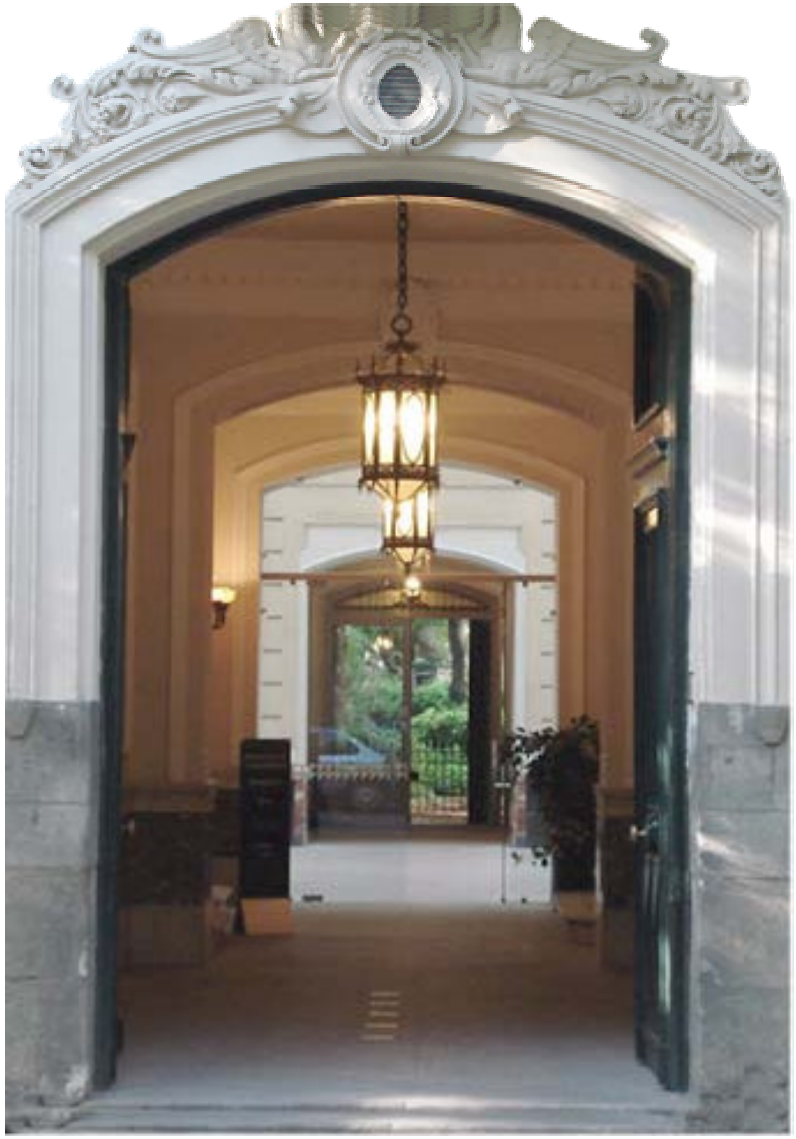
FAQ's



1ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

22 de abril de 2008

Creación e inscripción de ficheros
Transferencias internacionales
Códigos tipo
Medidas de seguridad
Inspección y potestad sancionadora.

La creación e inscripción de ficheros
Transferencias internacionales de datos
Los códigos tipo

María José Blanco Antón

Subdirectora General

Registro General de Protección de Datos

¿Cuál debe ser el contenido de la disposición general de creación, modificación o supresión de ficheros de titularidad pública?

El que determina el art. 20 LOPD y el art. 54 RDLOPD, que añade la denominación del fichero y el sistema de tratamiento. Éste último en los términos del art. 5.2.n) del RDLOPD: *"… automatizados, no automatizados o parcialmente automatizados"*

Tendrán que modificarse las disposiciones generales vigentes de creación de ficheros automatizados que sean mixtos y no se hubiese previsto esta circunstancia.

¿Qué ficheros tienen que notificarse al RGPD?

¿Los ficheros de contabilidad y facturación, los ficheros temporales?

Es OBLIGATORIA la notificación de cualquier fichero que contenga datos personales que se encuentre en el ámbito de aplicación de la LOPD

Los ficheros de contabilidad y facturación cuando sólo incluyen datos referidos a las personas previstas en los arts. 2.2 y 2.3 no tienen que inscribirse siempre que se ajusten a los términos previstos en los citados artículos: colectivos, tipos de datos y finalidades concretos.

En el caso de las personas de contacto, si incluyen datos de otros colectivos, el DNI u otro tipo de datos, … no se excluyen de la aplicación de la LOPD y por lo tanto, si tienen que ser notificados.

¿Qué ficheros tienen que notificarse al RGPD?

¿Los ficheros de contabilidad y facturación, los ficheros temporales? (cont)

Un fichero temporal creado para realizar un tratamiento ocasional a partir de un fichero existente NO tiene que inscribirse. SÍ tiene que estar inscrito el fichero de origen.

Ej. si se crea un fichero temporal para organizar las vacaciones del personal a partir del fichero de recursos humanos, tendrá que estar inscrito el fichero de recursos humanos. Respecto del fichero de vacaciones tendrán que adoptarse las medidas de seguridad correspondientes.

Un fichero creado para realizar tratamientos de datos periódicos, SI que tendrá que inscribirse. Ej. censo agrario, preinscripción anual en un polideportivo, ….

¿Cuándo hay que notificar un fichero al RGPD? ¿Supresión de los ficheros de datos de proveedores o personas de contacto? ¿Disolución de una compañía? ¿Modificación del nivel de medidas de seguridad? ¿Es posible notificar un fichero de nómina con datos de salud y nivel básico?

La inscripción en el RGPD tiene que mantenerse ACTUALIZADA

La creación de un fichero de titularidad privada tiene que notificarse con carácter previo a su puesta en marcha

Los ficheros de titularidad pública en el plazo de un mes desde la publicación de la disposición general

¿Cuándo hay que notificar un fichero al RGPD? ¿Supresión de los ficheros de datos de proveedores o personas de contacto? ¿Disolución de una compañía? ¿Modificación del nivel de medidas de seguridad? ¿Es posible notificar un fichero de nómina con datos de salud y nivel básico? (cont)

Tienen que notificarse las modificaciones que afecten a:

– Cambio de denominación social, forma societaria o de personalidad jurídica.

– Modificación del nivel de seguridad aplicable. En todo caso, concordancia entre el nivel aplicado, el exigido por el RDLOPD y el notificado.

– El fichero de nómina se puede notificar con datos de salud (grado de discapacidad – IRPF) y nivel de seguridad básico. OJO! en todo caso, se mantiene la obligación de aplicar todas las garantías exigidas para tratar datos especialmente protegidos

– Cualquier modificación del contenido de la inscripción. Ej. Sistema de tratamiento, automatizado con documentación en papel, notificar sistema mixto.

¿Cuándo hay que notificar un fichero al RGPD? ¿Supresión de los ficheros de datos de proveedores o personas de contacto? ¿Disolución de una compañía? ¿Modificación del nivel de medidas de seguridad? ¿Es posible notificar un fichero de nómina con datos de salud y nivel básico? (cont)

Tiene que notificarse la supresión de un fichero:

- –Si ha quedado excluido totalmente de la aplicación de la LOPD
- –Si cesa la actividad del responsable. Ficheros bloqueados se pueden suprimir.
- –Si desaparece la competencia o el objeto que ocasionó la creación del fichero

¿Cuándo se puede crear un fichero con varios responsables?

Sólo cuando existe habilitación o legitimación.

Debe estar articulado el protocolo de gestión del fichero (información, derechos ARCO, responsabilidades, …), el control de acceso y medidas de seguridad.

Cada responsable tiene que notificar el fichero al RGPD

Del fichero de control de visitas a un edificio que comparten varias empresas puede ser responsable la empresa de seguridad del edificio (Instrucción 1/1996, norma 2, párrafo primero).

El fichero de asuntos de un despacho colectivo de abogados no es un fichero con varios responsables. Cada profesional es responsable de sus expedientes. Control de accesos impedirá el uso de datos que no son de su competencia.

¿Qué requisitos se tienen que cumplir para realizar una transferencia internacional de datos a Bulgaria o Rumanía?

Las comunicaciones de datos en el EEE no son transferencias internacionales. Están sujetas a los requisitos de las cesiones de datos. Tienen que ser notificadas en el apartado de cesiones del formulario NOTA.

¿Una prestación de servicios desde Argentina a una empresa española, mediante el acceso a los ficheros de la compañía española ubicados en España requiere autorización del Director de la AEPD?

Es una transferencia internacional de datos. La Comisión Europea ha reconocido el nivel adecuado de protección de Argentina. Es preciso el cumplimiento previo de la LOPD. Sólo es necesaria la notificación al RGPD

¿Es obligatoria la autorización previa a una transferencia internacional de datos si ésta se realiza en ejecución de un contrato de prestación de servicios entre una empresa española, responsable del fichero, y la encargada del tratamiento, sucursal o filial de una empresa española?¿Cuánto tarda la Agencia en dar la autorización desde que se presenta correctamente la petición? ¿Habrá cambios en la documentación a presentar?

Si el destino de los datos es un país fuera del EEE requerirá autorización del Director.

Una vez solicitada la autorización acompañada de toda la documentación necesaria: poderes de representación, contrato basado en la Decisión 2002/16/CE, descripción detallada …. el plazo de tramitación es de 3 meses.

En las recomendaciones de la AEPD publicadas en el informe de transferencias internacionales (julio-2006) www.agpd.es se indica la documentación a presentar

¿Es obligatoria la autorización previa a una transferencia internacional de datos si ésta se realiza en ejecución de un contrato de prestación de servicios entre una empresa española, responsable del fichero, y la encargada del tratamiento, sucursal o filial de una empresa española?¿Cuánto tarda la Agencia en dar la autorización desde que se presenta correctamente la petición? ¿Habrá cambios en la documentación a presentar?

Si el destino de los datos es un país fuera del EEE requerirá autorización del Director.

Una vez solicitada la autorización acompañada de toda la documentación necesaria: poderes de representación, contrato basado en la Decisión 2002/16/CE, descripción detallada …. el plazo de tramitación es de 3 meses.

En las recomendaciones de la AEPD publicadas en el informe de transferencias internacionales (julio-2006) www.agpd.es se indica la documentación a presentar

Tras la aprobación del RDLOPD, ¿sigue igual el régimen de transferencias internacionales de datos y los grupos de empresas?

El régimen de transferencias internacionales de datos no se ha modificado.

El RDLOPD permite la autorización de estas transferencias internacionales de datos entre las diferentes empresas del grupo cuando el grupo tiene aprobado un sistema de BCR´s

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Las medidas de seguridad

Ricard Martínez Martínez.
Coordinador del Área de Estudios

¿Cuándo se aplica el nivel básico de seguridad a datos de salud?

- **Sólo en los casos previstos por el RDLOPD.**
  - **Cumplimiento de deberes públicos:**
    - **porcentaje de discapacidad**
    - **discapacidad si/no**
    - **apto/no apto**
    - **invalidez**
    - **incapacidad laboral (si/no, fecha)**
    - **enfermedad común, accidente laboral, enfermedad profesional.**

¿Cuándo se aplica el nivel básico de seguridad a datos de salud?

- **Si se aplica el nivel básico éste se proyecta sobre todas las medidas.**

- **Si se describe la enfermedad o situación de salud concreta que la causa, o se incluye un código numérico que permita establecerla: NIVEL ALTO**

¿Cuándo se aplica el nivel básico a datos de ideología, afiliación sindical o creencias?

- Únicamente en el caso previsto por el RDLOPD: realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros
  - detracción de cuota sindical
  - domiciliaciones bancarias

¿Cuándo se aplica el nivel básico a datos de ideología, afiliación sindical o creencias?

- **Nivel Alto:**
  - **asociación religiosa, partido o sindicato respecto de sus afiliados, socios o miembros**

¿Cuándo se aplica el nivel básico a datos de ideología, afiliación sindical o creencias?

- Tratamiento de datos en confección de la Declaración del IRPF (Iglesia Católica, donaciones a determinadas fundaciones):
  - nivel básico
  - no suponen necesariamente la adscripción política o religiosa del contribuyente

¿Qué se entiende por ficheros o tratamientos no automatizados en los que de forma accidental o accesoria se contengan datos especialmente protegidos?

- La finalidad del fichero no debe ser tratar este tipo de datos personales.
- El responsable no debe haber solicitado al titular este tipo de datos.
- Generalmente será el titular de los datos personales u otro sujeto quién sin haber requerido el dato lo aporte.

¿Qué se entiende por ficheros o tratamientos no automatizados en los que de forma accidental o accesoria se contengan datos especialmente protegidos?

- **Caso concreto: inclusión de un dato de salud incluido en un "parte de baja":**
  - **deber de formalizar el documento conforme a la ordenación vigente**
  - **no inclusión del documento en el fichero**

¿Qué nivel de seguridad debo aplicar?

- **Aplicación del nivel medio a Entidades Gestoras y Servicios Comunes de la Seguridad Social: únicamente en relación con el ejercicio de sus competencias en materia de recaudación.**

¿Qué nivel de seguridad debo aplicar?

- **Abogados, servicios sociales y/o profesionales que utilicen documentos o datos sobre violencia de género u otros asuntos de los que conozcan que incluyan datos especialmente protegidos:**
  - **no incidentalidad o accesoriedad**
  - **finalidad**
  - **nivel alto**
  - **no excepción en el caso de abogados de oficio**

¿Qué obligaciones de seguridad deben imponerse al encargado del tratamiento ?

- Precisión en la definición de las medidas.
- Contenido del documento de seguridad: flexibilidad.
  - Pueden existir documentos diferenciados por encargo
  - Identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

¿Qué obligaciones de seguridad deben imponerse al encargado del tratamiento ?

- Obligaciones de su personal.
- La delegación de la llevanza del documento de seguridad en el encargado:
  - debe cumplir con los requisitos del RDLOPD.
  - no exime el disponer de un documento propio del responsable respecto de los tratamientos que él realice materialmente.

¿En las prestaciones sin acceso a datos existen obligaciones de seguridad?

- Cualquier actividad que suponga un contacto directo o indirecto con el sistema de información y/o su entorno físico o lógico puede ser susceptible de poner en riesgo la seguridad de los datos:
  - limpieza
  - seguridad
  - mantenimiento o reparación de instalaciones (que no se refiera al propio sistema de información)

¿En las prestaciones sin acceso a datos existen obligaciones de seguridad?

- Incluye servicios de destrucción o almacenamiento de soportes cuando el prestador desconozca el criterio de archivo o no pueda recuperar dato alguno .

¿Qué permite la delegación de autorizaciones?

- Se trata de una posibilidad que permite flexibilizar la gestión de la seguridad.
- Habilita al responsable para delegar en otros usuarios de la organización las funciones y atribuciones establecidas para él en el Reglamento.
- No le exime de responsabilidad.

¿Qué debo hacer para documentar y/o notificar las funciones y obligaciones del personal?

- El responsable debe definirlas teniendo en cuenta los perfiles de usuario para lograr los objetivos del Reglamento.

- Deben anotarse en el documento de seguridad.

¿Qué debo hacer para documentar y/o notificar las funciones y obligaciones del personal?

- ¿Como informar al personal?
  - Lenguaje comprensible
  - Cualquier medio disponible
    - notificación
    - escrito
    - inicio del programa como pantalla de paso obligatorio
    - intranet corporativa

¿Cuál es el alcance de la obligación de anotar las salidas de soportes mediante correo electrónico?
¿Y si es un fax?

- **Correo electrónico:**
  - **el envío deberá incluir en su cuerpo o adjuntos datos de un fichero o tratamiento**
  - **no afecta al uso del correo "para escribir cartas"**
- **El propio sistema de indexación del gestor del correo-e puede servir como registro.**

¿Cuál es el alcance de la obligación de anotar las salidas de soportes mediante correo electrónico?
¿Y si es un fax?

- Afecta a cualquier otro procedimiento electrónico como ftp, descargas desde web o carpetas compartidas etc.

- Afecta al envío de faxes cuando incorporan datos de un fichero o tratamiento.

¿Debe registrarse la salida de soportes con destino a otra sede de la entidad? ¿Y a la del encargado?

- **Deben anotarse tanto en uno como en el otro caso ya que se trata de garantizar la trazabilidad de datos que salen materialmente del sistema de información.**

¿Qué significa guardar las copias de respaldo en lugar físico diferente?

- Concepto de lugar físico diferente:
  - Es preferible que se trate de un espacio físico diferenciado en el que no se den los mismos riesgos físicos que en de ubicación del SI (por ej. incendio o inundación).
  - Sería admisible un espacio distinto en la misma sede cuando:
    - Se justifique en el documento de seguridad.
    - Se adopten medidas complementarias para minimizar el riesgo (ubicación de la copia, armarios ignífugos o sistemas anti-incendio etc.)

¿Qué significa guardar las copias de respaldo en lugar físico diferente?

- No aplicable en ficheros no automatizados. No debe confundirse la copia de respaldo con la "copia de trabajo" a la que se hace referencia al regular la seguridad de los ficheros no automatizados.

¿La auditoria es LOPD? ¿quién debe realizarla? ¿debe notificarse?

- No se establece una auditoria LOPD. Sin perjuicio de que cuando alguna de las materias reguladas por la misma se proyecten sobre la seguridad deban ser tenidas en cuenta:
  - encargado
  - comunicaciones de datos que impliquen salidas de soportes

¿La auditoria es LOPD? ¿quién debe realizarla? ¿debe notificarse?

- **No se define o reconoce el perfil funcional o profesional de los auditores.**
- **No debe remitirse a la Agencia.**

¿Cuál debe ser el alcance del registro de accesos?

- Existe exención del mismo cuando se den los requisitos del Reglamento:
  - el responsable debe ser una persona física.
  - el responsable debe ser el único usuario.

¿Cuál debe ser el alcance del registro de accesos?

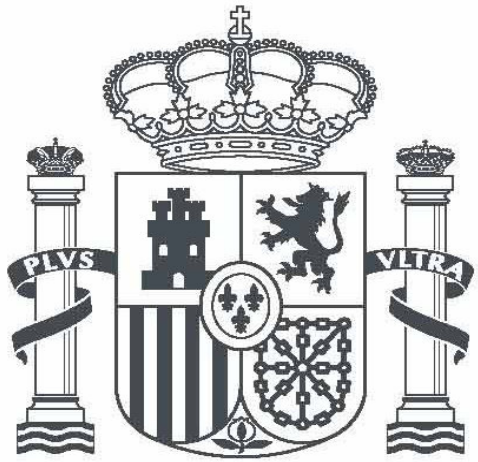
- ¿Cuál es su grado de trazabilidad en cuanto a la información que permita la identificación del Registro accedido en relación con los cambios realizados?
  - Debe guardarse la información necesaria para identificar el registro accedido y el hecho de su modificación sin que alcance al contenido concreto del mismo.

¿Cómo aplico el control de acceso a los documentos del nivel alto?

Mediante cualquier sistema o dispositivo disponible:

- **Utilización de plantillas básicas en soporte papel incorporadas al inicio del expediente.**
- **Registros automatizados en la gestión de entradas y salidas al archivo.**
- **Sistemas de trazabilidad.**

AGENCIA ESPAÑOLA DE **PROTECCIÓN DE DATOS**



Inspección y potestad sancionadora

José López Calvo
Subdirector General de Inspección

Inspección y potestad sancionadora

¿Por qué norma se regirán los procedimientos y actuaciones previas iniciadas antes de la entrada en vigor del nuevo reglamento? En caso de procedimientos incoados ahora ¿se va a aplicar el nuevo Reglamento?

La aplicación del nuevo reglamento queda regulada en sus disposiciones transitorias.

El reglamento se aplicará en plenitud a las denuncias que se presenten a partir de su entrada en vigor el 19 de abril y que se refieran a hechos producidos a partir de esa fecha.

Con carácter general el Reglamento ha recogido criterios sostenidos en procedimientos anteriores por lo que no debe producirse un cambio sustancial.

¿Qué consecuencias derivan de las declaraciones de infracción a las Administraciones Públicas?

Las consecuencias de la declaración de infracción son entre otras:

- Publicación de la infracción.

- Comunicación al Defensor del Pueblo.

- Posible derivación de un expediente disciplinario al funcionario responsable.

Inspección y potestad sancionadora

En caso de falta de compromiso por parte de los empleados de un responsable en el cumplimiento de medidas de seguridad. ¿Cómo se dilucida la responsabilidad de la empresa y del empleado?

La responsabilidad final no recae sobre la persona física sino sobre el responsable. Son múltiples los casos en los que se produce una vulneración por una actuación personal por lo que debe hacerse un importante esfuerzo formativo y de concienciación. Ejemplos:

- **secreto (ficheros P2P, documentación en vía pública).**
- **acceso a datos de salud por personas no habilitadas.**
- **contratación fraudulenta. Agentes comerciales. (SAN 25-4-2007).**
- **información a ex-cónyuge.**

¿Ha pensado la agencia publicar en la web junto a la sanción impuesta a una empresa el nombre del proveedor que realiza la adaptación?

El artículo 82 de la ley 62/2003 de 30 de diciembre prevé la publicación anonimizada de las resoluciones una vez notificadas. No se realiza previsión alguna respecto a los proveedores que realizan la adaptación.

Posibilidad de ejercer actuaciones de reclamación en el ámbito privado.

¿Cómo puede diferenciarse, con respecto a las sanciones, cuando se es una persona física o persona jurídica en cuanto a la cuantía de dicha sanción o si se diferencia por la gravedad de ésta?

Entre los elementos que se consideran para aplicar los elementos de ponderación del art. 45.4 y 5 de la LOPD se encuentra el hecho de que se trate de un sujeto que gestione gran cantidad de datos, aislado y puntual.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS