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos...” (art. 2). Incluye, por tanto, los datos en soporte papel siempre que esten estructurados como ficheros.

La Disposición Transitoria Tercera de la LOPD mantiene la vigencia de las normas reglamentarias preexistentes, entre las que se cita el Reglamento de Medidas de Seguridad, en cuanto no se oponga a la nueva Ley.

La previsión del Reglamento de aplicarse sólo a los ficheros automatizados se opone a la vigente LOPD, al haberse ampliado su ámbito de aplicación, como se ha expuesto, por lo que debe considerarse derogada.

En consecuencia, desde la entrada en vigor de la LOPD, resulta aplicable dicho Reglamento a los ficheros en soporte no automatizado que se hubieran creado con posterioridad a la entrada en vigor de la Ley Orgánica, el 14 de enero de 2000. Los ficheros en soportes no automatizados que existieran antes de dicha fecha dispondrán, a estos efectos, del período de adaptación establecido en la Disposición Adicional Primera (que finaliza en octubre de 2007).

No obstante, cuando resulte de aplicación el Reglamento de Medidas de Seguridad, conforme a los criterios expuestos, sólo deberán implantarse las medidas de seguridad que, pese a estar previstas para tratamientos automatizados, por su naturaleza sean también aplicables a ficheros no automatizados como, por ejemplo, la elaboración e implantación del Documento de Seguridad.

***SEXTA:** DEBER DE SECRETO*

El artículo 10 dispone que "*el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*".

En este sentido, se considera una buena práctica que las empresas incluyan anexos a todos los contratos de trabajo en los que quede reflejo del secreto profesional al que están obligados todos los trabajadores que tienen acceso a los datos de carácter personal en el desarrollo de su puesto de trabajo. La empresa debería hacer extensiva esta práctica a todos los empleados de las entidades prestatarias de servicios que tengan acceso a los datos personales de los clientes.

***SEPTIMA:** ACCESO A LOS DATOS POR CUENTA DE TERCEROS Y CESIONES DE DATOS*

En el apartado 3.6 de las conclusiones se han expuesto las previsiones de la LOPD sobre las definiciones de responsable del fichero y encargado del tratamiento. También se ha descrito cómo el acceso a la información por parte de un tercero puede constituir una cesión de datos o estar amparada en una prestación de servicios con las garantías de su artículo 12.

Asimismo, se han detallado para las distintas modalidades de gestión de los hoteles, quien obstenta la condición de responsable del fichero y qué entidad puede tener la consideración de encargada del tratamiento de datos al prestar servicios a aquel.

Partiendo de aquella descripción corresponde ahora señalar en qué condiciones permite la LOPD el tratamiento de los datos.

Cuando exista una relación entre el responsable del fichero que requiere un servicio y el encargado del tratamiento, que lo presta, conforme al artículo 12 de la LOPD es necesario que se establezcan las siguientes garantías:

1. La prestación del servicio concreto deberá formalizarse en un contrato escrito en el que se recoja expresamente que la entidad que va a prestar el servicio únicamente tratará los datos personales conforme a las instrucciones del responsable del tratamiento, que no los va a utilizar para otra finalidad diferente de la que figura en contrato y que tampoco los va a ceder a una tercera empresa ni siquiera para su custodia.

   Además de lo anterior, el contrato deberá recoger las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar.

2. La empresa prestadora del servicio, una vez extinguida la relación contractual, deberá destruir los datos o devolverlos a su responsable, así como todos los soportes o documentos en los que conste algún dato de carácter personal.

La misma recomendación se hace extensiva a otras situaciones en las que intervienen terceras empresas y que se han reflejado en el documento de conclusiones como son: la actividad que desarrollan las centrales de reservas, los servicios relacionados con el alojamiento de bases de datos, las consultorías realizadas por terceras empresas y los programas de fidelización en los que también intervienen terceros. Asimismo, cualquier otra actividad encargada a un tercero (aunque no haya sido detectada durante las actuaciones inspectoras) que pueda enmarcarse en el ámbito de una prestación de servicios, deberá observar la misma recomendación.

En consecuencia las cadenas hoteleras deberán revisar los contratos en vigor para incorporar las garantías exigidas por el artículo 12 de la LOPD a riesgo de incurrir, en caso contrario, en una posible cesión ilícita de los datos por parte del responsable del fichero y en un tratamiento de los datos personales, también ilícito, por parte del destinatario de los datos.

Del mismo modo deberán incluir aquellas garantías en los contratos que suscriban en el futuro, para la prestación de servicios que implique un acceso a datos personales.

Además, a los efectos expuestos y con el fin de facilitar e identificar claramente las garantías que se establecen en los casos de prestación de servicios, se considera una buena práctica la cita expresa en los contratos del artículo 12 de la LOPD.

Sin embargo, en el apartado de conclusiones, se han constatado situaciones en las que el acceso a la información no forma parte de la prestación de un servicio, sino que supone una autentica cesión o comunicación de datos personales. Así sucede, muy especialmente, en los tratamientos de datos de clientes que realizan las cadenas hoteleras bajo su propia responsabilidad con la finalidad de llevar a cabo estudios de mercado, perfiles sobre sus preferencias, promociones comerciales u otros similares.

En estos supuestos la comunicación de los datos de clientes y el tratamiento lícito de los mismos exige un consentimiento previo e informado del cliente, sin que pueda ampararse en las garantías del artículo 12 de la LOPD ya expuestas, aún cuando hubiera un contrato que cumpliera lo dispuesto en el citado artículo.

Esta exigencia del consentimiento previo e informado se encuentra recogida en el artículo 11 de la LOPD que establece que *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"*.

Además, conforme al artículo transcrito, los datos cedidos sólo podrán tratarse para las finalidades determinadas, explícitas y legitimas sobre las que se informó en el momento de obtener el consentimiento del cliente que, en todo caso, es revocable. Por ello se recomienda adecuar todos los formularios de recogida de datos personales, con independencia del método empleado para su recogida (papel, Internet, etc.), al objeto de incluir cláusulas informativas que permitan a los interesados consentir las cesiones detectadas e incluir un procedimiento para que el cliente pueda negar o revocar su consentimiento.

OCTAVA: *DERECHO DE LAS PERSONAS: ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICION*

El Título III de la LOPD bajo la rúbrica *"derechos de las personas"* reconoce en el artículo 15 el derecho de acceso y en el artículo 16 los de rectificación y cancelación. Por su parte, los artículo 6.4 y 30.4 hacen referencia al derecho de oposición. En cuanto a su ejercicio, el artículo 17 remite la regulación de los procedimientos al desarrollo reglamentario.

Las entidades que disponen de procedimientos definidos para resolver y atender los derechos de acceso, rectificación, cancelación y oposición deberán revisarlos de tal forma que permita resolver solicitudes realizadas por cualquier persona con independencia del hotel en el que se haya alojado o haya realizado una reserva conforme a la LOPD y a la Instrucción 1/998, de 19 de enero.

En los casos en los cuales el responsable del hotel, al disponer de ficheros propios, no comparte los datos personales de sus clientes con la matriz titular de la marca comercial, deberá definir los procedimientos que permitan resolver en plazo las solicitudes que dirijan los clientes a sus propias dependencias o a aquella ubicación que le indique el responsable del fichero en caso de prever otra dirección distinta de aquellas donde se ubican sus dependencias, también conforme a la citada Instrucción.

En relación con estos derechos debe destacarse como importante novedad que la vigente LOPD incorpora, trasponiendo la Directiva 95/46/CE, entre los derechos de las personas, el derecho de oposición junto a los derechos de acceso, rectificación y cancelación ya previstos en la hoy derogada L.O. 5/1992, de 29 de octubre.

Como se ha señalado, el artículo 17 de la Ley remite al desarrollo reglamentario los procedimientos para el ejercicio de dicho derecho.

La cuestión que se plantea, por tanto, atendiendo al tenor de la LOPD respecto al derecho de oposición y a la normativa preexistente declarada en vigor por la Disposición Transitoria

Tercera de la LOPD es la de si, interpretadas sistemáticamente, cabe concluir que el ejercicio del derecho de oposición puede integrarse en el desarrollo reglamentario que la Ley Orgánica declara subsistente. En este sentido se plantean, al menos, tres cuestiones básicas.

En primer lugar la relativa a la naturaleza de dicho derecho y a las condiciones para su ejercicio.

A este respecto no cabe duda de que estamos en presencia de un derecho personalísimo (art. 11 del Real Decreto 1332/1994, de 20 de junio) que se ejercerá independientemente de los restantes derechos reconocidos en la LOPD por su titular – excepto en los supuestos limitados en los que cabe la representación -, el cual deberá acreditar su identidad (art. 11 del Real Decreto citado y Norma Primera de la Instrucción 1/1998, de 19 de enero, de la AEPD), sin que quepa exigir contraprestación alguna por su ejercicio (art. 11 citado).

En segundo lugar la que afecta a los plazos para resolver sobre la petición de oposición al tratamiento de datos y a la necesidad de contestar a las solicitudes a través de las cuales se ejerza el derecho.

En este sentido cabe reseñar que el articulo 17 de la LOPD, que remite al desarrollo reglamentario el ejercicio de los derechos, distingue entre los relacionados con los derechos de acceso y oposición y los de rectificación y cancelación como se desprende de la expresión " ..así como.." que viene a diferenciar dos bloques distintos entre unos y otros, excepto en lo que sean de aplicación las normas comunes a todos ellos. En esta línea, parece que el plazo para atender el derecho de oposición deberá ser el de un mes, que coincide con el previsto para el derecho de acceso y se diferencia del plazo para hacer efectivo los derechos de rectificación y cancelación.

Ha de señalarse que una interpretación contraria no sería conforme con la Directiva 95/46/CE por cuanto que implicaría la inexistencia de un plazo para el ejercicio del nuevo derecho de oposición que la norma comunitaria obliga a incorporar y proteger en el derecho interno, con la consecuencia de que la LOPD no habría transpuesto dicha Directiva al no contemplar plazo para su satisfacción, quedando impune la falta de respuesta frente a su ejercicio. Y, no debe olvidarse, a este respecto, que la voluntad expresa del legislador al aprobar una nueva LOPD y derogar la L. O. 5/1992, ha sido la de trasponer aquella Directiva.

De ahí que, tanto la obligación asumida por el legislador de incorporar a nuestro derecho la Directiva Comunitaria, como una interpretación en pro del contenido esencial del derecho fundamental a la protección de datos (SS. del T.C 290 y 292/2000, de 30 de noviembre) permitan interpretar la literalidad del artículo 17 en los términos expuestos.

Quedaran a salvo, lógicamente, los desarrollos reglamentarios del derecho de acceso que resultan incompatibles con el contenido propio del derecho de oposición, pero no los relativos al plazo en que debe ser atendido.

En tercer lugar ha de atenderse a los aspectos procedimentales relativos a la posibilidad de que el derecho de oposición sea objeto de reclamación ante la APD (art. 18 LOPD) y a la tramitación de las reclamaciones que se planteen.

En este punto no cabe duda de que el articulo 18 de la LOPD establece una regla general relativa a la tutela de todos los derechos consistente en que cualquier actuación contraria podrá ser objeto de reclamación ante la Agencia (apartado 1), y que, aquél al que se deniegue total o parcialmente su ejercicio podrá ponerlo en conocimiento de ésta con la obligación, por parte de la autoridad de control, de asegurarse de la procedencia o improcedencia de la denegación; dictando resolución en el plazo máximo de seis meses (apartado 2.)

Y, tampoco cabe duda de que serán aplicables las disposiciones generales relativas a la tutela de derechos – en particular el articulo 17 del Real Decreto 1332/1994 citado - y los requisitos generales que para su ejercicio contempla la Norma Primera de la Instrucción 1/1998, de 19 de enero, entre los que se incluye, entre otros, la obligación del responsable del fichero de "contestar a la solicitud que se dirija, con independencia de que figuren o no los datos del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción " (apartado 4).

Por último, dado que en este caso todas las entidades auditadas tienen naturaleza jurídica-privada, debe señalarse que el plazo de 10 días previsto en el artículo 16 de la LOPD para hacer efectivo el derecho de rectificación o cancelación deberá computarse por días naturales y no por días hábiles.

NOVENA: *CREACIÓN, NOTIFICACIÓN E INSCRIPCIÓN EN EL REGISTRO GENERAL DE PROTECCION DE DATOS*

El artículo 26 de la LOPD recoge que "*Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos"*.

Dadas las diversas modalidades de gestión utilizadas por las cadenas hoteleras es preciso aclarar que la obligación de notificar ficheros o tratamientos al Registro General de Protección de Datos corresponde a las entidades que sean responsables de los ficheros. Por el contrario, los meros encargados del tratamientos que prestan servicios a aquellos no tienen obligación de notificar al citado Registro los tratamientos de datos personales realizados en el marco de aquella prestación.

En este sentido, dado que se ha detectado la existencia de hoteles franquiciados o con un contrato de gestión con la sociedad propietaria de la marca comercial que no incluye el uso de los ficheros automatizados y que disponen de ficheros informáticos propios para tratar los datos personales de sus clientes, al ser responsables de los mismos, deberán notificarlos a la Agencia Española de Protección de Datos, incluyendo la finalidad del fichero, ubicación física del

mismo, descripción de la tipología de datos de carácter personal que contiene, el nivel adoptado en base a la tipología de datos tratados, cesiones de datos que se produzcan o que se prevean realizar así como si se van a producir transferencias internacionales de datos a terceros países.

La solicitud de inscripción de ficheros se deberá efectuar mediante los modelos establecidos en la Resolución de la Agencia Española de Protección de Datos, de 30 de mayo de 2000 (B.O.E. nº 153, 27 de junio de 2000), por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el RGPD. Estos modelos se pueden obtener a través de Internet en nuestra página Web www.agpd.es.

Finalmente, debe resaltarse que tanto la solicitud de inscripción de ficheros en el RGPD como la notificación posterior de inscripción, son gratuitos.

DECIMA: *MOVIMIENTO INTERNACIONAL DE DATOS*

Los artículos 33 y 34 de la LOPD establecen el régimen al que habrán de someterse los movimientos internacionales de datos.

El artículo 33 de la LOPD establece que "*No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos*".

Por tanto, con carácter general, habrá de estarse a lo dispuesto en el artículo 33 de la Ley. No obstante, el artículo 34 establece las excepciones a la norma general, concretamente en los apartados e), f) y g) se establece expresamente lo siguiente:

> *"e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista".*
>
> *"f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado".*
>
> *"g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero".*

Por tanto, dado que la relación contractual para la prestación de los servicios de alojamiento países sólo podrá ampararse en el artículo 34 cuando concurra la excepción del apartado f). En otro caso, si la transferencia se va a realizar para que la empresa matriz remita un cuestionario de calidad, deberá solicitarse consentimiento informado del cliente.

En todo caso, si la transferencia se ampara en una excepción prevista en el citado artículo 34, deberán notificar la inscripción del fichero, cumplimentando el apartado de Transferencias Internacionales y justificar los supuestos consignados en la declaración con el fin de constatar que efectivamente concurren las circunstancias alegadas.

Si la transferencia no se fundamenta en alguno de los supuestos a los que se refiere el artículo 34 de la LOPD, deben distinguirse dos situaciones atendiendo al país de destino de los datos.

En los casos en que los países de destino dispongan de un nivel adecuado de protección de los datos personales, no será precisa la autorización del Director de la Agencia ni la concurrencia de ninguna de las excepciones señaladas respecto de la transferencia internacional, sin perjuicio de respetar el resto de los requisitos legales previstos para el tratamiento de los datos. Se consideran países que proporcionan un nivel de protección adecuado, los Estados Miembros de la Unión Europea o un estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado, estando incluidos, hasta la fecha, entre estos últimos, Suiza, la República Argentina, Canadá respecto de las entidades canadienses de ámbito federal, Guernsey y la Isla de Man.

En cuanto a los Estados Unidos de Norteamérica, aunque el país no proporciona y nivel de protección equiparable, sí lo ofrecerán las entidades estadounidenses adheridas a los "*principios de puerto seguro*" en cuyo caso, serán aplicables los mismos criterios que se han expuesto.

En los restantes países, si no concurre ninguna de las excepciones establecidas en el artículo 34, deberá recabarse la autorización del Director de la Agencia Española de Protección de Datos, en cumplimiento del artículo 33 de la LOPD. Dicha autorización será otorgada en caso de que el responsable del fichero aporte un contrato celebrado o a celebrar entre el transmitente y el destinatario, en el que consten las garantías necesarias, en los términos previstos en las Decisiones de la Comisión 2001/497/CE o 2002/16/CE de las Comunidades Europeas, de 15 de junio de 2001 y de 27 de diciembre de 2001, respectivamente, relativas a las cláusulas contractuales tipo para la transferencia internacional de datos personales a un tercer país y a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE.

Madrid a 25 de junio de 2004