

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



GUÍA

La protección
de datos en las
relaciones laborales

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



ÍNDICE **GUÍA**

**La protección
de datos en las
relaciones laborales**

1 PRESENTACIÓN

2 CUESTIONES GENERALES

- 2 ■ SUPUESTOS DE NO APLICACIÓN DE LA LOPD
- 3 ■ INSCRIPCIÓN DE FICHEROS
- 6 ■ CRITERIOS DE CANCELACIÓN Y BLOQUEO DE LOS DATOS

8 RECURSOS HUMANOS.

- 8 ■ INFORMACIÓN SOBRE EL TRATAMIENTO DE LOS DATOS PERSONALES. MODALIDADES:
- 9 ■ En procedimientos de selección de personal
- 10 ■ En la contratación
- 11 ■ Durante el desarrollo de la prestación laboral
- 11 ■ En las relaciones con los representantes sindicales
- 12 ■ CONSIDERACIÓN DE LOS DATOS ESPECIALMENTE PROTEGIDOS
- 13 ■ SISTEMAS INTERNOS DE DENUNCIAS O “WHISTLEBLOWING”
- 16 ■ CONTRATACIÓN DE SEGUROS DE VIDA Y PLANES DE PENSIONES
- 18 ■ EXTERNALIZACIÓN DE LA GESTIÓN DE LAS NÓMINAS

20 LA PREVENCIÓN DE RIESGOS LABORALES

- 20 ■ El consentimiento en la prevención de riesgos
- 21 ■ Los protagonistas de la prevención de riesgos
- 23 ■ El acceso a los datos por la empresa y los delegados de prevención

26 CONTROLES EMPRESARIALES

- 26 ■ Controles basados en el uso de tecnologías de la información
- 29 ■ Controles sobre el absentismo laboral

32 RELACIONES CON LOS SINDICATOS. COMUNICACIONES DE DATOS, TABLONES, CENSOS.

- 32 ■ Publicaciones de datos personales en tablones
- 34 ■ Cesiones de datos personales a los sindicatos
- 36 ■ Cesiones de datos contenidos en documentos TC2
- 38 ■ Entrega de TC2 al comité de empresa
- 39 ■ Cesión de nóminas y TC2 de los trabajadores de subcontratas a las empresas contratistas

41 DEBERES DE LOS TRABAJADORES QUE ACCEDEN A DATOS PERSONALES: SECRETO Y SEGURIDAD

44 RECURSOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



Presentación

La Agencia Española de Protección de Datos ha publicado distintas guías con el objetivo de promover la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD)

Uno de los principales objetivos de estas publicaciones ha sido ofrecer herramientas de ayuda a las organizaciones, públicas o privadas, para un adecuado cumplimiento de la legalidad vigente. Éstas guías se han planteado abordando cuestiones de carácter general, como en la Guía del Responsable, o de modo específico como en la Guía de Seguridad de datos o la Guía de Videovigilancia.

La Guía sobre protección de datos en las relaciones laborales plantea un nuevo enfoque. Se trata de examinar aspectos de la protección de datos que, o bien resultan fundamentales desde el punto de vista de la aplicación y el cumplimiento normativo, o bien han planteado dificultades de interpretación o aplicación práctica. Por ello, a diferencia de publicaciones anteriores, la Guía de Protección de datos en la empresa se plantea como objetivo considerar un conjunto de aspectos prácticos a los que las empresas deben enfrentarse habitualmente.

Por otra parte, tras prácticamente 10 años de vigencia de la LOPD y con un Reglamento de Desarrollo ampliamente publicitado, las empresas y las administraciones deben comenzar a adquirir la madurez suficiente que facilite un adecuado cumplimiento de la Ley. En estos momentos ya no se trata de adaptar las estructuras a una nueva norma sino de incorporar la protección de datos a la cultura empresarial y al diseño, organización y funcionamiento de las organizaciones. En esta tarea, disponer de información práctica ha sido una necesidad sentida de la pequeña y mediana empresa a la que se quiere atender especialmente.

Durante su trayectoria la Agencia Española de Protección de Datos ha atesorado un gran número de experiencias que plasmadas en los distintos epígrafes de esta Guía pueden servir para orientar en el cumplimiento de la normativa.



Gestión de Personal

■ SUPUESTOS DE NO APLICACIÓN DE LA LOPD

Una de las novedades que incorpora el Reglamento de desarrollo de la Ley Orgánica de protección de datos es la exclusión, bajo ciertas condiciones, de su aplicación a los datos de las definidas como “personas de contacto”.

«Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. (art.2.2 RDLOPD)».

En ningún caso esta exclusión supone no aplicar la LOPD a los ficheros de personal. El Reglamento plantea una excepción a la aplicación de las normas que garantizan el derecho a la protección de datos y por ello debe interpretarse en sentido estricto y de modo restrictivo. Para ello deben cumplirse varios requisitos:

- Que los datos tratados se limiten efectivamente a los meramente necesarios para identificar al sujeto en la persona jurídica a la que presta sus servicios. Cualquier tratamiento que contenga datos adicionales a los citados se encontrará plenamente sometido a la LOPD.

«Por ello, no se encontrarían excluidos de la Ley los ficheros en los que, por ejemplo, se incluyera el dato del documento nacional de identidad del sujeto, al no ser el mismo necesario para el mantenimiento del contacto empresarial. Igualmente, y por razones obvias, nunca podrá considerarse que se encuentran excluidos de la Ley Orgánica los

ficheros del empresario respecto de su propio personal, en que la finalidad no será el mero contacto, sino el ejercicio de las potestades de organización y dirección que a aquél atribuyen las leyes. (Informe 78/2008)»

- La finalidad del tratamiento debe perseguir una relación directa entre quienes traten el dato y la entidad y no entre aquéllos y quien ostente una determinada posición en la empresa. De este modo, el uso del dato debería dirigirse a la persona jurídica, siendo el dato del sujeto únicamente el medio para lograr esa finalidad.

«Así sucedería en caso de que el tratamiento responda a relaciones “business to business”, de modo que las comunicaciones dirigidas a la empresa, simplemente, incorporen el nombre de la persona como medio de representar gráficamente el destinatario de la misma. (Informe 78/2008)»

- Todo lo anterior no afecta en absoluto a las previsiones de la LSSIyCE de modo que los principios que rigen el envío de comunicaciones comerciales por medios electrónicos se aplican tanto a personas físicas como jurídicas, y entre ellas, las personas de contacto.

■ INSCRIPCIÓN DE FICHEROS

Coloquialmente se identifica el concepto de “fichero” o “base de datos” con los programas existentes que ofrecen ese tipo de prestación. Sin embargo la definición legal es mucho más amplia y desborda esta clase de software. Por tanto, el objeto al que se aplica la LOPD no se identifica con un programa informático determinado.

«k. Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. (art. 5 RDLOPD)».

Para que se trate de un fichero sujeto a la LOPD debe permitir el acceso a los datos «con arreglo a criterios determinados», por tanto debe contar con algún criterio de ordenación que permita recuperar datos de una persona determinada.

Ej. Apellidos nombre, número o código de cliente o factura, fecha, domicilio, teléfono...

El concepto de fichero no sólo se aplica a programas informáticos. La LOPD se aplica a los datos personales incluidos en soportes no informáticos cuando puedan ser objeto de tratamiento.

«Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica. (Art. 5.1.n) RDLOP»

Ej. Archivos organizados en soporte papel como historias clínicas, currículums, facturas. Grabaciones analógicas de audio o video de un sistema de videovigilancia. Negativos fotográficos.

El elemento determinante para identificar un fichero o un tratamiento no automatizado sometido a la legislación sobre protección de datos reside en que se trate de información estructurada en la que resulte posible recuperar los registros relativos a un individuo determinado.

«todo fichero de datos exige para tener esta consideración una estructura u organización con arreglo a criterios determinados. El mero acúmulo de datos sin criterio alguno no podrá tener la consideración de fichero a los efectos de la ley.

(...)

Es claro para este Tribunal que registro en soporte físico equivale a fichero en los términos de la ley. Basta la lectura completa de este artículo 2 y su comparación con el art. 3 de la Directiva del que trae causa, y que sirve para interpretarlo, para llegar a esa conclusión.

Pues bien, para que una actuación manual sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo...) tenga la consideración de "tratamiento de datos personales" sujeto al sistema de protección de la Ley Orgánica 15/1999 es necesario que dichos datos estén contenidos o destinados a ser incluidos en un fichero, esto es, en un conjunto estructurado u organizados de datos con arreglo a criterios determinados. Si no es así, el tratamiento manual de datos personales quedará fuera del ámbito de aplicación de la ley, no será un "tratamiento de datos personales" según el concepto normativo que la ley proporciona.

En realidad la existencia del "fichero" en el sentido legal es siempre precisa para que un tratamiento de datos personales esté sujeto al sistema de protección de la ley. En los casos de tratamiento automatizado de datos -siempre sometidos a la ley- es difícil imaginar la inexistencia de un fichero (aunque no se exija expresamente) puesto que los datos que se tratan mediante sistemas automatizados lo son siempre bajo unos criterios de estructura u organización previa. (Sentencia de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 16 de febrero de 2006)»

La LOPD establece el deber de notificar los ficheros:

«1) Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

(...)

3) Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación. (art. 26 LOPD)»

El sentido común suele identificar la existencia de un fichero sujeto a la LOPD cuando se utiliza un gestor de bases de datos, y en cambio considera que no existe cuando los datos se tratan con un procesador de textos. Sin embargo, aunque no se utilice una base de datos, puede existir un fichero objeto de inscripción.

Ej, 1) Una lista de clientes en un documento de un procesador de textos, “.pdf” etc. 2) La agenda de contactos profesionales en nuestro sistema de correo electrónico; 3) Los negativos fotográficos o las fotografías digitales cuando se identifica al cliente.

Por otra parte, también se suele identificar cada fichero con un único recurso. Sin embargo. La realidad es mucho más compleja. Un fichero puede incluir recursos objeto de tratamiento automatizado y no automatizado.

«1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.(art. 56 RDLOPD)»

Puede existir un mismo fichero en distintos ordenadores.

«de lo establecido en la Directiva y en la propia Ley Orgánica parece desprenderse que el concepto de fichero no va directamente vinculado a la exigencia de que el mismo se encuentre en una única ubicación, sino que será posible la existencia de ficheros distribuidos en lugares geográficos remotos entre sí, siempre y cuando la organización y sistematización de los datos responda a un conjunto organizado y uniformado de datos, sometido a algún tipo de gestión centralizada. [Informe 368/2003](#) ».

Podríamos considerar la existencia de un único fichero a efectos de inscripción en aquellos casos en los que quepa reconducirlos a una unidad en términos lógicos, por ejemplo, por estar ordenados a una misma finalidad.

Ej. La inscripción del fichero de recursos humanos puede incluir el software que se utiliza para la gestión de nóminas, los currículos que se gestionan en proceso de selección y las carpetas en los que se ordenan documentos como los TC2.

Debe señalarse que se inscriben los ficheros, pero no los tratamientos.

Ej. Los sistemas de videovigilancia en los que no se graba deben cumplir con las normas de protección de datos personales, salvo el deber de inscripción.

La Agencia Española de Protección de Datos dispone en su website de un sistema para la inscripción de ficheros denominado NOTA, que facilita por medio de modelos predefinidos la inscripción de los ficheros más comunes como los de personal o clientes.

■ CRITERIOS DE CANCELACIÓN Y BLOQUEO DE LOS DATOS

Cuando cesa la finalidad o cuando motivada y justificadamente se solicita por el afectado hay que proceder a cancelar los datos. La cancelación se da en dos etapas, la primera de las cuales es el bloqueo:

«Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos. (art. 5.b)»

Ello obliga a disponer de procedimientos de cancelación que contemplen el periodo de bloqueo. Para ello, debe tenerse en cuenta:

- Debe delimitarse el periodo de uso o conservación de los datos y el momento en el que cesa la finalidad o el hecho que legitimó su tratamiento.

Ej. Si un trabajador cesa en su relación laboral este hecho podría definir el momento en que se inicia el bloqueo de sus datos.

- Para definir el periodo de bloqueo se deberá tener en cuenta el Derecho aplicable ya que en el se encontrarán criterios de delimitación del mismo.

Ej. Las obligaciones tributarias prescriben a los 4 años. Por tanto, los datos relativos a las retenciones practicadas a un trabajador deberían bloquearse por un periodo de 4 años a partir de la fecha límite para presentar la declaración de cada ejercicio.

Cuando éste plazo no exista, o cuando sea inferior a un año se tendrán en cuenta los plazos de prescripción de las infracciones a la LOPD que, en el caso de las muy graves es de tres años.

- Debe impedirse la manipulación o alteración de los datos. En la práctica los datos permanecerán “congelados” e inaccesibles a los usuarios. La única acción posible será su puesta a disposición de las autoridades competentes.



Recursos Humanos

La gestión del personal plantea muy distintos interrogantes especialmente en lo relativo a los procesos de captación y uso de su información.

■ INFORMACIÓN SOBRE EL TRATAMIENTO DE LOS DATOS PERSONALES. MODALIDADES:

El deber de información del art. 5 LOPD forma parte del contenido esencial del derecho a la protección de datos. Este carácter esencial lo posee tanto en el caso de la recogida de los datos personales para un tratamiento que requiera consentimiento como en el supuesto de que no lo requiera.

«El artículo 5 de la Ley Orgánica 15/1999 viene a establecer un deber impuesto en general a los responsables de los tratamientos, de tal suerte que, en principio, será necesario informar al afectado del tratamiento de sus datos de carácter personal, tanto en los supuestos en que el mismo cuenta con el consentimiento del mismo como en los casos en que el tratamiento se encuentra habilitado por otras causas admitidas por el artículo 6 de la propia Ley. (Informe 60/2004)»

En el primer caso porque el consentimiento además de previo, libre y específico, debe ser informado por lo que la ausencia de información vicia la declaración de voluntad del afectado o interesado. Pero además, el contenido de la información que define el art. 5 LOPD constituye una garantía para los derechos del afectado ya que le permite conocer ante quién podrá ejercerlos.

«1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

- b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b, c y d del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban».

En el ámbito de la gestión de personal las organizaciones deben ser particularmente cuidadosas tanto en el procedimiento que se escoja para la información como en el momento en el que se proceda a la captación de datos personales.

EN PROCEDIMIENTOS DE SELECCIÓN DE PERSONAL

El primer tratamiento de datos personales puede producirse cuando el futuro trabajador sea un simple candidato a un puesto. Para ello deben tenerse en cuenta algunas cautelas:

- Es conveniente, cuando los recursos lo permitan, disponer de impresos de modelos de impresos tipo para la formalización del currículum y de un procedimiento de formalización y entrega de los mismos por los candidatos, ya que ello permite no sólo informar adecuadamente sino definir con precisión el tipo de datos a tratar, establecer las medidas de seguridad etc.
- Si para la selección de personal se realiza algún tipo de anuncio o convocatoria pública debería incluirse en ella la información del art. 5 LOPD.

- Si el currículum se presenta directamente por el candidato sin habersele solicitado deben fijarse procedimientos de información que supongan algún acuse o confirmación de conocer las condiciones en las que se desarrollará el tratamiento.

Ej. Si el currículum se remitió por correo postal o electrónico y se cuenta con una dirección electrónica facilitada por el propio interesado puede remitírsele información por ese medio solicitando confirmación de la recepción y condicionando el tratamiento de los datos al acuse de recibo.

Si se presentó en un mostrador u oficina de atención debería ser informado allí por cualquier medio que acredite el cumplimiento de este deber como por ejemplo carteles, documentos de acuse de recibo y en general cualquier medio que garantice y permita probar el cumplimiento del deber de información.

No debe olvidarse que el Reglamento de desarrollo de la Ley Orgánica de protección de datos indica que el deber de información deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

- En casos de grupos de empresas o de cualquier otra fórmula de colaboración empresarial debe tenerse en cuenta que la cesión de los datos contenidos en el currículum, o del propio documento debe contar con el consentimiento del candidato ([PS/00239/2007](#)).

EN LA CONTRATACIÓN

El contrato de trabajo es un medio adecuado para informar al trabajador respecto del tratamiento que se realizará respecto de sus datos. No obstante:

- No debe confundirse la información con la manifestación del consentimiento. Por ello, el contrato de trabajo constituye un medio adecuado para ofrecer información sobre los tratamientos directamente relacionados con la prestación laboral. No así para otros tratamientos.

Ej. Una empresa formaliza un convenio gracias al cual el trabajador obtiene ventajas para ciertas compras pero requiere que la primera le confirme la identidad del beneficiario. Tratándose de decisiones de consumo ajenas a la relación contractual, el contrato de trabajo resulta un instrumento ineficaz para obtener el consentimiento.

- No exime del deber información sobre todos aquellos nuevos tratamientos de datos personales que la empresa decida realizar con carácter posterior al nacimiento de la relación laboral.

DURANTE EL DESARROLLO DE LA PRESTACIÓN LABORAL

Las relaciones laborales son dinámicas y pueden estar sujetas a cambios sobrevenidos tanto desde el punto de vista del trabajador como desde la perspectiva de la empresa.

Ej. Un trabajador que inicialmente no se acogió a la posibilidad de descontar de su nómina la cuota sindical se afilia y lo solicita.

La empresa instala un nuevo sistema de control de presencia basado en el uso de instalaciones de videovigilancia.

Por ello será necesario informar al trabajador en todos aquellos casos en los que se produzcan cambios que afecten al tratamiento de los datos personales como la aparición de nuevas finalidades o de nuevos tratamientos.

EN LAS RELACIONES CON LOS REPRESENTANTES SINDICALES

En principio el deber de información del art. 5 LOPD tiene como destinatario al afectado o interesado.

“Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento”.art.5 RDLOPD

No obstante, en aquellos tratamientos que repercuten sobre el conjunto de los trabajadores resulta muy recomendable informar con carácter previo a la representación de éstos ya que facilita el conocimiento y la comprensión general de los mismos.

Ej. Esta necesidad se manifiesta de modo particular en el caso del desarrollo de controles empresariales, como la videovigilancia, los controles sobre la navegación en internet, o el uso de controles biométricos para registrar la entrada, salida o presencia en el puesto.

■ CONSIDERACIÓN DE LOS DATOS ESPECIALMENTE PROTEGIDOS

El art. 7 LOPD establece distintas categorías de datos especialmente protegidos:

1. Los datos sobre ideología, religión o creencias en los que cuando se recabe el consentimiento deberá advertirse del derecho a no prestarlo.

En el caso de estos datos y los relativos a la afiliación sindical el consentimiento será expreso y escrito salvo que se trate de una organización, -partido político, sindicato o entidad religiosa-respecto de sus miembros.

2. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

Se trata de datos que bien por su naturaleza religiosa o ideológica, bien por pertenecer al núcleo más íntimo de la persona resultan merecedores de una especial protección. Lo que obliga a disponer de procedimientos que garanticen:

- Una adecuada información en la recogida de los datos ya que aquí se acentúa la importancia del cumplimiento de este deber.

«En consecuencia, la posibilidad de admitir un consentimiento expreso que no conste por escrito para el tratamiento de los datos de salud, se encuentra condicionada a que pueda acreditarse que es una manifestación de voluntad libre, inequívoca y específica, que se presta una vez que se ha tenido conocimiento de una concreta información entre la que, necesariamente, ha de constar la finalidad determinada, explícita y legítima del tratamiento que se va a realizar sobre los datos personales del afectado. Lógicamente, la concurrencia de los extremos expuestos deberá constatarse en cada caso concreto. (PS/00029/2004 PS/00525/2007)»

- Antes de recabar este tipo de datos es necesario analizar la proporcionalidad del tratamiento y la legitimación para el mismo.

Ej. Como más adelante se examina, para la adaptación de un puesto de trabajo es posible que deban conocerse algunos datos de salud, o que estos se deduzcan de la adaptación propuesta. Pero ello no legitima al empresario para

incorporar y tratar los datos de salud en sus sistemas de información salvo que cuente con un servicio de prevención de riesgos laborales propio o un servicio médico de empresa. En estos últimos casos se gestionarán historias clínicas laborales, aunque el empresario y los responsables de gestión de personal tan sólo podrán conocer datos del tipo apto/no apto y las adaptaciones propuestas.

- El tratamiento de este tipo de datos se proyecta sobre la organización ya que exige adoptar medidas de seguridad de nivel alto, salvo en las excepciones previstas por el Reglamento de desarrollo de la Ley Orgánica de protección de datos. No obstante, debe recordarse que la normativa permite adaptar las medidas a la estructura real del sistema de información.

«8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad. (Art. 81 RDLOPD)»

■ SISTEMAS INTERNOS DE DENUNCIAS O “WHISTLEBLOWING”

Estos sistemas se suelen configurar mediante la creación de buzones internos a través de los cuales los empleados de la compañía, generalmente mediante un procedimiento online, ponen de manifiesto la existencia de conductas contrarias a la Ley o a las normas internas de conducta de la empresa, llevadas a cabo por empleados o auditores de las empresas.

Ej.: Los empleados pueden denunciar mediante estos sistemas conductas a través de las cuales se “soborna” a los auditores para que maquillen las cuentas de una empresa o aquellas en que un directivo de la firma facilita información reservada a terceros.

El establecimiento de estos sistemas podría ser conforme a las normas de protección de datos, pero para ello es necesario que se adecúen a los principios establecidos en esta normativa.

- La información reviste en este caso un carácter primordial. Tanto los denunciante como los potenciales denunciados deberán haber sido informados previamente de la existencia de estos

sistemas, del tratamiento de los datos que conlleva la formulación de una denuncia y de las consecuencias que para el denunciado puede comportar este hecho.

Así, podrá informarse en el contrato de trabajo o establecer este deber de información cuando se contrate un servicio externalizado, como una auditoría, y quepa la denuncia respecto de los contratados. Otra posibilidad es la de dirigir circulares informativas al personal y a su representación informando de la existencia y finalidad de un tratamiento de datos relacionado con estos buzones o sistemas de denuncias.

- Si los datos contenidos en los sistemas de denuncias fueran a ser transmitidos a una tercera compañía que investigue el hecho denunciado, se producirá una cesión de datos de la que el interesado, tanto el denunciante como el denunciado, deberá ser debidamente informado. Esta misma información deberá referirse, en su caso, a la posible transferencia internacional de datos a otras empresas del Grupo.

Ej.: Las denuncias sobre vulneración de las normas de protección de datos son transmitidas al “Chief Privacy Officer” que se encuentra en la matriz del Grupo en Japón.

- En todo caso, la existencia de estos buzones debería respetar el principio de proporcionalidad, de forma que las denuncias se refieran únicamente a supuestos en que los hechos o actuaciones tengan una efectiva implicación en la relación entre la empresa y el denunciado, concretando así que acciones deberán ser objeto de denuncia y especificando las normas legales o contenidas en códigos internos de conducta a las que las denuncias podrán referirse.

Ej.: En sistemas referidos al persona sería necesario que los buzones de denuncias se refiriesen a actuaciones que puedan, en la práctica llevar a una situación de sanción al trabajador o empleado o a la resolución de su contrato.

- Para garantizar la exactitud de la información deberían establecerse mecanismos que garanticen únicamente la aceptación de las denuncias en que el denunciante aparezca claramente identificado, no siendo adecuado establecer sistemas de denuncias anónimas. En todo caso, la confidencialidad de la información del denunciante debería quedar a salvo, no facilitándose, como regla general, su identificación al denunciado.
- Precisamente como consecuencia de lo anterior, será necesario que se extremen en relación con estos tratamientos las medidas que garanticen la adecuada seguridad y confidencialidad de la

información, pudiendo establecerse medidas reforzadas de seguridad y extremando las caute-
las que garanticen el cumplimiento del deber de secreto.

Ej.: Pueden adoptarse medidas como: 1) limitar el acceso al contenido de las denuncias a los usuarios que lleven a cabo la investigación y relacionarlos en el documento de seguridad; 2) establecer de un sistema de registro de accesos, aún cuando no corresponda aplicar las medidas de nivel alto del RLOPD; 3) firma de compromisos reforzados de confidencialidad con los usuarios autorizados, con especiales medidas disuasorias para el caso de vulnerarse el deber de secreto.

- La conservación del dato debería limitarse al tiempo necesario para la investigación de los hechos y sólo en caso de que de aquélla se desprenda la adopción de determinadas medidas contra el denunciado sería posible conservar los datos por un plazo superior, debiendo eliminarse en caso contrario.

Ej.: En caso de que la investigación de la denuncia contra un directivo pueda dar lugar a un procedimiento de despedido o a la exigencia de responsabilidades civiles sí será posible conservar los datos una vez acreditada en la investigación la realidad de los hechos denunciados en tanto persistan las acciones civiles o laborales que procedan.

- Deberán garantizarse los derechos de acceso, rectificación, cancelación y oposición por parte del denunciado, sin que ello implique facilitar a aquél el dato del denunciante. En todo caso, el denunciado debería poder conocer en el menor tiempo posible el hecho denunciado a fin de poder defender debidamente sus intereses.

Ej.: Facilitar al denunciado esta información tras un tiempo prudencial en que se lleve a cabo la investigación preliminar de los hechos.

- Los ficheros creados en el marco de estos sistemas deberán ser notificados al Registro General de Protección de Datos. Del mismo modo, deberán notificarse y/o autorizarse las transferencias internacionales de los datos que vayan a llevarse a cabo.

■ CONTRATACIÓN DE SEGUROS DE VIDA Y PLANES DE PENSIONES

En muchas ocasiones las empresas, y los grupos de empresas, constituyen seguros de vida y planes de pensiones en beneficio de sus empleados, bien de modo voluntario, bien en virtud de lo pactado en un Convenio Colectivo.

Debe tenerse en cuenta que:

- Los tratamientos de datos que resulten necesarios para la contratación de este tipo de productos se encontrarán legitimados, ya sea por el consentimiento del trabajador, ya sea por la existencia de la relación laboral.

- La empresa puede realizar distintos tipos de tratamientos:

- La cesión de los datos de identificación y contacto del trabajador a la empresa aseguradora o la gestora del plan de pensiones.

Ej. La empresa se limita a facilitar, previa información a los trabajadores, los datos de éstos a la aseguradora o gestora, para que a su vez ésta inicie su relación con el asegurado o participe del plan y recabe los datos que resulten necesarios.

- La recogida de datos vinculados al contrato a celebrar para su traslado a la aseguradora o gestora del plan de pensiones.

Ej. Poniendo a disposición del trabajador la ficha o solicitud de adhesión al seguro de vida colectivo que éste deberá cumplimentar con cuantos datos resulten necesarios, por ejemplo en relación con los beneficiarios.

- Es necesario en todo caso informar a los trabajadores en la recogida de datos en los términos arriba descritos, teniendo en cuenta la existencia de distintas posibilidades:

- En el contrato de trabajo.

Debe recordarse que cuando se requiera el consentimiento por no fundamentarse el tratamiento en los deberes u obligaciones de las partes en una relación laboral el contrato no es

el instrumento más idóneo. De utilizarse deberá informarse expresamente de los términos en los que debe ejercerse el derecho de oposición.

- Mediante la elaboración de información específica dirigida a los trabajadores.
- En este tipo de tratamientos debe tenerse muy en cuenta el derecho de oposición del trabajador cuando se traten sus datos sin consentimiento en virtud de las obligaciones que le imponga al empresario la normativa o el convenio colectivo.
- Pueden existir tratamientos que afecten a familiares o personas relacionadas con los trabajadores cuando estos deban designar beneficiarios del seguro o del plan de pensiones. En este caso el tratamiento de sus datos resulta legitimado por la existencia de la relación laboral si bien debe recordarse que los datos deben ser únicamente los necesarios, -proporcionalidad-, y únicamente en relación con la contratación del seguro o plan de pensiones, -finalidad-.

«La Agencia Española de Protección de Datos ha venido considerando que en supuestos no idénticos al presente, pero con los que podría entenderse que el mismo guarda cierta relación de semejanza, la referencia a las “partes” de una relación jurídica, prevista en el artículo 6.2 puede considerarse asimilada a los “elementos personales” de dicha relación, de modo que cuando la relación es formalizada por un afectado en beneficio de un tercero, el tratamiento de los datos de éste, que resulta necesario para la adecuada formalización de la relación, podría considerarse amparado por la Ley Orgánica 15/1999.

En este sentido, se ha considerado que el tratamiento de los datos del beneficiario de un seguro de vida se encuentra amparado por lo dispuesto en el artículo 6.2 de la Ley Orgánica 15/1999, aún cuando el beneficiario no haya prestado su consentimiento al tratamiento. (Informe 363/2008)»

- Por todo ello, resulta conveniente definir con precisión el procedimiento para la captación y tratamiento de los datos personales optando por el método más eficaz para garantizar los derechos de los afectados o interesados. En este sentido, desde el punto de vista de un tratamiento absolutamente respetuoso con el derecho fundamental lo más adecuado puede consistir en, previa información a los trabajadores, ceder a la aseguradora, o a la gestora del plan de pensiones, únicamente los datos de los asegurados o partícipes del plan de pensiones, dejando en sus manos el desarrollo de ulteriores gestiones.

■ EXTERNALIZACIÓN DE LA GESTIÓN DE LAS NÓMINAS

Es muy frecuente que la gestión de las nóminas se encomiende a un asesor laboral o a una empresa del grupo. La empresa contratada debe acceder a datos personales para poder realizar su prestación y, conforme a la LOPD es lo que se define como encargado del tratamiento.

« En concreto, en el caso en que la empresa facilite los datos a la gestoría precisamente con la finalidad de que por la misma se desarrollen las debidas actividades de tratamiento de los datos, por lo que será la cliente quien decida sobre la finalidad y uso de la información, aquella tendrá la condición de responsable del fichero y deberá notificar su existencia al Registro General de Protección de Datos.

Dado que en este caso nos encontraremos ante un supuesto en que la gestoría tendrá la condición de encargado del tratamiento, la relación entre ambas entidades deberá someterse a lo dispuesto en el artículo 12 de la Ley. ([Informe sobre análisis de la figura del Encargado del tratamiento](#)) »

El tratamiento de datos por cuenta de terceros es una figura regulada con mucho detalle por el artículo 12 LOPD, que establece la necesidad de formalizar un contrato y define su contenido y las obligaciones de las partes. Los artículos 20 y siguientes del RDLOPD han regulado los detalles de estas prestaciones con acceso a datos. De lo dispuesto en estas normas debe tenerse muy en cuenta que:

- El encargo se regulará mediante un contrato que deberá constar por escrito o de alguna otra manera que permita acreditar su celebración y contenido. Se excluye el contrato verbal.

Ej. Otra manera puede consistir en su celebración por medios electrónicos que dejen constancia de su contenido.

- El contrato previsto por el artículo 12 LOPD debe tener un contenido ajustado al tratamiento de datos personales que regule. No puede consistir en una mera repetición del precepto citado.
- Es muy relevante tener en cuenta las necesidades específicas de seguridad en particular cuando el tratamiento se realice en los soportes del encargado.

- Las condiciones para la destrucción o devolución de los datos de carácter personal al responsable del tratamiento, podrá consistir en su entrega a un nuevo encargado.
- Si el encargado acude a la subcontratación, habrá de ser autorizado para ello por el responsable. Para ello caben dos posibilidades.
 - La subcontratación puede preverse en el propio contrato con el encargado ya sea con indicación de la empresa subcontratista autorizada ya con la definición de los supuestos de subcontratación.
 - La autorización sobrevenida del responsable a petición del encargado.

En uno u otro caso el responsable debe conocer la identidad del subcontratado y entre el encargado y esté último debe celebrarse un contrato conforme al art. 12 LOPD.

- Pueden encargarse tareas específicas al encargado como la atención de los derechos de acceso, rectificación y cancelación o la llevanza del documento de seguridad.

Ej. Cuando un responsable contrata de modo externo la gestión de nóminas de modo que materialmente ésta se realiza en el entorno del encargado podría delegarse la llevanza del documento de seguridad.

- El RDLOPD permite al encargado conservar bloqueados los datos, cuando exista una responsabilidad u obligación legal que lo justifique.



La Prevención de riesgos laborales

La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales y sus normas de desarrollo imponen a la empresa la realización de un conjunto de actividades cuyo fin último es evitar o disminuir los riesgos derivados del trabajo. Para esta tarea resulta necesario tratar datos personales de los trabajadores.

Ej. Es obvio que como mínimo la planificación de la prevención obliga a disponer de una relación detallada de los puestos de trabajo y de las personas que los ocupan. Además hay que responder a un conjunto de preguntas sobre los riesgos específicos del puesto cuya respuesta en muchas ocasiones dependerá de características personales o de salud del propio trabajador. ¿Es alérgico a determinados elementos químicos? ¿Necesita ciertas condiciones de luminosidad o de tamaño de letra en la pantalla de su ordenador? ¿Es capaz de identificar con claridad una alarma acústica?

EL CONSENTIMIENTO EN LA PREVENCIÓN DE RIESGOS

En principio, el tratamiento de datos personales en materia de prevención de riesgos se encuentra legitimado por la existencia de un relación contractual cuyo cumplimiento, desarrollo y control, lo hace necesario (art. 6.2 LOPD).

Esto debe ser matizado en el ámbito de la vigilancia en la salud que puede ser voluntaria u obligatoria. La regla general es la de la voluntariedad, en cuyo caso se requiere el consentimiento.

«El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo.

Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento.(...) (art. 21.1 Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales)»

No obstante, esta vigilancia puede ser obligatoria conforme al artículo 21.1 de la Ley de Prevención de Riesgos Laborales, previo informe de los representantes de los trabajadores en supuestos en los

que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad.

No obstante, en uno y otro caso no debe olvidarse que:

- El cumplimiento del deber de información es esencial.
- Hay que prestar particular atención al principio de calidad y en particular a la proporcionalidad, limitándose a recabar y utilizar los datos estrictamente necesarios para la finalidad de prevención.

LOS PROTAGONISTAS DE LA PREVENCIÓN DE RIESGOS

El desarrollo de tareas de prevención de riesgos supone la presencia de áreas de actuación especializadas, -seguridad, ergonomía y psicología, higiene industrial, medicina y enfermería del trabajo-, y de profesionales con perfiles y exigencias organizativas diversas. Hay que disponer de medios y recursos adecuados que no siempre se encuentran a disposición de todas las empresas.

Ello ha determinado en la práctica que la legislación contemple la existencia de servicios de prevención propios y ajenos. Y que el desempeño profesional de la prevención de riesgos se asigne a diversos perfiles profesionales. Ello se proyecta sobre la protección de datos de dos modos.

- La condición de responsable del fichero o del tratamiento varía según se trate de un servicio de prevención propio, ajeno o mancomunado. Si se trata de un servicio propio la empresa será responsable del fichero que se genere para la gestión de la prevención.

No hay que olvidar que si el servicio de prevención es propio existirán en el seno de la empresa distintos perfiles y facultades de acceso a datos de salud. Serán plenos para el personal sanitario y son limitadísimos para la gerencia hasta el punto de abarcar únicamente conceptos del tipo apto/no apto.

Las empresas que actúan como servicios de prevención ajenos tienen la consideración de responsables del tratamiento ([Informe 0299/2009](#)).

- La realización de políticas de prevención de riesgos define distintos roles desde el punto de vista de la protección de datos personales. El servicio de prevención tendrá carácter interdisciplinar. Por ello, los sistemas de información que se dedican a la gestión de servicios de prevención deberán tener en cuenta:

- El nivel de seguridad. Que será alto en todos aquellos casos en los que se incluyan datos de salud con identificación precisa de las enfermedades, traumatismos etc., o se gestionan historias de salud laboral.

«Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética. (art 5.1.h RDLOPD)».

- Deberán definir de modo muy preciso los perfiles de acceso y las funciones de cada uno de los usuarios.

Ej. No puede ser el mismo el perfil del administrativo que organiza las citas que el de un médico del trabajo. Del mismo modo el responsable de la adaptación ergonómica de un puesto de trabajo debería poder acceder a los datos de salud que resulten necesarios para su actividad.

- La historia clínica del trabajador debe regirse además de por lo previsto en la LOPD por los principios de la Ley 41/2002.

«Al propio tiempo, de lo establecido en el párrafo segundo del artículo 22.4 de la Ley se deriva el derecho del personal sanitario que realice las acciones de vigilancia de la salud al conocimiento de la información médica que se derive de la misma. En este sentido, dicha información compondrá, según dispone la propia Ley, el historial clínico laboral del trabajador, debiendo tenerse en cuenta que, en cuanto historia clínica, la misma se sometería a lo establecido en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que impone la llevanza de la misma a los centros sanitarios o profesionales que realicen las actuaciones sanitarias en relación con el paciente, en este caso el trabajador que se somete a las pruebas que implican la realización de acciones de vigilancia de la salud. ([E/01040/2005](#))».

- Deben establecerse procedimientos para garantizar los derechos de acceso, rectificación y cancelación de los trabajadores.

Cuando se trate del acceso a la historia clínica debe recordarse que la legislación específica impone deberes como la limitación del acceso a las anotaciones subjetivas del facultativo, la existencia de límites a la rectificación contenidas en regulaciones sectoriales en materia de Seguridad Social, o la imposibilidad de proceder a la cancelación de datos que deban conservarse en virtud de la normativa sanitaria . En todo caso deberá contestarse la petición motivando la denegación.

EL ACCESO A LOS DATOS POR LA EMPRESA Y LOS DELEGADOS DE PREVENCIÓN

En prevención de riesgos laborales existen distintas previsiones normativas que comportan la posibilidad de realizar cesiones de datos personales. Así la legislación habilita y obliga a ceder datos a los delegados de prevención, a la autoridad sanitaria en el marco de la Ley General de Sanidad, a la inspección de trabajo, a la autoridad laboral, sin olvidar los supuestos específicos del artículo 11.2 LOPD como la cesión de datos requeridos por jueces y tribunales, o las necesarias en caso de urgencia médica, o en estudios epidemiológicos. Los casos que plantean mayores dificultades son los que se refieren al acceso a información por la propia empresa y por los delegados de prevención.

Las facultades de acceso a la información por parte de la empresa son muy limitadas y en la práctica se refieren a conocer las condiciones de aptitud o no aptitud del trabajador.

«Así, el tratamiento por parte de los servicios de prevención de riesgos laborales del historial médico, consecuencia de los reconocimientos médicos realizados a los trabajadores, deberá limitarse a las previsiones del artículo 22.4 de la LPRL que se citaba. En este sentido, se prohíbe el acceso a la información médica obtenida al amparo de lo dispuesto en la LPRL por parte del empresario o de cualquier tercero, incluidas las personas u órganos con responsabilidades en materia de prevención, distintos del “personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores”, con la única excepción de las conclusiones derivadas de dicho seguimiento en cuanto a la aptitud de los trabajadores para el desempeño del puesto de trabajo. (PS/00142/2005)».

No obstante, es posible que el empresario deba acceder de modo específico a información personal del trabajador necesaria para el cumplimiento de sus obligaciones que desborden el contenido apto/no apto. En tales casos, la legitimación para el tratamiento deriva de la propia Ley pero se limitará a los datos estrictamente necesarios.

Ej. Es evidente que si debe adaptarse una pantalla de ordenador con un determinado tamaño de letra existirán problemas visuales, si se debe cambiar una avisador acústico por uno visual existen problemas de audición y que si el

uniforme de trabajo debe ser de un determinado tejido puede existir una alergia. En todos estos casos puede deducirse la presencia de una discapacidad o enfermedad.

Se han admitido las cesiones de datos sobre la aptitud del trabajador en el caso de que la mutua contratada para el desarrollo de las tareas de prevención ya dispusiese con anterioridad de informaciones que fuesen relevantes para el desempeño del puesto de trabajo en una nueva empresa.

«Consideramos, por todo ello, y dadas las especiales circunstancias concurrentes, que en el presente supuesto la cesión de datos producida se encuentra amparada en el artículo 11.2.a) LOPD , y que tiene una finalidad legítima, cual es la que hace referencia a la correcta aplicación de la normativa sobre Seguridad Social y Prevención de Riesgos Laborales mencionada e, indirectamente, a la prevención del fraude, por lo que no es exigible el consentimiento del trabajador denunciante, Sentencia de la Audiencia Nacional de 24/05/07»

En el caso de los delegados de prevención se les faculta para acceder a la información y documentación relativa a las condiciones de trabajo que sean necesarias para el ejercicio de sus funciones y, en particular, a la prevista en los artículos 18, 23 Y 36 LPRL.

«c) Ser informados por el empresario sobre los daños producidos en la salud de los trabajadores una vez que aquél hubiese tenido conocimiento de ellos, pudiendo presentarse, aún fuera de su jornada laboral, en el lugar de los hechos para conocer las circunstancias de los mismos.

d) Recibir del empresario las informaciones obtenidas por éste procedentes de las personas u órganos encargados de las actividades de protección y prevención en la empresa, así como de los organismos competentes para la seguridad y la salud de los trabajadores, sin perjuicio de lo dispuesto en el artículo 40 de esta Ley en materia de colaboración con la Inspección de Trabajo y Seguridad Social. (art. 36.2 LPRL)».

En tal sentido podrán acceder a datos personales sobre daños en la salud de los trabajadores cuando tengan su origen en un hecho dañoso, relacionado con el entorno laboral, sólo para la finalidad de control que les atribuye la LPRL y limitada a los datos estrictamente necesarios, entendiéndose por tales los relativos a la gravedad y naturaleza de los daños. El delegado es un cesionario, viene vinculado por los principios de protección de datos personales, y debe guardar en particular el deber de confidencialidad conforme a la LOPD y a la legislación específica en la materia.

«A los Delegados de Prevención les será de aplicación lo dispuesto en el apartado 2 del artículo 65 del Estatuto de los Trabajadores en cuanto al sigilo profesional debido respecto de las informaciones a que tuviesen acceso como consecuencia de su actuación en la empresa. (Artículo 37.3 LPRL, E/00312/2007) »

«2. Los miembros del comité de empresa y éste en su conjunto, así como, en su caso, los expertos que les asistan, deberán observar el deber de sigilo con respecto a aquella información que, en legítimo y objetivo interés de la empresa o del centro de trabajo, les haya sido expresamente comunicada con carácter reservado. (art. 65.2 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores)»



Controles empresariales

El Estatuto de los Trabajadores ha atribuido facultades específicas a la empresa que posibilitan el control del desarrollo de la prestación laboral. El ejercicio de estas facultades comporta en muchas ocasiones tratamientos de datos personales.

«3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

4. El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones. (Art. 20.3 y 4 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores).

CONTROLES BASADOS EN EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN

Cuando para el desarrollo de la función empresarial de control se utilizan las tecnologías de la información, las posibilidades de repercusión en los derechos del trabajador se multiplican. La aplicación de este tipo de técnicas se manifiesta de muy diversos modos.

Pueden citarse entre otros, los controles biométricos como la huella digital, la videovigilancia, los controles sobre el ordenador, -como las revisiones, el análisis o la monitorización remota, la indexación de la navegación por Internet, o la revisión y monitorización del correo electrónico y/o del uso de ordenadores-, o los controles sobre la ubicación física del trabajador mediante geolocalización.

En la mayor parte de estos supuestos existen tratamientos de datos personales y, en consecuencia es necesario cumplir con los principios de protección de datos. La Agencia Española de Protección

de Datos y la jurisprudencia de los tribunales han venido indicando distintos supuestos en los que tales tratamientos son admisibles y las condiciones para su realización.

Por otro lado, el uso de tecnologías de la información multiplica las posibilidades de control empresarial y obliga a tener en cuenta el respeto a los derechos fundamentales de los trabajadores, a adoptar medidas de control que sean proporcionales y respeten su dignidad, su derecho a la protección de datos y su vida privada.

Existe por tanto, un conjunto de principios cuyo respeto resulta recomendable cuando no prácticamente ineludible.

- La legitimación para el tratamiento deriva de la existencia de la relación laboral y, por tanto, de acuerdo con el art. 6.2 LOPD, no se requiere del consentimiento.

«2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. (art. 6.2 LOPD)»

- A la hora de decidir adoptar una medida de control que comporte un tratamiento de datos personales debe aplicarse el principio de proporcionalidad.

Ej. Puede ser perfectamente razonable dotar de un dispositivo de geolocalización en tareas como el transporte de mercancías para las que resulte relevante conocer donde se encuentra el vehículo y en qué momento podrá realizar una determinada entrega. Ello no puede suponer que se facilite un dispositivo de esta naturaleza a todos los trabajadores de la empresa cuando su tipo de prestación no lo haga necesario.

- Debe existir una finalidad que, en este caso, no puede ser otra que la establecida por el art. 20.3 ET de «verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales».

« En cuanto a la posibilidad de que las huellas sean tratadas sin consentimiento del interesado, (...) será posible el tratamiento inconstitucional, ya que el artículo 6.2 de la LOPD prevé que no será preciso el consentimiento cuando los datos “se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento” ([Informe sobre Tratamiento de la huella digital de los trabajadores](#))»

- Los datos que se obtengan y almacenen deberán ser exactos y puestos al día y no podrán conservarse más tiempo del necesario. Se recomienda a los empleadores fijar un plazo de conservación.
- Debe cumplirse con el deber de información a los trabajadores. Este deber resulta particularmente relevante cuando se trate de controles sobre el uso de Internet y/o del correo electrónico.

En este caso es muy recomendable que la información a los trabajadores sea clara en lo que respecta a la política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales. Así como que incluya la finalidad de la vigilancia, y cuando pueda repercutir sobre medios que el trabajador utiliza normalmente una información sobre las medidas de vigilancia adoptadas.

Por otra parte, en la medida en la que este tipo de controles inciden sobre el conjunto de la empresa puede ser muy recomendable informar también a los representantes de los trabajadores de las políticas adoptadas en esta materia.

No se trata en absoluto de que el trabajador conozca el detalle de políticas de seguridad que pueden afectar a ámbitos que la empresa necesita proteger. Sin embargo, es indispensable que conozca por ejemplo si puede recibir mensajes privados, o depositar fotografías en determinados espacios en su ordenador o en un servidor corporativo.

La información previa y su prueba es esencial, ya que estos tratamientos no requieren el consentimiento del trabajador y son manifestación de los poderes de control del empresario.

«es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que

han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo por la protección de los derechos humanos. (Sentencia de la Sala de lo Social del Tribunal Supremo de 26 de septiembre de 2007)».

CONTROLES SOBRE EL ABSENTISMO LABORAL

El Estatuto de los Trabajadores faculta a las empresas para realizar controles en los supuestos de enfermedad o accidente de trabajo que motivan faltas de asistencia. Este control se realizará mediante reconocimiento médico y la norma establece las posibilidades de actuación del trabajador ante la negativa a someterse al reconocimiento.

«4. El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones. (art. 20 ET)».

Por otra parte hay que tener en cuenta dos elementos que se han señalado con anterioridad en esta Guía:

- El tratamiento de datos de salud requerirá del consentimiento expreso del trabajador o de la existencia de una previsión legal que exima del mismo. La LOPD contiene un régimen específico cuando se trata de la prestación de asistencia sanitaria que no resulta en absoluto aplicable a este caso.

«6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.(art. 7.6 LOPD)».

- Las posibilidades de acceso de la empresa a estos datos de salud y su utilización para fines distintos para los que fueron recabados resulta imposible ya que, como antes se señaló la empresa únicamente puede conocer las condiciones de aptitud.
- La incorporación de datos de salud a un fichero con la única finalidad de realizar controles del absentismo resulta desproporcionada.

«mediante la creación de la base de datos ahora discutida parece perseguirse un control más eficaz del absentismo laboral, según las facultades que al efecto reconoce al empresario la legislación vigente. En este sentido, lo primero que conviene advertir es que entre dichas facultades no figura la de proceder al almacenamiento en soporte informático de los datos atinentes a la salud de los trabajadores -y en concreto del diagnóstico médico- prescindiendo del consentimiento de éstos. Por otra parte, y con independencia de ello, lo verdaderamente relevante es que la medida adoptada por la empresa, sometida a los cánones establecidos para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, no reviste la consideración de solución idónea, necesaria y proporcionada para la consecución del fin, en este caso, el control del absentismo laboral [SSTC 66/1995, fundamento jurídico 5.; 207/1996, fundamento jurídico 4. E) y 69/1999, fundamento jurídico 4.], pues no se trata de medida de suyo ponderada y equilibrada, ya que de ella no se derivan más beneficios o ventajas para el interés general o para el interés empresarial que perjuicios sobre el invocado derecho a la intimidad. (STC 202/1999)».

El control del absentismo adquiere una relevancia particular cuando se realiza mediante la contratación de un prestador de servicios ya que, además de cumplir con las obligaciones propias de un encargado del tratamiento, debe atenerse a ciertas condiciones:

- La información al trabajador debe ser muy precisa e indicar que se trata de un control laboral. Como indica el art.5 una de las informaciones que deben facilitarse en su caso se refiere a la obligación de facilitar datos y las consecuencias de la negativa a suministrarlos.

La información se referirá a que se está verificando sus condiciones de aptitud por cuenta de la empresa y de la naturaleza de este tratamiento conforme al art. 20.4 del Estatuto de los trabajadores.

- Para poder incorporar sus datos de salud a una historia clínica se requerirá el consentimiento expreso del trabajador.

«estamos ante un supuesto en el que el objeto no es la atención del paciente - finalidad que justifica la excepción a la prohibición establecida en la ley ya que el mantenimiento del historial médico redundaría en beneficio de su salud- sino ante una técnica de control del absentismo laboral.(...)»

En este sentido, y en contra de lo que se razona, si resulta de aplicación lo razonado en la STC 202/1999, de 8 de noviembre, cuando razona que el fichero está fuera de las excepciones del art 7 de la LO pues "no se dirige a la preservación de la salud de los trabajadores, sino al control del absentismo laboral"; por lo que la existencia del mismo sin el consentimiento expreso del afectado es una medida inadecuada y lesiona el derecho de libertad informática. Por lo demás no es de aplicación el art 8 de la LO 15/1999, pues dicha norma que regula la cesión de datos relativos a la salud de las personas, parte de la previa existencia de un fichero legal de datos, y ya hemos visto que este no es el caso. En suma, debemos mantener el criterio sentado en nuestra SAN (1ª) de 12 de abril de 2002 (Rec 1271/2000). Sentencia de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 10 de mayo de 2002».

No existe obstáculo a que se persiga la doble finalidad de verificar el estado de salud del trabajador y controlar el absentismo. Pero, si existe un tratamiento relacionado con la salud deberá obtenerse el consentimiento expreso del trabajador.

- En el caso de que el prestador externo desarrolle servicios de vigilancia en la salud debería articular procedimientos que garanticen el cumplimiento de los principios de protección de datos, y en particular el deber de información, el principio de finalidad y la garantía del consentimiento en cada uno de los tratamientos.
- Por último no debe olvidarse que para este tipo de servicios el prestador externo tiene la condición de encargado del tratamiento y deben de cumplirse las previsiones del artículo 12 de la LOPD.



Relaciones con los sindicatos. Comunicaciones de datos, tabloneros, censos.

La Constitución Española reconoce el derecho a la libertad sindical, y la legislación de desarrollo establece un conjunto de derechos, competencias y funciones para los representantes de los trabajadores cuya satisfacción requiere del tratamiento de datos personales y del establecimiento de ciertos flujos de datos habitualmente mediante comunicaciones de éstos desde la empresa.

«1. Todos tienen derecho a sindicarse libremente. La Ley podrá limitar o exceptuar el ejercicio de este derecho a las Fuerzas o Institutos armados o a los demás Cuerpos sometidos a disciplina militar y regulará las peculiaridades de su ejercicio para los funcionarios públicos. La libertad sindical comprende el derecho a fundar sindicatos y a afiliarse al de su elección, así como el derecho de los sindicatos a formar confederaciones y a fundar organizaciones sindicales internacionales o afiliarse a las mismas. Nadie podrá ser obligado a afiliarse a un sindicato.

2. Se reconoce el derecho a la huelga de los trabajadores para la defensa de sus intereses. La Ley que regule el ejercicio de este derecho establecerá las garantías precisas para asegurar el mantenimiento de los servicios esenciales de la comunidad. (art. 28 CE)».

PUBLICACIONES DE DATOS PERSONALES EN TABLONEROS

La Ley Orgánica de libertad sindical reconoce un derecho a disponer de un tablón de anuncios que permita facilitar información sindical a los trabajadores.

«Con la finalidad de facilitar la difusión de aquellos avisos que puedan interesar a los afiliados al sindicato y a los trabajadores en general, la empresa pondrá a su disposición un tablón de anuncios que deberá situarse en el centro de trabajo y en lugar donde se garantice un adecuado acceso al mismo de los trabajadores.(8.2.a Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical)».

La publicación de notas informativas, anuncios, convocatorias, declaraciones e incluso sentencias en este tipo de tabloneros constituye una práctica habitual. Por otra parte, la evolución tecnológica ha dado lugar a que estos tabloneros se ofrezcan online, bien en espacios cedidos por la propia empresa, bien en dominios pertenecientes al propio sindicato. Cuando estos documentos contienen datos personales la simple publicación de éstos constituye un tratamiento que puede comportar el acceso a datos por terceros carentes de legitimación.

«el derecho a la libertad sindical, (...) ha de prevalecer sobre el derecho a la protección de datos personales, cuando, como sucede en el caso examinado, la acción sindical ampara la actuación del sindicato recurrente para divulgar entre los trabajadores de los centros los datos precisos, y únicamente necesarios, para el entendimiento de la noticia, teniendo un conocimiento cierto de la información relevante desde el punto de vista sindical. (SAN de 19 de diciembre de 2007, E/00729/2008)»

Ello obliga a tener en cuenta una serie de aspectos con el fin de aplicar adecuadamente las normas y garantizar los derechos de las personas concernidas:

- Será responsable del tratamiento de datos en el tablón de anuncios y por tanto de las informaciones publicadas en el mismo, aquél órgano u organización que decida sobre su uso y finalidad y sitúe materialmente la información en él.
- Debe considerarse el espacio físico o virtual concreto en el que se situará el tablón con la finalidad de que, en caso de contener información personal, ésta sólo resulte visible a los usuarios legitimados para consultarla.

Ej. No es razonable que un tablón del que se pueda obtener información sindical, se sitúe en una zona de acceso libre para clientes o proveedores.

- Es fundamental que los tabloneros sindicales online se sitúen en las intranet de la empresa, nunca en Internet.

«Si la información en cuestión se hubiera publicado en la intranet corporativa, a la vista de las circunstancias concurrentes, no se habría apreciado vulneración del derecho a la protección de datos y seguramente el denunciante no hubiera puesto los hechos en conocimiento de la AEPD.

Lo que singulariza este caso respecto el contemplado en aquella sentencia, es que los datos de carácter personal: nombre, apellidos, categoría profesional (agente de movilidad) y número de carnet profesional, se publican en una página web en Internet y la publicación en dicha red no es idónea, necesaria ni proporcionada para mantener informados a los trabajadores en aquellas cuestiones que directa o indirectamente puedan repercutir en las relaciones laborales.

Este acceso a los datos personales del denunciante (...) a cualquier usuario de Internet es lo que singulariza este caso respecto del contemplado en la citada sentencia de 19 de diciembre de 2007 .

Por ello, a la vista de las circunstancias concretas concurrentes, considera la Sala que el derecho a la libertad sindical se puede satisfacer plenamente sin necesidad de publicar en Internet los datos personales del denunciante, por lo que la citada publicación no puede ampararse bajo el ropaje del citado derecho de libertad sindical.

En la línea expuesta, señalar que tampoco puede prevalecer el derecho de información veraz y los de libertad de expresión sobre el de protección de datos, pues pudo informarse sin aportar datos personales del denunciante en Internet, siendo este el criterio seguido en la sentencia de esta Sección de 16 de febrero de 2007 citada por la resolución impugnada, que contrariamente a lo alegado en la demanda, si presenta similitud con el presente.

Además, la información publicada carece de relevancia pública e interés general, que son los factores predominantes que toma en consideración el Tribunal Constitucional para otorgar preferencia al derecho a la libertad de expresión frente a otros derechos constitucionales. (Sentencia de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 8 de julio de 2009)»

- Debe tenerse muy en cuenta el principio de calidad desde el punto de vista de la proporcionalidad de los tratamientos y de la finalidad de los mismos.

Ej. La información publicada debería limitarse a la estrictamente necesaria. Así, si en un momento dado decidiera publicarse una determinada resolución administrativa o de una sentencia judicial de interés para los trabajadores debería procederse a la anonimización de los datos cuando se pueda afectar a los derechos de las partes u otras personas que pudieran aparecer en ellos y la publicación de los datos carezca de relevancia desde el punto de vista de la libertad sindical.

- Es recomendable considerar la posibilidad de que los tablones impidan el acceso a la información por terceros no autorizados.

ACCESO A DATOS POR EL COMITÉ DE EMPRESA

El Estatuto de los Trabajadores atribuye un amplio haz de facultades a los representantes sindicales y en particular al comité de empresa. En algunos casos el ejercicio de estas facultades puede comportar el acceso a datos.

Ej. Conforme al artículo 64 del ET el comité de empresa, tendrá derecho a: ser informado de todas las sanciones impuestas por faltas muy graves y a recibir la copia básica de los contratos y la notificación de las prórrogas y de las denuncias correspondientes a los mismos en el plazo de diez días siguientes a que tuvieran lugar.

No obstante este acceso potencial a datos personales debe estar regido por el cumplimiento estricto de los principios de protección de datos.

- Únicamente podrán cederse datos en aquellos casos en los que resulte estrictamente necesario para el cumplimiento de los deberes que el Estatuto de los Trabajadores establece para la empresa.

Ej. En todos aquellos casos en los que la información pueda presentarse de modo estadístico o anonimizado permitiendo al comité cumplir con sus funciones se optará por éste método.

Ej. En el caso del acceso a la copia básica no se está habilitando para la cesión de todos los datos del trabajador sino únicamente de aquellos que permiten el desenvolvimiento de la función de control asignada a la representación de los trabajadores.

- Los destinatarios de la información serán los previstos por la norma que habilite para la cesión.

Ej. En ocasiones tiende a confundirse sindicatos y representantes de los trabajadores. Cuando la posibilidad de acceder a información personal se concede a un comité de empresa o la persona que ostente la representación de los trabajadores el deber de secreto se extiende a las relaciones que el representante mantiene incluso con su sindicato.

- El comité de empresa o los representantes sindicales que acceden a información de los trabajadores están obligados a guardar secreto y al cumplimiento de los principios de la LOPD y de los específicamente previstos en las normas que les sean de aplicación.

«2. Los miembros del comité de empresa y éste en su conjunto, así como, en su caso, los expertos que les asistan, deberán observar el deber de sigilo con respecto a aquella información que, en legítimo y objetivo interés de la empresa o del centro de trabajo, les haya sido expresamente comunicada con carácter reservado.

3. En todo caso, ningún tipo de documento entregado por la empresa al comité podrá ser utilizado fuera del estricto ámbito de aquélla ni para fines distintos de los que motivaron su entrega.

El deber de sigilo subsistirá incluso tras la expiración de su mandato e independientemente del lugar en que se encuentren.

(Art. 65 del Estatuto de los Trabajadores)».

CESIONES DE DATOS PERSONALES A LOS SINDICATOS

La cesión de datos más común a las organizaciones sindicales es la relativa al cobro de la cuota sindical en el pago de la nómina. Puesto que se trata de una solicitud que debe realizar el propio trabajador deben darse las condiciones del art. 7.2 LOPD.

«Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.»

El tratamiento de estos datos requiere la adopción de procedimientos por parte de la organización ya que se trata de proteger información particularmente sensible.

- Es recomendable disponer de procedimientos de captación del consentimiento como impresos o modelos de solicitud en los que el trabajador autorice de modo expreso y por escrito el tratamiento.
- Es muy importante limitar el uso de estos datos a la finalidad para la que se han recabado: cobrar la cuota y transferir las cantidades a la organización sindical.

Ej. Por ejemplo, no es posible tratar el dato de afiliación sindical con la finalidad de practicar descuentos en el salario a los afiliados del sindicato convocante de una huelga. (STC 11/1998).

- Debe recordarse que si el tratamiento se da exactamente en los términos y para las finalidades aquí descritas el nivel de seguridad será básico.

En segundo lugar, hay que referirse al envío de información sindical a través del correo electrónico. Esta actividad requiere el tratamiento de datos personales puesto que, como en reiteradas ocasiones se ha señalado una dirección electrónica es un dato personal.

El Tribunal Constitucional ha señalado que el envío de este tipo de mensajes de correo electrónico constituye un derecho de los sindicatos amparado por el derecho fundamental la libertad sindical (STC.281/2005). No obstante deben darse ciertas condiciones como que la empresa disponga del

servicio de correo electrónico, que los envíos se realicen de modo proporcional y no perjudique el normal funcionamiento de la organización.

Cuando se den las circunstancias anteriores existirá legitimación para que se produzca una cesión de datos personales a los sindicatos. Sin embargo deben tenerse en cuenta las siguientes consideraciones:

- Existen procedimientos automatizados que pueden permitir la satisfacción del derecho a la libertad sindical sin necesidad de realizar una cesión y, por tanto minimizando los riesgos y las obligaciones de cumplimiento normativo para el empresario y el sindicato.

Ej. La utilización de listas de distribución permite que el sindicato remita la información a una dirección corporativa del tipo listasindical@empresa.es, sin acceso a los datos. Por otra parte, aunque la empresa si trata datos personales puede incorporar la información del art. 5 LOPD en los pies de los correos y automatizar la cancelación y la oposición a los tratamientos mediante las bajas en las listas a petición del usuario ([Informe 0101/2008](#)).

- La comunicación de datos se limitará a los estrictamente necesarios.

Ej. En ningún caso se cederán datos como la dirección de cuentas privadas del trabajador.

- El dato se utilizará estrictamente para la finalidad para la que fue cedido.
- El sindicato como cesionario está obligado a cumplir con las previsiones de la LOPD.
- El sindicato debe satisfacer el derecho de oposición de los trabajadores salvo en el supuesto de elecciones sindicales, momento en el cual prevalece la libertad sindical respecto del derecho a la protección de datos.

«A tenor de las previsiones contenidas en la LOPD acerca del derecho de oposición, debe reconocerse el derecho de los trabajadores a mostrar su oposición a la recepción de mensajes con contenido sindical y, consiguiente, la obligación de los Sindicatos de cesar en el tratamiento de los datos de los solicitantes. No obstante, en lo referente a la información sindical remitida a los trabajadores en período electoral, debe concluirse que en periodo electoral debe prevalecer el derecho a la actividad sindical consagrado en el artículo 2.1 de la Ley Orgánica de Libertad Sindical sobre el derecho fundamental a la protección de datos.

Así las cosas, los trabajadores durante el proceso electoral sindical, no pueden oponerse al tratamiento de sus datos personales, siempre que el uso que realice el Sindicato sea adecuado para los fines del propio proceso electoral ([TD/01119/2008](#))».

No debe olvidarse que la celebración de elecciones sindicales legitima las cesiones de los datos censales necesarios para permitir al sindicato remitir información electoral y participar en el proceso electoral.

CESIONES DE DATOS CONTENIDOS EN DOCUMENTOS TC2

Las normas laborales, y en particular los convenios colectivos plantean dos tipos de supuestos que habilitan para facilitar la entrega de copia de estos documentos y, como consecuencia, para la cesión de los datos personales que contienen. Estos casos se dan con motivo de dos finalidades muy precisas, el control sindical de la actuación de la empresa y la garantía del cumplimiento de los deberes empresariales en supuestos de subcontratación.

ENTREGA DE TC2 AL COMITÉ DE EMPRESA

La entrega de este tipo de documentos esta sujeta al cumplimiento de ciertos principios:

- El comité debe actuar en el marco de las funciones que le atribuye el Estatuto de los Trabajadores.

«En el caso de cesión de los datos de los trabajadores, la misma únicamente podría entenderse amparada en caso de que se produjera en el ámbito de las funciones desarrolladas por los órganos de representación del personal, al encontrarse reconocido por el Estatuto de los Trabajadores el derecho de los órganos de representación a acceder a determinados datos de los trabajadores en el ámbito de sus competencias, en caso contrario será necesario el consentimiento del interesado para proceder a la comunicación de sus datos. Por otra parte, además, la utilización de los datos por parte de los representantes de los trabajadores debería limitarse a la finalidad de control que al mismo atribuye el propio Estatuto.(...)»

En consecuencia, teniendo en cuenta las competencias del Comité de Empresa de recibir copia de los contratos de trabajo celebrados por la empresa, lo que conlleva necesariamente el conocimiento de las personas vinculadas con ella por una relación de carácter laboral y el ejercicio de la labor de vigilancia en materia de seguridad social, no existe objeción a la cesión al mismo de los datos referentes a los trabajadores, siempre que no excedan de los contenidos en los citados contratos. (Informe 0247/2009)»

- El tipo de información a la que cabe acceder es limitado.

«teniendo en cuenta las competencias del Comité de Empresa en ningún caso podrá suponer el acceso a por ejemplo la nómina de los trabajadores. Sólo existe obligación de entregar los TC-1, boletín de cotización para la Seguridad Social en el que se reflejan los datos relativos a la identificación de la empresa y a la determinación de la deuda y el TC-2 en el que aparece reflejada la relación nominal de trabajadores y contiene los datos relativos a la identificación de los trabajadores, a sus bases de cotización y a las prestaciones que les hayan sido satisfechas en régimen de pago delegado» BUSCAR INFORME DE 28 DE MAYO DE 2007.

No obstante el convenio colectivo podría contener previsiones específicas que al ser fuentes reguladoras de la relación laboral podrían ampliar el ámbito de la cesión.

«El artículo 3 del Estatuto de los Trabajadores de 24 de marzo de 1995, incluye a los Convenios Colectivos entre las fuentes de la relación laboral que regulan los derechos y obligaciones concernientes a la misma. De ello se deduce que, prevista expresamente en el Convenio Colectivo, la comunicación de datos planteada encontraría cabida en el apartado c) del artículo 11.2 que citábamos en el párrafo anterior, posibilitando que los datos salgan del seno de la empresa, respondiendo así al desarrollo y cumplimiento de la relación laboral entre el responsable del fichero y el interesado. (Informe 252/2006)»

- En cualquier caso no existe legitimación para publicar este documento en un tablón de la empresa.

«Por tanto al resultar de aplicación el artículo 7.3 de la citada Ley Orgánica (la LOPD), se requiere una Ley o el consentimiento expreso de cada trabajador para comunicar los datos del TC2. (Informe 0247/2009)».

CESIÓN DE NÓMINAS Y TC2 DE LOS TRABAJADORES DE SUBCONTRATAS A LAS EMPRESAS CONTRATISTAS

En los casos de existencia de subcontratas el Estatuto de los Trabajadores establece obligaciones respecto de la empresa principal que pueden legitimar para realizar cesiones de datos personales. Deben distinguirse dos supuestos:

- El momento previo a la contratación o subcontratación, en el que para comprobar que los contratistas están al corriente del pago de las cuotas de la Seguridad Social debe solicitarse un certificado a la Tesorería y no cabe cesión alguna.

«Los empresarios que contraten o subcontraten con otros la realización de obras o servicios correspondientes a la propia actividad de aquéllos deberán comprobar que dichos contratistas están al corriente en el pago de las cuotas de la Seguridad Social. Al efecto, recabarán por escrito, con identificación de la empresa afectada, certificación negativa por descubiertos en la Tesorería General de la Seguridad Social, que deberá librar inexcusablemente dicha certificación en el término de treinta días improrrogables y en los términos que reglamentariamente se establezcan. Transcurrido este plazo, quedará exonerado de responsabilidad el empresario solicitante. (art. 42.1 del Estatuto de los Trabajadores)».

- En momentos posteriores respecto de la responsabilidad solidaria de las obligaciones de naturaleza salarial y las contraídas con la Seguridad Social existiría una legitimación basada en la existencia de un interés legítimo derivado de lo dispuesto por la Ley (art. 10 RDLOPD)

«El artículo 42.2 del Estatuto de los Trabajadores, impone al contratista principal una responsabilidad solidaria, responsabilidad que implica atender el cumplimiento de una obligación de naturaleza salarial y las referidas a la Seguridad Social durante el período de vigencia de la contrata.

(...) cuando estemos en presencia de una obligación solidaria cada uno de los deudores deberá prestar íntegramente la cosa objeto de la misma. Por tanto, si el contratista principal es obligado solidariamente de la deuda salarial y a las referidas a la Seguridad Social durante el período de vigencia de la contrata, deberá de conocer el contenido íntegro de dicha obligación para poder cumplirlas.

(...)

En consecuencia, la cesión de los TC2 estaría amparada en el artículo 7.3 de la Ley Orgánica 15/1999, en relación con el artículo 42.2 del Estatuto de los Trabajadores y por el alcance que el Código Civil impone a las obligaciones solidarias. (Informe 0412/2009)».

Esta legitimación alcanzaría a los datos relativos a la afiliación sindical. En las nóminas puede existir datos de esta naturaleza cuando se trate del cumplimiento del deber de detraer y trasladar al sindicato la cuota sindical que formen parte de estas obligaciones solidarias.

- Debe aplicarse el principio de proporcionalidad al definir el conjunto de trabajadores afectados.

«En todo caso, el acceso por parte del contratista debería limitarse a los datos relacionados con los trabajadores subcontratados y no a cualesquiera trabajadores de la empresa subcontratada. (Informe 0412/2009)»



Deberes de los trabajadores que acceden a datos personales: secreto y seguridad.

La LOPD trata el deber de seguridad junto con el deber de secreto cuando regula los principios de protección de datos. Por tanto les concede a ambos una importancia central.

«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 (art. 9)

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

Ambos principios resultan necesarios y constituyen una garantía para el derecho fundamental a la protección de datos. El secreto y la confidencialidad aseguran que los datos personales sólo sean conocidos por el afectado o interesado y por aquellos usuarios de la organización cuyo perfil les atribuye competencia para usar, consultar, modificar o incluir los datos en los sistemas de información.

«Este deber de secreto comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el “deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo”. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática, a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30/11, y, por lo que ahora interesa, comporta que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto. (PS/00192/2008, Sentencias de la Sección Primera de la Sala de lo Contencioso-Administrativo de 18 de febrero de 2002 y 1 de febrero de 2006)»

Por otra parte, la seguridad garantiza además de la confidencialidad, la disponibilidad de los datos, y con ella su recuperación ante cualquier evento, y la integridad de los mismos protegiéndolos

frente a cualquier manipulación no autorizada. La empresa debe disponer de políticas de cumplimiento de estos dos principios, ya que con ellas no sólo se garantiza un derecho fundamental sino que además se ofrece confianza y seguridad al público. Además, con la implementación de medidas de seguridad se protegen activos que son importantes para la empresa como los datos de sus clientes y proveedores.

Para el adecuado cumplimiento de estos dos deberes resulta ineludible disponer de políticas de gestión de personal en los que se definan de modo muy claro los perfiles funcionales de cada puesto, y de procedimientos de formación del personal. No es extraño por tanto que el RDLOPD ordene de modo específico ambos aspectos.

«1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento. (art. 89 RDLOPD)».

En determinados sectores como la sanidad la exigencia de fijar perfiles de usuario deriva de la Ley, que define de modo muy preciso el perfil funcional de cada tipo de trabajador.

«1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

(...)

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

(art. 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica)».

Las obligaciones de secreto y seguridad en materia de protección de datos constituyen deberes muy específicos vinculados al hecho del propio tratamiento y van más allá del secreto profesional en su concepción tradicional. Su inadecuado cumplimiento pone en riesgo el derecho fundamental a la protección de datos y causa habitualmente un grave perjuicio reputacional a la empresa.

Ej. El abandono de documentos sin destruir en la basura común por el personal de limpieza, es una de las infracciones más comunes en materia de protección de datos. Recientemente la ausencia de límites a la instalación de programas peer to peer, como el conocido e-mule, ha expuesto al acceso de cualquiera miles de datos de los ciudadanos.

Por todo ello es muy recomendable:

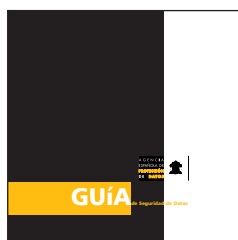
- Diseñar las funciones y responsabilidades de la plantilla de personal teniendo en cuenta su relación con el tratamiento de datos personales.
- Formar adecuadamente a los trabajadores teniendo en cuenta su distinto grado de responsabilidad y garantizando que conozcan sus deberes de seguridad y secreto. La formación debe contribuir a crear una cultura de compromiso con la protección de datos.
- Advertir y formar incluso a aquellos trabajadores que no teniendo una relación directa con los sistemas de información y los tratamientos de datos personales puedan poner en peligro el secreto o la seguridad de los mismos.

RECURSOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

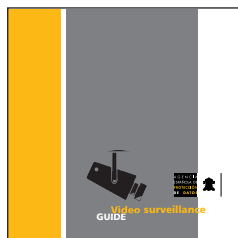
La Guía sobre protección de datos en las relaciones laborales tiene por objeto analizar aspectos concretos sobre esta materia. La Agencia Española de Protección de Datos dispone de un conjunto de Guías y recursos que le permitirán profundizar en esta materia y le ayudarán a aplicar adecuadamente la normativa vigente.



La Guía del Responsable de ficheros contiene indicaciones sobre los principios básicos que deben ser tenidos en cuenta para cumplir adecuadamente con la legislación sobre protección de datos.



La Guía de Seguridad de Datos le ayudará a implementar, revisar y aplicar las medidas de seguridad contenidas en el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal.



La Guía de Videovigilancia describe todas las cuestiones relacionadas con el tratamiento de imágenes y en particular las relativas a la seguridad y al uso con fines de control laboral.



El sistema de **NOT**ificaciones Telemáticas a la **AEPD (NOTA)**, permite a los responsables de ficheros con datos de carácter personal de titularidad pública y de titularidad privada cumplir con la obligación que la LOPD establece de notificar sus ficheros a la Agencia Española de Protección de Datos a través de una herramienta que le informa y asesora acerca de los requerimientos de la notificación. Se trata de una herramienta gratuita que permite notificar de forma simplificada una serie de ficheros relacionados con la gestión de comunidades de propietarios, clientes, libro recetario de las oficinas de farmacia, pacientes, gestión escolar, videovigilancia, nóminas y recursos humanos de titularidad privada.



EVALUA es un procedimiento de diagnóstico basado en un autotest o formulario con preguntas con respuesta múltiple. Basta con realizar el mismo para que al final la Agencia Española de Protección de Datos le facilite un informe con indicaciones y recursos que le orienten, en su caso para cumplir con lo dispuesto en la LOPD o verificar su estado de cumplimiento en relación con las medidas de seguridad.

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

