

**AGENCIA ESPAÑOLA  
DE PROTECCIÓN DE DATOS**

**INFORME SOBRE TRANSFERENCIAS  
INTERNACIONALES DE DATOS**

**INSPECCIÓN SECTORIAL DE OFICIO ESPAÑA – COLOMBIA EN  
CENTROS DE ATENCIÓN AL CLIENTE**

**JULIO 2007**

## **INDICE**

- I. ANTECEDENTES Y SITUACIÓN ACTUAL**
  
- II. INSPECCIÓN SECTORIAL DE OFICIO ESPAÑA-COLOMBIA EN EL SECTOR DE LOS CENTROS DE ATENCIÓN AL CLIENTE**
  - 1 METODOLOGÍA DE INSPECCIÓN**
    - A SELECCIÓN DE LA MUESTRA DE INSPECCIÓN**
    - B FASES DE LAS ACTUACIONES**
    - C TRATAMIENTOS DE DATOS VERIFICADOS**
    - D ENTORNO TECNOLÓGICO**
  - 2 CONCLUSIONES DE LA INSPECCIÓN**
    - A TRATAMIENTOS DE DATOS AUDITADOS**
    - B MEDIDAS DE SEGURIDAD**
  
- III. NOVEDADES PROCEDIMENTALES**
  - 1 INFORMACIÓN PÚBLICA**
  - 2 CONFIDENCIALIDAD DE LA DOCUMENTACIÓN DEL EXPEDIENTE**
  - 3 CUMPLIMIENTO DE OTRAS OBLIGACIONES LEGALES**

#### **IV. RECOMENDACIONES**

**1 INSPECCIÓN SECTORIAL DE OFICIO ESPAÑA - COLOMBIA  
EN EL SECTOR DE LOS CENTROS DE ATENCIÓN AL  
CLIENTE**

**2 PROCEDIMIENTO DE AUTORIZACIÓN**

**3 INDICADORES DE VERIFICACIÓN DE LA SOLICITUD**

#### **ANEXO. MARCO NORMATIVO**

El presente documento tiene por objeto describir el marco regulador que ha de tenerse en cuenta para la realización de transferencias internacionales de datos de carácter personal, así como señalar la forma de solicitar la preceptiva autorización de Director de la Agencia Española de Protección de Datos en los casos en los que se tenga previsto transferir datos de carácter personal con destino a países que no proporcionan un nivel de protección adecuado cuando dicha transferencia no se encuentre amparada en ninguna excepción prevista en el artículo 34 de la LOPD.

A lo largo del documento se señalan las iniciativas puestas en marcha por la Agencia Española de Protección de Datos al objeto de auditar las prácticas existentes en el sector de los Centros de Atención a Clientes en el ámbito de los operadores de telecomunicaciones, y de dotar de mayor transparencia y garantías en el procedimiento de autorización de las transferencias internacionales de datos. Asimismo, se recogen las recomendaciones formuladas a partir de estas iniciativas.

## I ANTECEDENTES Y SITUACIÓN ACTUAL

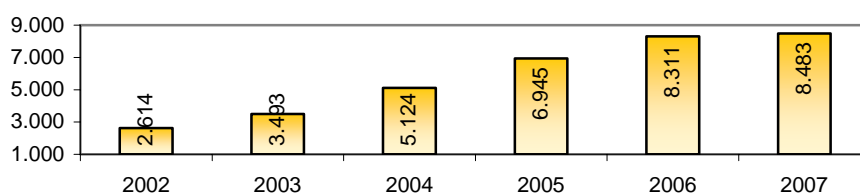
La integración económica y social resultante del establecimiento y funcionamiento de un mercado globalizado, ha implicado un desarrollo notable de los flujos transfronterizos de datos personales entre distintos agentes públicos y privados establecidos en diferentes países. Este flujo de datos se ha visto favorecido por factores como el avance de las tecnologías de la información y, en particular, el desarrollo de Internet, que facilitan considerablemente el tratamiento y el intercambio de información, y que permiten compartir recursos tecnológicos, centralizar determinadas actividades y procesos, y abaratar costes en la prestación de servicios por la propia empresa fuera del país en el que se encuentra establecida.

La Agencia Española de Protección de Datos ha podido constatar este aumento importante transferencias internacionales de datos a través de las notificaciones de ficheros que son inscritos en el Registro General de Protección de Datos, en el que a 1 de julio de 2007 han sido declaradas 8.483 transferencias.

En esta cifra se incluyen las comunicaciones de datos notificadas al Registro que tienen como destino los países del Acuerdo sobre el Espacio Económico Europeo, y los que han sido considerados por la Comisión Europea con un nivel adecuado de protección en aplicación de la Directiva 95/46/CE, en cuyo caso se encuentran Suiza, Argentina, Guernsey e Isla de Man, así como Canadá, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos, y Estados Unidos, respecto de las entidades adheridas a los principios de "Puerto Seguro" o "Safe Harbor". Asimismo, comprende las que no teniendo como destino un país con nivel adecuado de protección, se encuentran amparadas en las excepciones previstas en el artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y, por último las 149 que han requerido la Autorización del Director de la Agencia.

### Evolución de las transferencias internacionales de datos notificadas en el Registro.

1.7.2007



Autorizaciones de transferencias internacionales. 1-7-2007<sup>1</sup>

	2000	2001	2002	2003	2004	2005	2006	2007		Total Autoriza- ciones
								Autoriza- ciones	Otras solicitudes	
EEUU	1	9	2	6	40	9	16	4	4	87
Marruecos	1	-	-	-	2	2	2	1		7
India	-	-	-	-	4	-	3		1	7
Singapur	-	-	-	-	1	-	1		1	2
Japón	-	-	-	-	-	1	-		1	1
Panamá	-	-	-	-	-	2	-			2
Colombia	-	-	-	-	-	1	4	2	3	7
Malasia	-	-	-	-	-	1	1		1	2
Tailandia	-	-	-	-	-	1	-		1	1
Chile	-	-	-	-	-	1	7	7	1	15
Uruguay	-	-	-	-	-	1	1		2	2
Filipinas	-	-	-	-	-	-	3	1		4
Perú	-	-	-	-	-	-	4	3	3	7
China	-	-	-	-	-	-	1		1	1
Hong Kong	-	-	-	-	-	-	1			1
Guatemala	-	-	-	-	-	-	1			1
Paraguay							1			1
Australia									1	
Brasil									1	
Canadá									1	
Egipto									1	
El Salvador									1	
Nicaragua									1	
Nigeria									1	
Solicitudes presentadas	2	9	2	19	56	45	54	49		236
Archivadas/en tramitación	-	-	-	13	6	16	17		36	88
Autorizaciones	2	9	2	6	47	19	46	18		148

Por lo que respecta a las finalidades para las que se realizan estas transferencias internacionales que han requerido la autorización del Director de la Agencia, se pueden destacar:

- Fines relacionados con necesidades propias de **la gestión empresarial en un contexto global**. Las empresas multinacionales requieren la realización de transferencias internacionales de datos para finalidades tales como la gestión, mantenimiento y soporte técnico de los sistemas de información. Por otra parte se solicitan estas autorizaciones en relación con la gestión eficiente de los recursos

<sup>1</sup> Estos datos se refieren exclusivamente a las transferencias que requieren autorización del Director por tener como destino países que no disponen de un nivel de protección adecuado. Es preciso tener en cuenta que existen autorizaciones que tienen mas de un destinatario ubicados en países diferentes. Asimismo, algunas solicitudes de autorización han sido resueltas en el año siguiente al de su presentación.

humanos, los clientes y los proveedores, así como la prestación de servicios de apoyo administrativo en relación con estos.

En esta categoría de transferencias internacionales se encuentra el 58% de las autorizaciones otorgadas por la Agencia, que están relacionadas con grupos multinacionales que tienen su empresa matriz fuera de España, principalmente en los **Estados Unidos de América**, y su actividad empresarial distribuida por diferentes países. A modo de ejemplo, se puede citar la gestión global de personal en compañías internacionales.

- La atención telefónica a los clientes, y otras acciones de marketing telefónico dirigidas a mejorar el grado de satisfacción de los mismos, como la gestión centralizada de los servicios de atención al cliente.

En este grupo destacan principalmente las prestaciones de **servicios de atención al cliente o telemarketing** por importadores de datos establecidos en **Latinoamérica**, que se han visto incrementadas significativamente en los dos últimos años, y que corresponden con un 22% de todas las autorizaciones de la Agencia.

En relación con este tipo de autorizaciones la Agencia ha podido constatar la existencia de cierta inquietud respecto a estos tratamientos. En distintas reuniones con representantes de sindicatos se ha puesto de manifiesto la existencia de personas o colectivos que son titulares de otros derechos o intereses legítimos que pueden resultar afectados por las correspondientes resoluciones de autorización.

Teniendo en cuenta esta problemática, la Agencia ha considerado necesario, no sólo valorar la suficiencia jurídica de las garantías aportadas por los solicitantes, sino su efectivo cumplimiento. Adicionalmente se ha tratado de dotar de mayor transparencia al procedimiento de autorización, para lo que se han adoptado las siguientes iniciativas:

- Realización de una **inspección sectorial de oficio** a determinados importadores de datos destinatarios de transferencias internacionales previamente autorizadas en centros de atención a clientes establecidos en terceros países.
- Introducción de un trámite de información pública en la tramitación de los procedimientos en los que se exige autorización del Director la Agencia Española de Protección de Datos, de acuerdo con el artículo 33.1 de la Ley Orgánica 15/1999.

## **II. INSPECCIÓN SECTORIAL DE OFICIO ESPAÑA – COLOMBIA EN EL SECTOR DE LOS CENTROS DE ATENCIÓN AL CLIENTE**

La inspección sectorial de oficio España Colombia tuvo por objeto verificar el efectivo cumplimiento de la Ley Orgánica 15/1999 y su normativa de desarrollo en los centros de atención telefónica a clientes establecidos por empresas del sector de las telecomunicaciones para concluir con la formulación por el Director de la Agencia de unas RECOMENDACIONES dirigidas a mejorar las prácticas del sector en relación con la protección de datos.

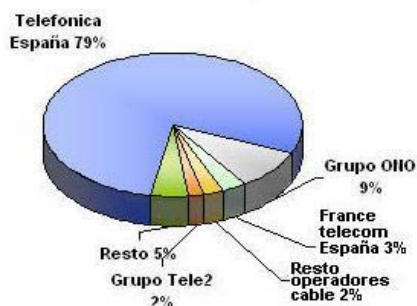
### **1. METODOLOGÍA DE INSPECCIÓN**

#### **A. SELECCIÓN DE LA MUESTRA DE INSPECCIÓN**

La selección de la muestra a inspeccionar se realizó en mayo de 2007. En esta fecha, para todo el sector de telecomunicaciones, constaban en el Registro General de Protección de Datos un total de 22 autorizaciones de transferencias internacionales de datos, que representan un 15% del total de autorizaciones, si se exceptúan las que tienen por destino los Estados Unidos de América. A excepción de 3 transferencias autorizadas que tienen como país destinatario Marruecos, el lugar de destino del resto son países latinoamericanos, en la mayor parte Chile, Perú, Colombia y en menor número Guatemala, Uruguay y Panamá.

Para determinar la selección de la muestra también se ha atendido a criterios basados en las cuotas de mercado publicadas por la Comisión del Mercado de las Telecomunicaciones, y a la repercusión social que se manifestó en diversos medios de comunicación. en relación a transferencias de datos de clientes de este operador a la República de Colombia.

Cuotas de mercado por ingresos totales del servicio telefónico básico fijo



Cuotas de mercado por ingresos totales de servicios de telefonía móvil automática



FUENTE: CMT Obtenido de Red.es Observatorio Julio 2006

Las solicitudes de transferencia internacional de datos efectuadas al amparo del artículo 33 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, cuando el prestador de servicios se encuentra instalado en países no declarados con un nivel de protección equiparable, habitualmente se amparan en el cumplimiento de las garantías concretadas en la Decisión de la Comisión 2002/16/CE. Éstas deben plasmarse en un contrato escrito, celebrado entre el exportador y el importador de datos en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

En el caso de Colombia, en los contratos suscritos entre los operadores de telecomunicaciones y las compañías que actúan como encargados de los tratamientos se ha incluido una cláusula que especifica el acuerdo por todas las partes de que la Agencia Española de Protección de Datos se encuentra facultada para auditar al importador en la misma medida y condiciones que lo haría respecto del exportador de datos conforme a la legislación española vigente en materia de protección de datos. Además, se estipula que el importador de datos garantiza que, a petición del exportador y/o de la Agencia, pondrá a disposición de esta última sus instalaciones de tratamiento de datos para que se lleven a cabo las auditorías que se consideren oportunas.

## B. FASES DE LAS ACTUACIONES

La inspección de datos ha centrado las actuaciones de investigación en las transferencias internacionales de datos autorizadas a dos operadores del sector de las telecomunicaciones que ofrecen la explotación del servicio de atención telefónica

comercial, el servicio de atención de averías y telemarketing, en relación con los servicios de telefonía fija e Internet al cliente residencial, así como telefonía móvil al sector de autónomos y pequeña y mediana empresa.

La metodología empleada se ha basado en la identificación de las finalidades de las transferencias y en el desarrollo de un plan de actuación en tres fases consistentes en la realización de visitas presenciales a los responsables de ficheros en España, en inspeccionar a los encargados de tratamiento con sede en ambos países y en auditar a los encargados de los tratamientos ubicados en Colombia.

La primera fase de visitas presenciales a las sedes de los operadores de telecomunicaciones ha abordado los siguientes objetivos:

- Analizar y concretar los servicios prestados desde las empresas ubicadas en Colombia
- Auditar los tratamientos que se realizan sobre los datos de carácter personal, y obtener información relativa los accesos que se efectúan desde España y desde Colombia.
- Comprobar que la información a la que se accede es adecuada a lo establecido en la prestación de servicio contratado.
- Estudiar las medidas de seguridad implementadas para el acceso a los datos de carácter personal realizados desde España y desde las entidades ubicadas en Colombia.
- Evaluar el entorno tecnológico utilizado para la transferencia internacional de datos.

En una segunda fase se han realizado inspecciones a las entidades encargadas del tratamiento que disponen de sede en España y sucursal en Colombia. Estas actuaciones se han centrado en los siguientes aspectos:

- Análisis de los servicios prestados desde las sedes ubicadas en España y desde las ubicadas en Colombia, así como los flujos de datos entre ambas.
- Comprobar la adecuación de los tratamientos realizados por estas entidades con las finalidades recogidas en los contratos de prestación de servicios.
- Contrastar los datos de carácter personal a los que se tiene acceso desde estas entidades y verificar si son pertinentes en relación con los servicios establecidos.

- Verificar las medidas de seguridad implementadas en relación a las instrucciones establecidas por el responsable del fichero y su adecuación a lo recogido en el Real Decreto 994/1999 de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Evaluar el entorno tecnológico utilizado para el acceso a los datos de carácter personal, como encargado del tratamiento del operador de telecomunicaciones.

En una última fase se han realizado visitas a los encargados de los tratamientos ubicados en Colombia, con la colaboración de los operadores de telecomunicaciones responsables de los ficheros. En esta fase se han detectado dos casuísticas distintas que han dado lugar a dos formas de actuación:

Por un lado, en el caso de entidades españolas con sucursal en Colombia, la visita se planteó como una inspección realizada en un local de la entidad que actúa como encargado del tratamiento, al objeto de contrastar lo ya verificado en la sede española, incidiendo en los aspectos más relevantes en función del lugar desde el que se presta el servicio. En la realización de estas actuaciones se contó en todo momento con la colaboración del responsable del fichero y de los encargados del tratamiento ubicados tanto en España como en Colombia.

Por otra parte, en las visitas presenciales realizadas por el Subdirector General de la Inspección de Datos y tres Inspectores de Datos de la Agencia a los encargados de tratamiento con sede únicamente en Colombia, se requirió al operador de telecomunicaciones responsable del fichero para que, a solicitud de los Inspectores de Datos y en estrecha colaboración con éstos, facilitase toda la información y documentación y permitiese el acceso a los sistemas de información necesarios para poder realizar la auditoría, utilizando los recursos implantados en la entidad colombiana.

En ambos casos, los objetivos perseguidos por las actuaciones han sido:

- Comprobar la adecuación de los tratamientos realizados por estas entidades con las finalidades recogidas en los contratos de prestación de servicios.
- Contrastar los datos de carácter personal a los que se tiene acceso desde estas entidades y verificar si son pertinentes en relación con los servicios establecidos.

- Verificar las medidas de seguridad implementadas en relación a las instrucciones establecidas por el responsable del fichero y su adecuación a lo recogido en citado Reglamento de Medidas de Seguridad.
- Evaluar el entorno tecnológico utilizado para el acceso a los datos de carácter personal, como encargado del tratamiento del operador de telecomunicaciones.

## **C. TRATAMIENTOS DE DATOS VERIFICADOS**

Los tratamientos realizados por las empresas contratadas se efectúan para prestar a los operadores de telecomunicación los siguientes servicios:

- Explotación del servicio de atención telefónica comercial al cliente residencial. Desde Colombia se reciben y realizan llamadas de clientes y tratamientos de datos relacionados con información sobre provisiones pendientes y facturación, e incidencias y reclamaciones al respecto. Asimismo pueden, a petición del cliente, recabar datos personales para el alta de nuevas líneas telefónicas.
- Explotación del servicio de atención telefónica comercial a los clientes autónomos y pequeña y mediana empresa. El servicio que se realiza consiste en el tratamiento de datos para la gestión administrativa y resolución de incidencias, verificación de la documentación aportada en solicitudes de alta, baja de los servicios contratados y emisión de llamadas cuando sea necesario informar al cliente.
- Servicios de Telemarketing a clientes del operador. Se realiza el contacto telefónico con los clientes para ofertar el producto y, en su caso, la grabación del mismo en el propio Sistema de Información del responsable.

## **D. ENTORNO TECNOLÓGICO**

Respecto de la estructura tecnológica de deslocalización de los servicios, en el caso de empresa española prestadora de servicios con sucursal en Colombia se utilizan dos enlaces de fibra óptica que conectan directamente una sede de la entidad ubicada en España, que a su vez se conecta con la red corporativa del operador de telecomunicaciones. Esto permite que los usuarios que trabajan desde Colombia tengan acceso a los mismos servicios y recursos que los que lo hacen desde la red de área local de los centros españoles. Para mayor seguridad, la arquitectura de conexiones de

comunicación mencionada utiliza un sistema de cifrado para todos los procesos que implican acceso a datos personales.

Respecto a la entidad prestadora de servicios con sede únicamente en Colombia, la estructura tecnológica de deslocalización se basa en el alquiler de líneas, propiedad del operador con quién han contratado la prestación de servicio origen de la transferencia internacional. En este caso, se corresponde con dos líneas dedicadas, a través de cable submarino, que se conectan directamente con la red troncal del operador. La administración de los dispositivos de la red de comunicaciones es realizada por personal del operador.

Hasta la fecha, en las auditorías y controles realizados por los responsables de los ficheros no se ha detectado ninguna incidencia.

## 2 .CONCLUSIONES DE LA INSPECCIÓN

### A. TRATAMIENTOS DE DATOS AUDITADOS

Los tratamientos de datos corresponden con los servicios especificados en los contratos aportados en la solicitud de las transferencias internacionales autorizadas por la Agencia Española de Protección de Datos.

Los datos personales que tienen acceso las entidades encargadas del tratamiento se consideran los necesarios para la prestación de los servicios contratados.

El acceso a los datos personales se efectúa directamente sobre los Sistemas de Información y ficheros de los responsables ubicados en territorio nacional e independientemente de la ubicación geográfica del encargado del tratamiento.

En ningún caso se produce transferencia de los ficheros de los operadores de telecomunicaciones a las empresas que actúan como encargadas del tratamiento.

Los servicios que se realizan actualmente pueden ser modificados –añadidos o suprimidos– en todo momento ya que como se ha manifestado, utilizan los sistemas de Información del propio operador.

Bajo criterios de calidad de servicio y coste, todos los operadores de telefonía inspeccionados tienen previsto aumentar en breve, bien los servicios deslocalizados que requieren acceso desde terceros países a datos de sus clientes, o bien el porcentaje de operaciones realizadas desde Colombia.

## **B . MEDIDAS DE SEGURIDAD**

### **Medidas adoptadas por los responsables de los ficheros:**

- Los operadores de telecomunicaciones han adoptado diversas medidas para proteger la información contenida en sus ficheros, entre otras, no permitir la realización de réplicas de los ficheros con datos personales fuera del territorio español, utilizar líneas dedicadas de comunicaciones para los accesos desde Colombia y haber implementado dispositivos de seguridad lógica.
- La confidencialidad en los accesos a la información se realiza estableciendo un canal cifrado entre extremos, si bien se ha detectado que no se ha implementado esta medida a todos los flujos de datos.
- Los accesos realizados por teleoperadores ubicados tanto en España como en Colombia quedan reflejados en los Sistemas de Información de los operadores de telecomunicación auditados.

### **Medidas adoptadas por los encargados del tratamiento:**

- Los prestadores de servicios ubicados en Colombia siguiendo las instrucciones de los responsables de los ficheros, han anulado en todos los puestos de trabajo utilizados por los teleoperadores los dispositivos periféricos que permiten extraer información.
- No se han instalado aplicaciones ofimáticas que faciliten la captura de pantallas ni disponen de facilidades de impresión de documentos.
- La identificación y autenticación de los teleoperadores ubicados en Colombia con accesos a los ficheros con datos personales del operador, se realiza mediante la

utilización de un código de usuario y una contraseña a través de una herramienta propiedad del responsable del fichero que gestiona la asignación de las contraseñas y los perfiles de acceso a los datos.

### III NOVEDADES PROCEDIMENTALES

Como se ha subrayado anteriormente se ha incluido un trámite de información pública en el procedimiento de autorización de transferencias internacionales de datos.

Este trámite tiene por objeto dotar de mayor transparencia al procedimiento y garantizar la intervención en el mismo de quienes consideren pertinente la realización de alegaciones. No obstante esta publicidad debe tener en cuenta la garantía de confidencialidad respecto de determinados datos del expediente.

Por último, debe señalarse que determinadas transferencias exigen una información previa al comité de empresa conforme a su normativa específica.

#### 1. INFORMACIÓN PÚBLICA

La incorporación de este trámite en el procedimiento de autorización de las transferencias internacionales de datos se acomoda a la regulación que con carácter general se contempla en el artículo 86 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

En este sentido, dado que el plazo de información pública que establece el art. 86.1 de la LRJPAC es de 20 días, lo que dificulta a la Agencia la tramitación del expediente en el plazo legalmente establecido, se ha propuesto la introducción en el **Proyecto de Reglamento** de desarrollo de la LOPD que está tramitando el Ministerio de Justicia, la aplicación del art. 86.4 para reducir el plazo de información pública a 10 días.

#### 2. CONFIDENCIALIDAD DE LA DOCUMENTACIÓN DEL EXPEDIENTE

Teniendo en cuenta que la documentación va a ser objeto de información pública, el exportador podrá indicar el grado de confidencialidad de la misma, si ésta está afectada por el secreto comercial en los términos señalados en el art. 37.5 de la Ley 30/1992 de Procedimiento Administrativo (LRJAP). En todo caso, podrán someterse al trámite de información pública las cláusulas contractuales generales que regulen la transferencia y la descripción de la misma.

### 3. CUMPLIMIENTO DE OTRAS OBLIGACIONES LEGALES

Como condición previa a la realización de una transferencia internacional de datos el exportador de los datos debe cumplir con el resto de obligaciones que establece la normativa de protección de datos, y cualquiera otra que pudiera resultar de aplicación.

Un caso paradigmático se da cuando la transferencia de datos puede afectar a otros derechos de los trabajadores. En este caso se deberá tener en cuenta el cumplimiento de las obligaciones relacionadas con el derecho laboral y, en particular, la obligación de informar al **comité de empresa** de acuerdo con el art. 42.4 del Estatuto de los Trabajadores (RDL 1/1995, de 24 de marzo) en relación con la transposición de la Directiva 2002/14/CE, por la que se establece un marco general relativo a la información y a la consulta de los trabajadores en la Comunidad Europea.

## IV. RECOMENDACIONES

### 1. INSPECCIÓN SECTORIAL DE OFICIO ESPAÑA – COLOMBIA EN EL SECTOR DE LOS CENTROS DE ATENCIÓN AL CLIENTE

Del resultado de las actuaciones practicadas por parte de la Inspección de Datos en empresas que realizan transferencias internacionales de datos para la prestación de servicios relacionados con Centros de Atención al Cliente, se desprende que el aspecto más relevante a tener en cuenta lo constituye las **medidas de seguridad** de los Sistemas de Información a los que se permite el acceso, para garantizar la confidencialidad e integridad de los datos de los clientes.

Por ello, el Director de la Agencia de Protección de Datos, en virtud de las potestades que le otorga en 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 por las entidades, al objeto de adecuar los tratamientos automatizados que realizan a los principios de la normativa vigente en materia de protección de datos de carácter personal.

**PRIMERA:** En relación con la Seguridad de los Datos Personales. (Artículo 9 de la LOPD y RD 994/1999)

El Real Decreto 994/1999, de 11 de junio de 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 a la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

#### a) Nivel de seguridad.

De acuerdo a lo establecido en el citado Reglamento, las entidades deberán cumplir las medidas de seguridad aplicables a cada uno de los ficheros en función de su clasificación.

En los casos que permiten obtener una evaluación de la personalidad del ciudadano, debe garantizarse la adopción de las medidas de seguridad de nivel medio en lo concerniente a la obligatoriedad de la realización de una auditoria bienal sobre el cumplimiento del Reglamento de Seguridad, al establecimiento de un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al Sistema de Información y a la verificación de que está autorizado, a los

controles de acceso físicos adecuados, así como al establecimiento de un registro de entrada y salida de soportes con datos de carácter personal.

#### **b) Acceso a través de redes**

El acceso a los datos de carácter personal a través de redes de telecomunicaciones, debe realizarse con las medidas de seguridad que garanticen un nivel de seguridad equivalente al correspondiente a los accesos en modo local, cumpliendo en cada caso con lo previsto en el Reglamento de Medidas de Seguridad en función de la naturaleza de los datos accedidos. Por ello, se considera una buena práctica, en los casos en los que no resulte normativamente exigible, como se ha verificado en las empresas inspeccionadas, la utilización de canales físicos seguros ya sea a través de líneas propietarias como dedicadas, evitando en lo posible la utilización de redes públicas de telecomunicación. En los casos de utilización de redes públicas es recomendable utilizar canales lógicos seguros empleando protocolos que permitan el cifrado de la información.

#### **c) Identificación y Autenticación**

El artículo 11 de dicho Reglamento también especifica que cuando el mecanismo de autenticación se base en la existencia de contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento de las mismas que garantice su confidencialidad e integridad. Dichas contraseñas deberán ser cambiadas periódicamente y almacenadas de forma ininteligible.

Por otra parte, el artículo 18 del citado Reglamento especifica que los usuarios que accedan a datos de carácter personal deberán poderse identificar de forma inequívoca y personalizada, verificándose que están autorizados para dicho acceso. Así mismo, debe limitarse la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Se recomienda que se delimite con precisión los perfiles de acceso a los Sistemas de Información, de tal forma que se garantice que los usuarios disponen de acceso únicamente a las funcionalidades necesarias acorde con el trabajo desempeñado.

Así mismo, es conveniente la utilización de un sistema de gestión integral de códigos de usuarios y contraseñas, gestionados y controlados directamente por el responsable del fichero, estableciendo mecanismos de identificación y autenticación de forma que la identificación del usuario que intenta acceder al sistema sea inequívoca y personalizada, y que garantice la confidencialidad e integridad de las contraseñas. También se deberá utilizar un sistema de distribución de contraseñas que asegure la confidencialidad de las mismas.

#### **d) Funciones y obligaciones del personal**

Conforme a lo especificado en el artículo 9 del Reglamento de Medidas de Seguridad, las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los Sistemas de Información deben estar claramente definidas y documentadas, debiendo adoptar el responsable, las medidas necesarias para que todo el personal conozca cuáles son sus funciones y obligaciones así como las normas de seguridad que afecten al desarrollo de las mismas y las consecuencias derivadas de su incumplimiento.

En consecuencia, el responsable del fichero deberá exigir al importador que adopte las medidas adecuadas para dar a conocer a todo su personal la normativa de protección de datos española que a ellos atañen.

#### **e) Registro de Incidencias**

Conforme a lo especificado en el artículo 10 y en su caso el 21 del Reglamento de Medidas de Seguridad se debe establecer un Registro de Incidencias en el que se incluyan las anomalías que afecten o pudieran afectar a la seguridad de los datos y que contenga al menos: tipo de incidencia, fecha y hora en la que se ha producido, persona que realiza la notificación, persona a quién se notifica y efectos derivados.

A este respecto, sería recomendable que el responsable del fichero tuviera conocimiento de las incidencias en materia de seguridad acaecidas en el importador y relacionadas con el acceso a los datos origen de la transferencia.

#### **f) Auditoria**

El artículo 17 del Reglamento de Medidas de Seguridad obliga a la realización de una auditoria de seguridad interna o externa que verifique el cumplimiento de dicho Reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años. El informe de auditoria debe ser analizado por el responsable de seguridad competente dictaminando sobre la adecuación de las medidas y controles al Reglamento, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias necesarias para su adopción por el responsable del fichero.

Por ello, se considera una buena práctica, en los casos en los que no resulte normativamente exigible, que estas auditorias se realicen, por parte del responsable del fichero, a todos los tratamientos realizados por los importadores de datos de carácter personal independientemente de la naturaleza de los mismos. El responsable del fichero comunicará, en todo caso, las conclusiones al importador con objeto de que adopte las medidas correctoras adecuadas, cuyo control deberá ser efectuado por el responsable del fichero.

#### **g) Terminales de acceso a los datos**

Para mayor seguridad, se recomienda que en los puestos de trabajo deslocalizados se anulen todos aquellos dispositivos periféricos que permiten extraer información así como se eliminen aquellos procedimientos que faciliten la captura de datos, disponiendo únicamente de las aplicaciones necesarias para la prestación del servicio.

El acceso a la red Internet se limitará a los puestos de trabajo estrictamente necesarios.

**SEGUNDA:** En relación con el acceso a los datos por cuenta de terceros (artículo 12 de la LOPD).

#### **Respecto a la prestación de servicios**

Así mismo, como concurre en las empresas inspeccionadas, además, el exportador y el importador han de suscribir un contrato de prestación de servicios, a tenor de lo dispuesto en el art. 12 de la LOPD.

A estos efectos, se recomienda que en las prestaciones de servicios que tengan por objeto la realización de un tratamiento de datos por parte de un tercero, la entidad tenga en cuenta, como responsable del fichero que la prestación habrá de plasmarse en un contrato, que deberá constar por escrito, y que establecerá expresamente que el destinatario únicamente tratará los datos conforme a las instrucciones del transmitente, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato y que adoptará las medidas de seguridad exigibles al transmitente conforme a las normativa española de protección de datos.

Además, deberá indicarse que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento.

En los casos analizados, el acceso a los datos por las empresas ubicadas en terceros países, se realiza telemáticamente a través de las aplicaciones informáticas facilitadas por el responsable del fichero, no existiendo, en principio, la posibilidad de disponer de copia de datos en soportes o documentos.

En cualquier caso, la receptora no podrá comunicar los datos, ni siquiera para su conservación, a otras personas.

**TERCERA:** En relación con el deber de secreto (artículo 10 de la LOPD).

Las empresas deberán adoptar las medidas oportunas para que los trabajadores estén informados de las exigencias en materia de seguridad y de la obligación del deber de secreto. A este respecto, se considera una buena práctica el que los trabajadores suscriban un documento en el que se les informe de dichos términos.

Se recomienda incluir en los contratos de trabajo cláusulas relativas al deber de secreto respecto de los datos personales a los que tienen acceso los empleados como consecuencia de su actividad, ya sean los propios empleados de la entidad como los empleados de las empresas prestatarias de servicios para la entidad con acceso a los datos personales de los clientes.

## 2 . PROCEDIMIENTO DE AUTORIZACIÓN

La tramitación del procedimiento de autorización de transferencias internacionales de datos y la incorporación de un trámite de información pública, debe ajustarse al plazo de tramitación legalmente establecido en el que la Agencia tiene que resolver estos expedientes. Por ello, es muy importante extremar el cuidado en la presentación de la documentación correspondiente, a los efectos de agilizar su tramitación.

A tal efecto, deberían tenerse en cuenta las siguientes recomendaciones:

**PRIMERA.** Cumplimiento de obligaciones previas.

El responsable que solicita una autorización de transferencia internacional de datos está obligado al cumplimiento del resto de obligaciones que establece la Ley Orgánica 15/1999 para realizar los correspondientes tratamientos de datos en España.

Entre otros, deberá haber cumplido con la obligación de notificar los ficheros afectados al Registro General de Protección de Datos, y mantener actualizada la información de dicha inscripción.

Por otra parte, deberá cumplir con cualquier otra obligación legal relacionada con el objeto de la transferencia internacional. Entre estas, si fuera el caso, deberá haber informado al Comité de Empresa en los términos previstos en el Estatuto de los Trabajadores.

## **SEGUNDA.** Requisitos de la solicitud

En la solicitud ante la Agencia, el exportador deberá consignar:

- La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código/s de inscripción en el Registro General de Protección de Datos
- La transferencia o transferencias respecto de las que se solicita la autorización, con una descripción de la finalidad que la justifica y las operaciones básicas de tratamiento asociadas a la misma, así como una descripción detallada de los datos personales del fichero o ficheros, señalados en el punto anterior, que sean objeto de la transferencia.
- La documentación que incorpore las garantías exigibles para la obtención de la autorización, en la que deberá hacerse constar una descripción de las medidas de seguridad concretas que van a ser adoptadas, tanto por el exportador como por el importador de los datos durante la transferencia de los mismos, y en relación con el fichero o ficheros objeto de la misma.
- Una copia compulsada del contrato entre el exportador y el importador de los datos, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes.
- También puede resultar de interés para facilitar la valoración de la solicitud cualquier otra información que pueda contribuir a aclarar en qué situaciones van a producirse los flujos de información, la indicación de la infraestructura tecnológica a utilizar, especificando si se trata de un acceso remoto, o mediante envío de soportes, o cualquier otro dato relevante.

## **TERCERA.** Cláusulas contractuales tipo

Las Decisiones de la Comisión adoptadas conforme a lo previsto en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, actualmente son las siguientes:

- Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país.
- Decisión 2002/16/CE, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del

tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE.

- Decisión 2004/915/CE , de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países.

En el caso de que la transferencia se ampare en alguna de estas Decisiones el contrato entre el exportador y el importador deberá incluir dichas cláusulas contractuales elaboradas por la Comisión, adaptadas a la situación concreta de la transferencia para la que se solicita la autorización, no limitándose a una transcripción literal sino desarrollando los ejemplos citados por las Decisiones, y en todo caso incluyendo:

- los datos identificativos del exportador e importador de los datos,
- detalles de la transferencia, en particular las categorías especiales de los datos personales,
- cláusulas de tercero beneficiario determinadas que los interesados podrán exigir al exportador e importador de los datos,
- las obligaciones del exportador de los datos,
- las obligaciones del importador de los datos,
- responsabilidad frente a daños causados a los interesados,
- mediación y jurisdicción,
- cooperación con las autoridades de control,
- legislación aplicable,
- variación del contrato, y
- obligaciones una vez finalizada la prestación del servicio.

#### **CUARTA.** Plazos de tramitación

La tramitación del procedimiento aconseja la colaboración y diligencia del solicitante. Para ello es muy conveniente conocer los trámites y plazos de éste, y contestar ante los requerimientos de la Agencia a la mayor brevedad.

En concreto, es recomendable que el responsable del fichero sea particularmente diligente en la respuesta a las alegaciones presentadas en el trámite de información pública, especialmente cuando no se vaya a plantear ninguna otra alegación por su parte. En este caso, debería dirigirse por escrito a la Agencia informando del hecho, ya que ello permite concluir el trámite y agilizar el procedimiento.

#### **QUINTA.** Binding Corporate Rules

Un modelo alternativo para cumplir con los requisitos que permiten autorizar las transferencias internacionales consiste en la fijación de reglas corporativas vinculantes o BCR (Binding Corporate Rules). Este modelo suele plantearse en el caso de grupos de compañías internacionales y posee una cierta complejidad en su tramitación.

Cuando una compañía o grupo de compañías internacionales opte por esta vía, debería previamente evaluar su conveniencia, en base a los documentos de trabajo del Grupo de Trabajo del artículo 29: WP 107, WP 108 y WP 74, por los que se exponen, respectivamente, el procedimiento de cooperación para la emisión de dictámenes comunes sobre las normas corporativas vinculantes, la lista de control para solicitar la aprobación de BCR's y la aplicación del art. 26.2 de la Directiva 95/46/CE, a las Binding Corporate Rules para las transferencias internacionales de datos.

### **3. INDICADORES DE VERIFICACIÓN DE LA SOLICITUD**

Con el fin de establecer el adecuado equilibrio entre las garantías exigibles a los solicitantes junto con la agilidad en el trámite de los expedientes de autorización de transferencias internacionales a continuación se incluye una lista con los indicadores de control que deberán tenerse en cuenta en la solicitud de autorización y que pretende servir de ayuda para establecer la existencia de un entorno de control adecuado en lo relativo al tratamiento de datos de carácter personal.

#### **ÚNICA.** Relación de indicadores de verificación de la solicitud de autorización.

Antes de proceder a solicitar una autorización de transferencia internacional de datos se recomienda verificar los siguientes extremos al objeto de agilizar la tramitación de la misma.

- ¿El exportador de datos ha presentado la solicitud expresa de autorización de las transferencias internacionales?
- ¿Se han identificado el/los ficheros a cuyos datos se refiere la transferencia internacional con la indicación de su denominación y código/s de inscripción en el RGPD?
- ¿Se ha descrito la finalidad que justifica la transferencia?
- ¿Se ha descrito las operaciones básicas de tratamiento asociadas a la finalidad de la transferencia?
- ¿Se han descrito de forma detallada los datos de carácter personal que van a ser objeto de la transferencia?
- ¿En la documentación aportada se ha hecho constar una descripción de las medidas de seguridad concretas que van a ser adoptadas por el exportador?
- ¿En la documentación aportada se ha hecho constar una descripción de las medidas de seguridad concretas que van a ser adoptadas por el importador?
- ¿Se ha aportado copia del contrato entre el exportador y el importador?
- ¿El contrato corresponde con la relación entre el exportador y el importador?
- ¿En caso de prestación de servicio, se ha acreditado el cumplimiento del marco contractual de la prestación del servicio?
- ¿Se ha aportado acreditación de los poderes de los firmantes?
- ¿Se ha indicado el grado de confidencialidad de la documentación para ser objeto de información pública?
- ¿Se ha aportado la declaración del cumplimiento del deber de informar al comité de empresa de acuerdo con el art. 4.2 de Estatuto de los Trabajadores?
- ¿Están identificados todos los participantes en las transferencias?
- ¿Pueden existir subcontrataciones que no se encuentran identificadas en el contrato?
- ¿En el contrato presentado se recogen todas las garantías establecidas en la Decisión?
- ¿Las categorías de datos incluidas en la transferencia internacional coinciden con las categorías de datos que figuran en la inscripción de los ficheros en el RGPD?
- ¿Se tiene previsto transferir datos especialmente protegidos?
- ¿Se ha incluido correctamente la cláusula de responsabilidad?

## ANEXO. MARCO NORMATIVO

### 1. Glosario

Resulta necesario aclarar la terminología más específica utilizada en relación con las transferencias internacionales:

- **Transferencia internacional de datos:** Se considera transferencia internacional de datos al tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.
- **Exportador de datos personales:** la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
- **Importador de datos personales:** la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

### 2. Marco general

El artículo 1, segundo párrafo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos, establece que *“los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1”*.

La regulación de las transferencias internacionales se contempla en los artículos 33 y 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.

A este respecto, el artículo 33.1 indica 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 de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas”.*

Por otra parte, el artículo 33.2 establece los criterios para determinar el carácter adecuado de protección al disponer, *“el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países”.*

Esta autorización sólo se verá exceptuada en los supuestos previstos en el artículo 34 de la Ley, o cuando los datos tengan como destino un Estado miembro de la Unión Europea, o perteneciente a los países que se encuentran amparados en el Acuerdo sobre el Espacio Económico Europeo, o respecto del cual la Comisión de las Comunidades Europeas haya adoptado una Decisión de adecuación conforme a la Directiva 95/46/CE.

Los supuestos previstos por el citado artículo 34 son los siguientes:

- Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
- Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- 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.

- 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.
- Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.

Por su parte, la transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia Española de Protección de Datos la competencia para verificar su cumplimiento.

Respecto a la notificación de las transferencias previstas al Registro General de Protección de Datos (RGPD), la LOPD establece que cualquier persona o entidad que pretenda efectuar una transferencia internacional de datos deberá hacerlo constar expresamente al proceder a la notificación del fichero al RGPD.

### **2.1. A países del Espacio Económico Europeo**

El envío de datos a un país del Espacio Económico Europeo aún cuando supone un movimiento internacional de datos a los efectos de aplicación de la LOPD se considera bien una cesión de datos o una prestación de servicios y está sujeta, por lo tanto, a lo dispuesto en los artículos 11, 12 y 21.

### **2.2. A países con nivel adecuado de protección**

Además de los países que conforman el Acuerdo sobre el Espacio Económico Europeo, en el que están incluidos todos los Estados Miembros de la Unión Europea, así como Liechtenstein, Islandia y Noruega, se consideran países con un nivel adecuado de protección aquellos para los que la Comisión de las Comunidades Europeas ha declarado su adecuación:

- Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza.

- Decisión 2000/520/CE de la Comisión de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro (“safe harbor”) para la protección de la vida privada, y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.
- Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense (Personal Information and Electronic Documents Act).
- Decisión 2003/490/CE, de la Comisión de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.
- Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de los datos personales en Guernsey.
- Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man.

Cuando se tiene previsto realizar una transferencia internacional de datos con destino a uno de estos países con nivel adecuado de protección, deberá comunicarse dicha transferencia a la Agencia mediante la cumplimentación del correspondiente apartado del formulario electrónico NOTA de notificación de ficheros.

### **2.3. A países que no proporcionan un nivel adecuado de protección**

La transferencia internacional de datos a un país que no proporciona un nivel de protección equiparable al que presta la LOPD sólo puede realizarse si se ha obtenido una autorización previa del Director de la Agencia, en los términos que se exponen en el apartado 3 de este documento, o bien si dicha transferencia se ampara en alguna de las excepciones previstas en el art. 34 de la LOPD.

### **2.4. Excepciones a la autorización**

En el caso de las transferencias internacionales de datos amparadas en el consentimiento del interesado se deberá tener en cuenta que para que dicho consentimiento tenga la consideración de inequívoco, tal como exige el art. 34.e) de la LOPD, será necesario que en la solicitud del mismo conste, además del destinatario de la transferencia, el país de destino, así como, la finalidad específica y determinada para la que se transfieren los datos de carácter personal.

En cualquier caso, cuando la transferencia se encuentra habilitada en cualquiera de las excepciones previstas en el citado art. 34 de la LOPD deberá comunicarse dicha transferencia a la Agencia mediante la cumplimentación del correspondiente apartado del formulario electrónico NOTA de notificación de ficheros.

## **2.5. Autorización de transferencia internacional de datos**

Cuando la transferencia internacional de datos tiene por destino un país para el que no se ha reconocido un nivel de protección equiparable y no se dan las circunstancias del art. 34, además de observarse lo dispuesto en la LOPD es preciso obtener la autorización del Director de la Agencia Española de Protección de Datos, de acuerdo con el art. 33.1 de la LOPD.

Esta autorización sólo se otorga cuando el responsable del tratamiento ofrece garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de la protección de datos de las personas, así como respecto al ejercicio de tales derechos.

Dichas garantías pueden derivarse, en particular de las cláusulas contractuales, previstas por el art. 25.2 de la Directiva 95/46/CE. En este sentido, y teniendo en cuenta el art. 26.4 de la Directiva, los Estados Miembros se encuentran vinculados por las Decisiones de la Comisión por la que se establecen las cláusulas contractuales a aplicar en los contratos de responsable a responsable y de responsable a encargado. Actualmente se encuentran publicadas tres Decisiones:

- Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país.
- Decisión 2002/16/CE, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE.
- Decisión 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países.

En este sentido, debe tenerse en cuenta que los Estados Miembros estarán vinculados por cualquier otra futura Decisión que la Comisión pueda adoptar dando cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

La Agencia Española de Protección de Datos como titular de la competencia legal para autorizar las transferencias internacionales de datos ha adoptado las medidas necesarias para ajustarse a las citadas Decisiones de la Comisión.

## **2.6. Solicitud de autorización de transferencia internacional de datos**

A continuación se detalla el procedimiento de solicitud y tramitación de una autorización de transferencia internacional de datos, acompañado de una serie de recomendaciones.

El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos se iniciará habitualmente a solicitud del exportador que pretenda llevar a cabo la transferencia.

En cualquier caso, en la solicitud ante la Agencia, el exportador deberá consignar de manera clara y precisa la finalidad, el colectivo/s de interesados y los datos objeto de la transferencia internacional, así como la identificación del fichero o ficheros afectados por la misma, y la documentación que incorpore las garantías exigibles para la obtención de la autorización, en la que conste una descripción de las medidas de seguridad concretas que van a ser adoptadas, tanto por el exportador como por el importador de los datos.

Cuando de la información aportada en el expediente, no puede deducirse los extremos antes señalados, se requiere al responsable al objeto de que aporte toda la documentación necesaria y aclare dichos puntos, al objeto de que los datos que se tenga previsto transferir sean adecuados y pertinentes en relación con la finalidad objeto la de la transferencia internacional.

La presentación de una solicitud de autorización de transferencia internacional da lugar al inicio del correspondiente expediente en el Registro General de Protección de Datos. El Registro General de Protección de Datos podrá requerir al solicitante, si la documentación no es completa o no reúne todos los requisitos formales, o bien si de la descripción de la transferencia se puede desprender alguna inconsistencia en el tratamiento de los datos, o en el cumplimiento de las garantías suficientes, al objeto de que en el plazo de 10 días practique la subsanación y mejora de la solicitud que sean necesarias de acuerdo con lo dispuesto en el art. 71.1 de la Ley 30/1992.

Si transcurrido el plazo de 10 días no se ha recibido contestación se declara archivado el expediente mediante la correspondiente resolución del Director, que el Registro General de Protección de Datos notifica al solicitante.

La tramitación del procedimiento continúa con la instrucción del mismo, en la que se analiza el detalle de la transferencia y las cuestiones de fondo en relación con las garantías aportadas. Si es preciso alguna aclaración se procede a realizar el correspondiente requerimiento de subsanación. En todo caso, el Director de la Agencia Española de Protección de Datos dicta el Acuerdo de inicio del trámite de información pública que se remite al BOE. El plazo de subsanación es de 10 días, suspendiéndose el procedimiento si transcurrido este plazo no se hubiera recibido contestación.

El periodo de información pública es de 20 días desde la publicación en el BOE, periodo durante el cual quienes lo consideren adecuado podrían tener acceso a la documentación relativa a la transferencia internacional objeto de autorización para realizar, en su caso, las alegaciones que estimen pertinentes.

Si se reciben alegaciones durante este periodo, éstas se incorporan en el expediente, y se da traslado de las mismas al solicitante iniciándose el trámite de audiencia al interesado por un plazo de 10 días.

Una vez transcurrido este plazo, o en su caso, en el momento de recibir las alegaciones que considere oportunas el interesado, y siempre antes de que transcurran tres meses desde el inicio del expediente, la Agencia dicta la correspondiente resolución motivada poniendo fin a la tramitación del expediente.

Cuando el Director de la Agencia Española de Protección de Datos resuelve autorizar la transferencia internacional de datos, se da traslado de la Resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción, notificándose al solicitante y, una vez notificada, se publica en la página web de la Agencia.

De esta Resolución de autorización o denegación de la autorización de la transferencia internacional de datos se da traslado así mismo, al **Ministerio de Justicia**, al efecto de que se proceda a su notificación a la **Comisión Europea** y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

## 2.7. Binding Corporate Rules o Reglas Corporativas Vinculantes

También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

El sistema de Binding Corporate Rules o Reglas Corporativas Vinculantes se encuentra desarrollado en los siguientes documentos de trabajo del Grupo de Autoridades Europeas de Protección de Datos (Grupo de Trabajo del artículo 29):

- WP107, de 14 de abril de 2005, por el que se expone un procedimiento de cooperación para la emisión de dictámenes comunes sobre las salvaguardas adecuadas que resultan de las normas corporativas vinculantes “Binding Corporate Rules”
- WP108, de 14 de abril de 2005, por el que se establece un modelo en forma de lista de control para solicitar la aprobación de normas corporativas vinculantes o Binding Corporate Rules
- WP 74, de 3 de junio de 2003, sobre transferencias internacionales de datos personales a terceros países: Aplicación del art. 26.2 de la Directiva 95/46/CE, a las Binding Corporate Rules para las transferencias internacionales de datos.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.