



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

RECOMENDACIONES DE LA AGENCIA DE PROTECCIÓN DE DATOS EN RELACIÓN CON LA GESTIÓN DE TARJETAS UTILIZADAS EN LAS GRANDES SUPERFICIES COMERCIALES PARA LA ADECUACION DE SU FUNCIONAMIENTO A LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Por acuerdo del Director de la Agencia de Protección de Datos (APD), se procedió durante el año 2000 a realizar un Plan de Inspección de oficio al Sector de Grandes Superficies Comerciales con objeto de determinar los procedimientos y tratamientos que aplican sobre los datos de sus clientes, en relación con las tarjetas de pago y fidelización que emiten, así como en la utilización como medio de pago de otras tarjetas externas, y verificar su adecuación a las prescripciones de la legalidad vigente sobre protección de datos de carácter personal, Ley 15/1999, de 13 de diciembre (L.O.P.D.) y normativa que la desarrolla, así como coadyuvar al conocimiento de la misma, a cuyo efecto dicho Plan Sectorial culmina con el dictado de las pertinentes Recomendaciones en las que se recogen los criterios que han de seguir las entidades inspeccionadas para el mejor cumplimiento de la Ley.

A tal efecto, y en desarrollo del Plan se han inspeccionado durante el último cuatrimestre del año 2000 tres Grandes Superficies Comerciales, aunque también ha sido necesario inspeccionar a los respectivos Establecimientos Financieros de Crédito, con los que cada uno de los centros tiene suscritos contratos para la emisión de tarjetas financieras específicas con las que se puede operar en los mencionados centros, toda vez que estos establecimientos financieros son igualmente responsables de los ficheros en los que también se recogen y tratan los datos de los clientes.

1. CONCLUSIONES DE LA INSPECCIÓN

De las actuaciones efectuadas por la Inspección de Datos en las tres Grandes Superficies Comerciales investigadas, así como del análisis de la documentación recabada en las mismas y normativa vigente en materia de protección de datos, se desprenden las conclusiones que se exponen a continuación, distinguiendo, a efectos de su mejor sistemática, los tres tipos de ficheros inspeccionados:

- *Ficheros de Tarjetas de pago de grandes superficies comerciales:*
Contienen los datos de los solicitantes y titulares de tarjetas emitidas por los establecimientos financieros de crédito bajo la marca del centro



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

comercial correspondiente, con las cuales se pueden abonar las compras y solicitar financiación de las mismas en cada uno de los centros comerciales inspeccionados.

- *Ficheros de otras Tarjetas de pago*: Contienen los datos derivados o relacionados con las operaciones que efectúen los clientes utilizando otras tarjetas distintas de las anteriores, emitidas por entidades financieras y que permiten comprar y pagar con ellas en la generalidad de los establecimientos.
- *Ficheros de fidelización de clientes*: Contienen los datos de aquellos clientes que son socios de los Clubes de fidelización promovidos por los propios centros comerciales.

1.1- Ficheros de Tarjetas de pago de grandes superficies comerciales

Cada una de las grandes superficies comerciales tiene establecida una relación contractual con los correspondientes establecimientos financieros de crédito por la que se vinculan al sistema de pago de la tarjeta, de manera que dichas tarjetas sean admitidas como medio de pago en todos sus centros, pudiendo también solicitar los clientes financiación sobre las compras que realicen.

Los datos de las solicitudes de tarjetas y de los titulares de las mismas se recogen en ficheros automatizados, los cuales se encuentran inscritos en el Registro General de Protección de Datos. Los responsables de estos ficheros son los establecimientos financieros de crédito como entidades emisoras de estas tarjetas.

- Recogida de los datos de solicitud de Tarjetas

Los datos son recogidos habitualmente a través de formularios de solicitud que cumplimenta directamente el propio interesado o el personal del centro comercial, debiendo ser suscritos con su firma por el interesado para que tengan validez. Entre los datos recabados se encuentran los siguientes:

Identificativos y de domicilio: Número de DNI, nombre y apellidos, fecha de nacimiento, sexo, nacionalidad, domicilio y número de teléfono.

Situación familiar: estado civil, número de hijos o personas a su cargo, régimen económico del matrimonio.



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

Profesionales: nombre de la empresa, domicilio, cargo, número de teléfono, antigüedad en el puesto y situación (fijo, eventual o pensionista).

Económicos: Ingresos mensuales, situación de la vivienda habitual (en alquiler, en propiedad, con padres, en hotel), otros ingresos y datos bancarios.

Algunas entidades también solicitan documentación acreditativa de la situación económica del interesado, como su última nómina y el documento que acredite el mantenimiento de una cuenta bancaria en la que domiciliará los pagos de los recibos.

En algunas ocasiones, el personal del centro comercial recaba los datos directamente del solicitante cumplimentando un formulario de uso interno que no se facilita al cliente.

- Derecho de información y consentimiento de los afectados

En los formularios de solicitud y contratos de Tarjeta se informa de la inclusión de los datos personales aportados por el afectado en un fichero automatizado cuyo responsable es el establecimiento financiero, así como de la inclusión en un fichero cuyo responsable es el centro comercial, si éste no pertenece al grupo de empresas del establecimiento financiero. También se informa de la finalidad de la recogida de los datos (gestión y registro de las operaciones que el Titular efectúe, así como la valoración del riesgo de las operaciones solicitadas) y de la obligación de facilitar los datos solicitados, en cuanto a que son necesarios para la valoración del riesgo y para el mantenimiento y efectividad de la relación contractual que se establece.

Igualmente, se informa sobre la posibilidad del ejercicio de los derechos de acceso, rectificación, cancelación y oposición comunicando las direcciones de los responsables de los ficheros ante los que pueden ejercitarse tales derechos.

No obstante, en los casos en que es el personal del centro comercial el que recaba los datos directamente del solicitante cumplimentando un formulario de uso interno que no se facilita al cliente, no se ha acreditado que se facilite a dicho solicitante la información a que se refieren los párrafos anteriores.

- Tratamientos de datos

Los datos aportados por los clientes son sometidos a los siguientes tratamientos:

- a) Emisión de la tarjeta.



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

Las tarjetas emitidas por las entidades financieras cumplen con las especificaciones recogidas en estándares ISO. Entre los datos que se recogen grabados en el anverso de la misma figuran: código identificativo de la entidad emisora, número de tarjeta y apellidos y nombre del titular. En la banda magnética existente en el reverso se almacena, entre otra, la siguiente información: número de cuenta, apellidos e inicial del nombre y fecha de caducidad.

Las solicitudes de tarjeta son analizadas por los propios establecimientos financieros, los cuales siempre disponen de sistemas automáticos (técnicas de scoring, sistemas expertos,...) que proceden a evaluar el riesgo de la situación crediticia del interesado. El resultado final del análisis se concreta en una decisión acerca de la solicitud, aprobando o denegando la misma. Esta decisión es, en algunos casos, revisada por una persona y, en otros, el resultado de la denegación por el sistema automático supone directamente la no concesión de la tarjeta. En algunos casos no se informa al interesado de que su solicitud ha sido denegada, salvo que éste lo solicite expresamente.

Los establecimientos financieros tienen en cuenta para autorizar la concesión de la tarjeta la posible inclusión de los datos personales del interesado en ficheros externos de solvencia patrimonial, así como el hecho de que conste en sus ficheros automatizados algún impagado derivado de relaciones que haya mantenido anteriormente con ellos.

Se ha verificado que los establecimientos financieros eliminan periódicamente de sus ficheros automatizados los datos de las solicitudes de tarjeta que resultaron denegadas, razón por la que el cliente no llegó a establecer ninguna relación comercial. No obstante, se comprobó que una entidad mantenía en sus ficheros automatizados información de un gran número de solicitudes que habían resultado denegadas hace ya varios años.

b) Pagos realizados con la tarjeta

Para abonar las compras que realice en los centros comerciales el cliente debe aportar su tarjeta, procediéndose a la lectura de la banda magnética a través de los terminales punto de venta (TPV) y capturándose la información necesaria para proceder a la autorización de la operación y para la impresión del ticket de compra.

Con el fin de aprobar la operación, el terminal punto de venta establece comunicación con los sistemas informáticos del establecimiento financiero



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

correspondiente. Entre los datos enviados referidos al cliente sólo se encuentra su número de tarjeta.

Recibida la transacción en los sistemas informáticos del establecimiento financiero se procesa la misma y se procede a autorizar o denegar la operación, enviando la correspondiente respuesta al terminal punto de venta.

Todas las gestiones realizadas por los establecimientos financieros para la recuperación de recibos devueltos o que son finalmente impagados, como pueden ser envío de cartas o conversaciones telefónicas mantenidos por los clientes, se recogen en sus ficheros automatizados. Alguna entidad mantiene dicha información en la historia del cliente incluso después de que la deuda haya sido regularizada.

c) Tratamiento con fines publicitarios

Los establecimientos financieros incluyen habitualmente junto al extracto mensual de las operaciones realizadas información publicitaria de productos que se ofertan en los centros comerciales o en otras sociedades del Grupo al que pertenecen. Asimismo, en algún caso se realizan estudios de hábitos de compra para el envío de publicidad a sectores determinados de clientes.

- Comunicaciones de datos

Los establecimientos financieros remiten al Banco de España para su inclusión en el fichero Central de Información de Riesgos, los datos de aquellos clientes que hayan realizado compras a crédito por importes superiores a un millón de pesetas. Asimismo, comunican los datos de sus impagados a ficheros de incumplimiento de obligaciones dinerarias.

También es habitual que las remesas de recibos y facturas que envían los establecimientos financieros a las entidades bancarias, para su cargo en la cuenta de los clientes, se remitan telemáticamente a través de entidades bancarias intermediarias, las cuales se encargan de remitirlos finalmente al banco donde el cliente ha domiciliado sus recibos.

- Acceso a los datos por cuenta de terceros

La gran mayoría de los establecimientos financieros suelen establecer contratos y acuerdos de confidencialidad con otras empresas para la prestación de diferentes



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

servicios, lo que supone la entrega de soportes conteniendo los datos personales de sus clientes. Entre los servicios prestados se han detectado los siguientes:

- Estampación de la Tarjeta.
- Impresión, manipulación y envío de los extractos de cuenta y recibos mensuales, así como de la publicidad que remiten.
- Prestación de diversos servicios informáticos incluyendo la gestión diaria del propio fichero de clientes
- Revisión de las solicitudes de Tarjeta y estudio de autorización o denegación de las mismas.
- Atención telefónica, incluyendo la gestión de recuperación de impagos.

En el caso de un establecimiento financiero, el contrato para la prestación de servicios de impresión de los extractos mensuales de la cuenta de tarjeta, así como su manipulación, ensobrado y puesta en Correos, había sido suscrito por la empresa matriz del Grupo al que pertenece, en vez de por ella misma.

- Otros accesos

Asimismo, es muy habitual que el personal de los centros comerciales tenga acceso a los ficheros de clientes de los establecimientos financieros, para poder realizar las gestiones que soliciten los clientes en sus lugares de compra habituales.

1.2- Ficheros de otras Tarjetas de pago

Los centros comerciales disponen de equipos servidores específicos conectados a los TPV, en los cuales se consolidan los datos de las operaciones efectuadas por los clientes.

El cliente para abonar las compras que realice en los centros comerciales debe aportar su tarjeta, procediéndose a la lectura de la banda magnética a través de los TPV y capturándose la información necesaria para proceder a la autorización de la operación y para la impresión del ticket de compra.

El TPV determina el tipo de Tarjeta y establece comunicación con su correspondiente centro autorizador. Entre los datos que se envían a dicho centro para la aprobación de la



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

operación, siguiendo protocolos estándar, se encuentran: número de tarjeta, centro comercial donde se efectúa la compra, su importe y fecha y hora de realización, no enviándose otros datos de carácter personal como el nombre y apellidos del cliente.

En algunos casos los centros comerciales establecen comunicación a través de una entidad bancaria intermediaria, que es la encargada de establecer las comunicaciones oportunas para proceder a la autorización de la operación. Como respuesta a la transacción recibida del centro comercial, el centro autorizador analiza los datos de la operación y devuelve un resultado de aprobación o denegación de la misma.

Los centros comerciales disponen de ficheros de *log* de cajas y de movimientos de las operaciones que se efectúen utilizando tarjetas, en los cuales se incluyen entre otros los siguientes datos: Número de tarjeta, fecha de caducidad, importe de la compra, entidad emisora de la tarjeta y departamento de venta; no recogiendo ningún otro dato que permita identificar al titular de la tarjeta.

Por ello, las entidades consideran que estos ficheros no contienen datos de carácter personal al no poder identificar a su titular, ya que no disponen de ninguna otra información respecto del mismo, considerando también que no procede la notificación de dichos ficheros al Registro General de Protección de Datos.

Los centros comerciales consolidan los datos de las operaciones efectuadas por sus clientes con la información de facturación remitida por las entidades bancarias. Éstas no suelen coincidir con la entidad bancaria en la que el cliente ha domiciliado los cargos realizados con la Tarjeta, sino que son otras, denominadas “bancos merchant”, que realizan labores de intermediación en la gestión del cobro de las operaciones, percibiendo una comisión por ello.

En uno de dichos Centros se analizaron los ficheros resultantes de la conciliación y se comprobó que se almacenan los siguientes datos: fecha de operación, número de tarjeta, importe, compra/anulación, comisión y campo asociado, número de autorización y fecha de conciliación.

1.3- Ficheros de Tarjetas de fidelización de clientes

Algunos centros comerciales son también responsables de ficheros automatizados en los que se recogen los datos de sus clientes que pertenecen a sus propios Clubes de fidelización. Uno de ellos es un Club infantil, que ofrece a sus socios diversas actividades de ocio.



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

- Recogida y tratamiento de datos personales

Los datos de los socios son recabados por los propios centros comerciales a través de formularios específicos que son firmados por los propios interesados. En el caso del Club infantil el formulario de adhesión debe ser suscrito con su firma por el padre o madre del menor, figurando que autoriza la inclusión de los datos de su hijo en un fichero automatizado cuyo responsable es el centro comercial. También se informa en el formulario de las cesiones de datos que se realizan a las empresas que gestionan los servicios propios del Club y de la posibilidad del ejercicio de los derechos de protección de datos.

En los formularios de los demás Club de fidelización figura que el interesado autoriza la automatización de sus datos personales y se le informa de aspectos tales como:

- Obligación de facilitar los datos contenidos en el formulario para convertirse en socio del Club.
- Comunicaciones de datos de los socios a otras empresas del Grupo y a otras que gestionan los servicios del Club.
- Posibilidad de ejercicio de los derechos que la Ley Orgánica 15/1999 reconoce a los afectados, ya sea por vía telefónica o por correo.

Un centro comercial dispone de un *datawarehouse* en el que se almacenan los datos de sus socios y de las compras que éstos hayan realizado, detalladas por cada uno de los artículos adquiridos. Esta información se utiliza para realizar estudios de mercado y para campañas de promociones y lanzamiento de productos, obteniéndose los datos personales de aquellos socios entre los que se lanzará la promoción.

- Acceso a los datos por cuenta de terceros

Los centros comerciales han establecido contratos y acuerdos de confidencialidad con empresas para la prestación de diferentes servicios, para lo cual hacen entrega de soportes conteniendo los datos personales de sus socios. Entre los servicios que se prestan se encuentran los siguientes:

- Impresión, manipulación y envío de información relacionada con los Clubes, así como de la publicidad que se remita.
- Mantenimiento del fichero (altas, actualizaciones).



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

- Atención telefónica a socios.

Así mismo, en uno de los contratos suscritos por una de las entidades inspeccionadas consta la autorización para que la empresa contratada para la prestación de un servicio pueda, a su vez, subcontratar determinados servicios para la conversión de los soportes de datos que se faciliten.

1.4- *Medidas de Seguridad adoptadas en las tres clases de ficheros.*

En relación con las medidas de seguridad establecidas en el Real Decreto 994/1999, de 11 de junio, los aspectos más relevantes de tales medidas implementadas en los ficheros automatizados cuyos responsables son los centros comerciales y establecimientos financieros emisores de tarjetas, se detallan a continuación de manera conjunta ya que se refieren a conclusiones comunes a todos los ficheros inspeccionados.

- Niveles de seguridad

Los niveles de seguridad de los ficheros inspeccionados, atendiendo a la naturaleza de la información que contienen, es el nivel básico para los ficheros de fidelización de clientes, y el de nivel medio para los otros dos, ya que además de datos identificativos contienen datos de servicios financieros. A excepción de un establecimiento financiero, el resto considera sus ficheros de emisión y gestión de tarjetas como de nivel de seguridad medio

- Documento de seguridad

Todas las entidades inspeccionadas disponen de uno o varios documentos en los que se recoge la normativa de seguridad contemplando los aspectos que se exigen en el art. 8 del Reglamento (controles periódicos, desechado o reutilizado de soportes, funciones y obligaciones del personal...), estando en unas entidades más detallado que en otras.

- Registro de incidencias

Todas las entidades disponen de registros donde se recogen todas las incidencias que se producen, no sólo las específicas de seguridad, cumplimentándose en general los



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

aspectos que se detallan en los arts. 10 y 21 del Reglamento (tipo de incidencia, momento en el que se ha producido...).

- Identificación y autenticación de los usuarios

El mecanismo que se utiliza en todos los sistemas, para asegurar la identificación y autenticación de los usuarios, es la asignación a éstos de un código y de una contraseña, lo que permite la identificación de los usuarios que acceden al sistema. En los sistemas operativos y productos de seguridad éstos se encuentran configurados para obligar a los usuarios a cambiar las contraseñas periódicamente, así como para bloquear a los usuarios desde los que se intente reiteradamente un acceso no autorizado, conforme a lo previsto en los arts. 11 y 18 del Reglamento.

No obstante, no existe una asignación personalizada de usuarios para el personal de los centros comerciales que tiene acceso a los ficheros de clientes de los establecimientos financieros, creándose usuarios genéricos u otorgándose permisos específicos de acceso en función de la ubicación del terminal desde el que se vaya a acceder.

- Control de acceso

En general, todos los sistemas inspeccionados están diseñados para restringir a los usuarios el acceso a los datos del fichero teniendo en cuenta las funciones que desempeñan. En cuanto al control de acceso físico a los locales donde se encuentran ubicados los equipos informáticos y los ficheros, se encuentra restringido, utilizando medidas como el mantenimiento de una puerta cerrada bajo llave, u otras más sofisticadas como la implantación de un sistema de control de acceso biométrico mediante huella dactilar.

- Gestión de soportes, copias de respaldo y responsable de seguridad

Los soportes magnéticos se almacenan e inventarían en áreas y mediante herramientas específicas. Así mismo, todas las entidades tienen definidos procedimientos para la realización de copias de respaldo de los datos contenidos en sus ficheros, ya que mantienen un claro interés en preservar la disponibilidad de la información y contemplan la figura del responsable de seguridad, cumpliéndose en general las medidas que sobre estos aspectos contempla el Reglamento de Medidas de Seguridad.

2.- RECOMENDACIONES



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

A tenor de lo expuesto y en atención al resultado de las actuaciones practicadas por parte de la Inspección de Datos, se han observado ciertas deficiencias en los sistemas de información cuyos responsables son las Grandes Superficies y Establecimientos financieros inspeccionados en relación al cumplimiento de las prescripciones de la Ley Orgánica 15/1999, cuya subsanación supondría una mejora en la aplicación de la citada Ley Orgánica y en la normativa que la desarrolla.

Por lo tanto, el Director de la Agencia de Protección de Datos, en virtud de las potestades que le otorga el artículo 5 c) y d) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, dicta las siguientes **RECOMENDACIONES** que deberán ser observadas, en particular, por las entidades inspeccionadas y, con carácter general, por todas las entidades del sector y establecimientos financieros de crédito, emisores de las tarjetas de referencia, al objeto de adecuar plenamente los tratamientos automatizados que realiza a los principios de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal,

PRIMERA: DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Con carácter general se ha detectado que las entidades inspeccionadas cumplen las prescripciones previstas en el art. 5 L.O.P.D., en tanto en cuanto se informa de la existencia del fichero y finalidad de la recogida, obligatoriedad de facilitar los datos, posibilidad de ejercicio de los derechos que al afectado reconoce la ley y comunicación de datos a efectuar.

Sin embargo, se ha observado que en algunas ocasiones el personal del centro comercial recaba los datos directamente del solicitante de la tarjeta cumplimentando un formulario de uso interno que no facilita al interesado. En estos casos, cuando los formularios para la recogida de los datos no sean cumplimentados directamente por el interesado, deberán adoptarse las medidas pertinentes para asegurar que el personal del centro que proceda a la recepción de los datos facilite la información a la que se refiere el citado art. 5.1 de la L.O.P.D. por ser de obligada comunicación por el responsable del fichero, toda vez que el desconocimiento de esos datos básicos supone una clara indefensión para el cliente que le imposibilita el ejercicio de los derechos de acceso, rectificación, cancelación y oposición reconocidos por la Ley.

SEGUNDA: CONSENTIMIENTO DEL AFECTADO EN EL TRATAMIENTO DE SUS DATOS PERSONALES



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

De acuerdo con lo dispuesto en el apartado 1 del artículo 6 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

Ciertamente, la Ley permite que en la mayoría de los casos el consentimiento se preste de forma “tácita”. Sin embargo, en los supuestos aquí analizados, dada la trascendencia de las relaciones negociales o contractuales que se van a derivar, se considera una buena práctica que el afectado suscriba con su firma los formularios y solicitudes de contratos de tarjetas, como muestra de que consiente el tratamiento de sus datos personales en los mismos términos en los que se le informa en dichos formularios o contratos.

En particular, vistos los tratamientos que realizan los establecimientos financieros de crédito sobre los datos de los solicitantes de tarjetas y clientes, deberá prestarse especial atención en recabar el consentimiento para la valoración del riesgo crediticio de los datos personales aportados por los afectados en su solicitud de obtención de tarjeta, informando, en su caso, de que dicha valoración estará apoyada por la utilización de un sistema automático. En ningún caso podrá realizarse tal valoración si no se cuenta para ello con el consentimiento informado del interesado.

Además, y puesto que en algunos casos no se informa al interesado de que su solicitud de tarjeta le ha sido denegada, deberá tenerse en cuenta que de conformidad con el art. 13.2 L.O.P.D., el afectado podrá impugnar decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. Por ello, en el caso de que un establecimiento financiero de crédito deniegue una solicitud de las tarjetas que emita y, con el fin de permitir al interesado el recurso de dicha decisión, debería informarle de dicha denegación y de las razones que la hayan motivado

En relación a los clubes de fidelización promovidos por los centros comerciales y teniendo en cuenta los tratamientos que realizan sobre los datos de sus socios, deberá recabarse su consentimiento autorizando que se puedan realizar con sus datos estudios de mercado o elaboración de perfiles, a utilizar por el centro para campañas de promoción y lanzamiento de productos, salvo que tales estudios se realicen disociando los datos de los afectados.

TERCERA: CALIDAD DE DATOS

El art. 4.2 L.O.P.D. dispone que *“los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.....”*



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

El envío de publicidad que realizan tanto los centros comerciales como los establecimientos financieros emisores de tarjetas, es, en principio, ajeno a la relación comercial o contractual existente entre las citadas entidades y los clientes. Por tanto, y a fin de evitar posibles infracciones del principio de calidad de datos consagrado en el artículo transcrito, desviando la finalidad para la que los datos fueron recabados, deberá obtenerse el consentimiento de los clientes para enviar publicidad personalizada de productos de terceras entidades.

CUARTA: CANCELACIÓN DATOS

Se ha comprobado que, en general, las entidades cancelan periódicamente de sus ficheros los datos personales de las solicitudes de tarjetas que fueron denegadas, aunque en un caso se comprobó que la entidad aún mantenía en sus ficheros gran número de solicitudes denegadas varios años atrás.

En este sentido, la Ley Orgánica 15/1999, en el artículo 4.5 bajo el epígrafe “calidad de datos”, consagra el principio de conservación limitada de los datos al disponer: *“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. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados”*.

Por otra parte, los apartados 3 y 5 del artículo 16 de la citada Ley especifican: *“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. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado”*.

Por ello, en virtud de las prescripciones legales transcritas, todas las entidades afectadas deberán proceder al bloqueo de todos aquellos datos de carácter personal incluidos en sus sistemas de información que hayan dejado de ser necesarios al fin para el que fueron recabados o registrados y proceder a su cancelación definitiva una vez cumplidos los plazos de prescripción derivados de las obligaciones o responsabilidades nacidas del tratamiento. El bloqueo sólo permitirá el tratamiento de tales datos para la finalidad que lo justifique. Por excepción, se podrán mantener determinados datos por interés histórico, estadístico o científico, de acuerdo con su legislación específica.



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

QUINTA: COMUNICACIÓN DE DATOS

De acuerdo a lo establecido en el artículo 11.1 de la L.O.P.D., *“los datos de carácter personal objeto de tratamiento sólo podrán se 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”*. El consentimiento no será preciso, entre otros, cuando la cesión está autorizada en una Ley o si la comunicación se efectúa previo procedimiento de disociación.

En consecuencia, cuando las entidades a las que afecta esta recomendación comuniquen o cedan los datos personales recabados de sus clientes a otras empresas del Grupo de sociedades al que pertenezca el establecimiento financiero o centro comercial, deberán cumplir acumulativamente las dos condiciones impuestas por el transcrito art. 11.1. Además, la finalidad de la cesión ha de ser cognoscible para el interesado en el momento de prestar el consentimiento, no siendo lícito el mero consentimiento genérico para ceder sus datos conforme a expresiones tales como “ceder sus datos a otras empresas del grupo”, “realizar publicidad”, “remitirle ofertas comerciales”.....

En definitiva, el consentimiento ha de otorgarse para supuestos y finalidades concretas y determinadas, siendo nulo de pleno derecho, de conformidad con lo dispuesto en el art. 11.3 de la misma Ley, el consentimiento para la cesión absoluta o indeterminada.

SEXTA: DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN.

De conformidad con lo dispuesto en los artículos 15 y concordantes de la Ley Orgánica 15/1999, los derechos de acceso, rectificación, cancelación y oposición de los datos de carácter personal contenidos en ficheros automatizados, se configuran como uno de los ejes fundamentales sobre los que se articula la protección de los datos de ciudadanos, y aparecen regulados, además, en el Real Decreto 1332/1999 y en la Instrucción 1/1998 de la Agencia de Protección de Datos. Los derechos de acceso, así como los de rectificación, cancelación y oposición de datos son derechos personalísimos y los responsables de los ficheros, resolverán sobre la solicitud en los plazos establecidos por la ley. En el supuesto de que el responsable considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente en el plazo legalmente establecido. Si no fuere debidamente atendido, el afectado podrá reclamar ante la Agencia de Protección de Datos.



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

La norma Primera de la Instrucción 1/1998, establece los requisitos generales a cumplir tanto por el ciudadano en la solicitud del ejercicio de los derechos como por parte del responsable del fichero con objeto de resolver sobre la solicitud. A tal efecto, el apartado 5 de la citada norma dispone *“El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos”*.

Se ha detectado en la inspección practicada a los centros comerciales que es muy frecuente que el cliente se limite a solicitar la rectificación de sus datos personales (v. gr.: cambio de domicilio) personándose en el centro o incluso por teléfono (a lo que accede el personal del centro), pero sin que tal rectificación pueda considerarse “formalmente” como el derecho reconocido como tal en la L.O.P.D. Obviamente, no es competencia ni voluntad de esta Agencia regular el ejercicio de prácticas comerciales o relaciones negociales entre proveedor y cliente, pero sí entiende que a fin de dar una mejor respuesta a los ciudadanos en el ejercicio de sus derechos, sería conveniente que los responsables de los ficheros establecieran un procedimiento documentado con objeto de su conocimiento y cumplimiento por parte de todas las personas que integran la organización.

De otro lado, el artículo 6.4 de la L.O.P.D. establece que, *“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 cuando se den todas las circunstancias previstas en la norma transcrita.

SÉPTIMA: ACCESO A LOS DATOS POR CUENTA DE TERCEROS.

Todos los centros comerciales y entidades financieras tienen contratado con terceros la prestación de determinados servicios , lo que supone la entrega de soportes informáticos conteniendo datos personales.

De conformidad con lo dispuesto en el artículo 12.2 de la L.O.P.D., *“la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los*



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

comunicará ni siquiera para su conservación, a otras personas. En el contrato se estipularán, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar". De otro lado, la L.O.P.D., establece las medidas de seguridad que deberán de cumplir los ficheros automatizados que contengan datos de carácter personal, tanto por el responsable del fichero como por el encargado del tratamiento.

Por todo ello, con objeto de conseguir una mejor adecuación de los tratamientos automatizados a los principios de la normativa de protección de datos, los responsables de los ficheros deberán estipular las medidas de seguridad que el "encargado" del tratamiento está obligado a implementar, así como efectuar los controles necesarios con objeto de verificar de forma periódica el cumplimiento de las mismas.

Con base en estas consideraciones legales, que en cualquier caso siempre deberán ser tenidas en cuenta por los responsables de los ficheros, en la inspección practicada se han observado tres particularidades que deberán ser corregidas:

- a) En un caso, el contrato de prestación de servicios ha sido firmado o celebrado por la matriz del Grupo al que pertenece el establecimiento financiero de referencia y el encargado del tratamiento. Pues bien, en todo caso el contrato de prestación de servicios deberá concluirse entre el responsable del fichero y el encargado del tratamiento, sin que pueda ser suscrito por otras empresas del Grupo de sociedades al que pertenezca dicho responsable.
- b) El supuesto de subcontratación de prestación de servicios detectado en una de las entidades inspeccionadas no podrá llevarse a cabo a tenor de lo dispuesto en el art. 12.2 *in fine* L.O.P.D., que prohíbe al "encargado" del tratamiento (prestador del servicio) ceder los datos obtenidos del "responsable" del fichero, cuando dice "*ni los comunicará ni siquiera para su conservación, a otras persona*". La Ley impone, pues, una limitación a la subcontratación que impide la celebración del contrato aquí referido. No obstante, el encargado del tratamiento podrá celebrar estos contratos siempre y cuando actúe en nombre y por cuenta del responsable del fichero.
- c) Finalmente, en el caso de acceso a los datos del cliente de los establecimientos financieros, realizado por el personal de los centros comerciales que presta servicios de atención al cliente, dicho acceso no podrá realizarse salvo que exista previa solicitud del interesado y esté amparado en el mantenimiento o cumplimiento de una relación contractual o esté regulada en un contrato de prestación de servicios.

OCTAVA: NOTIFICACIÓN E INSCRIPCIÓN REGISTRAL.



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

La creación de ficheros de datos de carácter personal deberá ser notificada previamente a la Agencia de Protección de Datos, cumplimentando el formulario establecido al efecto en la Resolución del Director la Agencia, de 30 de mayo de 2000 (BOE nº 153, de 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 correspondientes solicitudes de inscripción en el Registro General de Protección de Datos, los cuales también pueden obtenerse a través de Internet en la página: www.agenciaprotecciondatos.org.

Los ficheros que recogen los datos de las operaciones efectuadas por los clientes en los centros comerciales utilizando tarjetas de pago, cuyos responsables son los propios centros, y que contengan cualquier información concerniente a personas físicas identificadas o identificables, como es el número de la tarjeta con la que se ha realizado la operación, son considerados ficheros con datos de carácter personal en los términos establecidos en la LOPD, siéndoles de aplicación todo lo dispuesto en la misma; por ello, la creación de estos ficheros deberá ser notificada a la Agencia.

NOVENA: SEGURIDAD DE LOS DATOS.

La Ley Orgánica 15/1999, en su artículo 9 dispone que *“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. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria”*.

El Real Decreto 994/1999, aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que se clasifican en tres niveles atendiendo a la naturaleza de la información tratada y la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

En particular, los establecimientos financieros de crédito, al contener en sus ficheros datos de servicios financieros, deberán cumplir al menos las medidas de nivel básico y medio que en el citado Reglamento se establecen, de conformidad con lo previsto en su art. 4.2. Las mismas medidas deberán cumplir los ficheros de los que son responsables los centros comerciales cuando prestan servicios financieros.



AGENCIA DE PROTECCIÓN DE DATOS

CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

En el supuesto en que, siendo de aplicación lo previsto en el art. 18.1 del Reglamento, se hayan creado usuarios genéricos que permitan el acceso a la información el responsable del fichero deberá establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. De esta forma, los establecimientos financieros de crédito deberán adoptar las medidas oportunas, para garantizar que se otorga un código de usuario único a cada una de las personas que accedan a sus ficheros, aun en el caso de que las mismas presten sus servicios en los centros comerciales, no siendo en ningún caso válidas las asignaciones genéricas de usuarios.

Madrid, a 27 de julio de 2001
EL DIRECTOR DE LA AGENCIA
DE PROTECCIÓN DE DATOS
Fdo. Juan Manuel Fernández López