

¿Cómo afecta la normativa de protección de datos al departamento de recursos humanos de mi empresa?

Este artículo pretende poner de manifiesto los aspectos más trascendentes que en el ámbito de un departamento de recursos humanos de una empresa se deben tener en cuenta para cumplir con las exigencias establecidas por la legislación vigente en materia de protección de datos de carácter personal.

En primera fase, se debe analizar los datos de carácter personal que puede llegar a manejar un departamento de recursos humanos. En un sentido amplio, en un departamento de recursos humanos existe una gran variedad de datos personales tales como: datos identificativos, datos académicos, datos profesionales, datos económicos, datos formativos, datos sindicales, datos de salud, datos de absentismo laboral....etc.

En segundo lugar, se debe agrupar dichos datos en función de las finalidades a las que responden (entre otros criterios posibles), dando lugar a lo que la Ley Orgánica de Protección de Datos denomina “*fichero*”¹. Por tanto, se puede concluir que en un departamento de recursos humanos pueden obrar ficheros muy diversos entre otros y a modo de ejemplo, “**Nóminas**” “**Remuneraciones**”, “**Candidatos**”, “**Prevención de Riesgos Laborales**”, “**Control Horario**”, “**Seguridad**”, “**Vacaciones**”etc.

Una vez realizada esta fase de análisis y determinación de los distintos tipos de datos personales y como pueden ser agrupados, se procede a examinar, a grandes rasgos, cada uno de los requisitos principales que se han de tener en cuenta para cumplir con la normativa de protección de datos de carácter personal

1. INSCRIPCIÓN

Toda persona física o jurídica que trate datos de carácter personal debe proceder a la inscripción del fichero ante la Agencia Española de Protección de Datos de Carácter Personal, a través de los medios que dicho ente dispone al efecto (papel, soporte magnético o a través de Internet). Por tanto, se deberán declarar los ficheros que se hayan detectado en la fase de análisis.

Dejando a un lado los aspectos más generales de la inscripción tales como razón social de la empresa, dirección, ejercicio de derechos, descripción.....etc, reviste especial trascendencia a la hora de llevar a cabo la declaración del fichero el nivel de seguridad aplicable al mismo. El Reglamento de medidas de seguridad (RMS) establece tres tipos de medidas de seguridad diferentes aplicables a los ficheros en función del tipo de datos que contengan. Así, los ficheros pueden ser de nivel básico, cualquier fichero por el mero hecho de contener datos de carácter personal, de nivel medio, cuando alberga entre otros datos relativos a la administración pública, sanciones administrativas o penales, o de nivel alto, cuando contiene datos de los catalogados como especialmente protegidos, es decir salud, afiliación sindical...etc. A nivel doctrinal (artículo 4.4 RMS) se reconoce un cuarto nivel denominado básico cualificado o medio atenuado, aplicable bajo el criterio subjetivo de poseer suficientes datos para extraer un perfil de la personalidad del individuo. Los ficheros que frecuentemente se encuentran en los departamentos de recursos humanos de la empresa suelen ser de nivel básico o básico cualificado, si bien nada obsta a que sean catalogados de nivel alto si concurren en alguno de ellos, cualquiera de los siguientes datos, porcentajes de minusvalías, descuento de la cuota de afiliación sindical, absentismo laboral...etc

Otro dato que debe ser tenido en cuenta, es que no sólo deben ser declarados los ficheros automatizados sino también todos los ficheros no automatizados o en soporte papel (como pueden ser los ficheros de currícula o del resultado, apto o no apto, de los reconocimientos médicos que se realicen los trabajadores), si bien a este tipo de ficheros no les son aplicables las medidas de seguridad establecidas en el RMS puesto que éstas solo se refieren a ficheros

¹ Definición de fichero.

automatizados, si bien deben tomarse precauciones para garantizar la confidencialidad de los datos.

2. CONSENTIMIENTO / INFORMACIÓN

Son dos principios que están muy relacionados entre sí. La regla general es que para realizar cualquier tratamiento de datos de una persona se precisa su consentimiento si bien, la LOPD lo excepciona para determinados supuestos como el del artículo 6.2 que establece que *no será necesario el consentimiento cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*. Por ejemplo son necesarios los datos de los trabajadores para gestionar su vinculación laboral con la empresa, para hacer las nóminas...etc., si bien, el hecho de no precisar el consentimiento de los trabajadores para tratar sus datos personales no obsta que la empresa no cumpla con el deber de información, por tanto y en todo caso, la empresa debe informar al trabajador de:

- 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.

Destaca dentro de la información que las empresas deben dar a sus trabajadores para llevar a cabo el tratamiento de sus datos, el apartado de los destinatarios de la información dado que las empresas han de informar de todas las cesiones de datos que lleven a cabo, incluyendo las que realizan a determinados organismos públicos como son la Agencia Tributaria, Tesorería General de la Seguridad Social, Instituto Nacional de Empleo.....etc ya que el hecho de no precisar el consentimiento para realizar dichas cesiones, ya que hay una ley que las autoriza, no obsta para que los trabajadores sean informados.

La regla general de que la empresa no precisa el consentimiento de los trabajadores para llevar a cabo el tratamiento de sus datos personales, tiene sus excepciones dado que si la empresa trata datos especialmente protegidos (porcentajes de minusvalías, descuento de la cuota de afiliación sindical, absentismo laboral....) precisará el consentimiento expreso y habitualmente por escrito de los trabajadores.

Un supuesto que suele crear confusión en las empresas es el cumplimiento de los principios de consentimiento e información con respecto al tratamiento de los datos de las personas que remiten voluntariamente el curriculum vitae (c.v) a la empresa, ya que se suele entender que dichas personas o candidatos por el hecho de enviar c.v. están dando su consentimiento para el tratamiento de los datos. En este sentido y como se ha reflejado anteriormente consentimiento e información son cosas distintas y por tanto las personas aunque voluntariamente hayan enviado el c.v. deben de ser informadas de los postulados del artículo 5 LOPD, si bien es cierto que habitualmente no podrá realizarse con anterioridad a la recepción de los datos a no ser que la empresa tenga un medio articulado para ello, como por ejemplo que tenga un lugar en la página web destinado a la recepción de c.v.

Otra especialidad, en relación con el se centra en el apartado referido a la seguridad; si bien los empleados pueden ser informados en el contrato de trabajo de que van a ser grabados a la entrada del edificio, accesos, pasillos...etc es recomendable que se informe colocando carteles que recojan las medidas a las que anteriormente se ha hecho referencia. Además y dado que estos sistemas de seguridad suelen afectar tanto a empleados como a visitantes estos últimos en todo caso deben ser informados es conveniente la inserción de dichos carteles informativos.

3. CALIDAD DE LOS DATOS

Los datos personales de los trabajadores deben ser adecuados pertinente y no excesivos para las finalidades para las cuales fueron recabados, en este sentido y dependiendo de la finalidad que la empresa haya informado a sus trabajadores tratará los datos conforme a este principio o no.

La conservación de los datos que se hallan en el departamento de recursos humanos debe ir aparejada a la utilidad o vigencia del contrato que los origina. Por tanto, en la medida en que la relación entre el empleado y la empresa está vigente, se entiende justificado el mantenimiento de todos los datos que pudieran recabarse durante dicha relación contractual.

Con carácter general la empresa conserva los datos de los trabajadores al día puesto que los trabajadores deben comunicar a la empresa (por su propio interés) las modificaciones que se hayan producido en su situación personal, estado civil, hijos...etc para verse beneficiado de determinadas ventajas fiscales.

Por lo que se refiere al bloqueo y eliminación de los datos se estima que los datos deben ser bloqueados cuando se extingue la relación laboral, y conservados, en todo caso por un plazo no superior a 4 años. Este plazo incluiría las posibles reclamaciones que se puedan hacer tanto por infracciones relativas al tratamiento de los datos (3 años), las derivadas del contrato laboral (1 o 3 años, en caso de sucesión de empresas) o las derivadas de aspectos sociales (4 años).

En relación con los datos de los candidatos es recomendable imponer la obligación de mantener los datos actualizados en el propio interesado que remite su c.v., si bien y dado que esto no es habitual se recomienda que en el plazo máximo de 1 año desde su recepción se proceda a sus destrucción.

Por último, las grabaciones de las imágenes (seguridad) deben ser eliminadas transcurrido un mes desde que fueron efectuadas.

4. FLUJO DE DATOS (ACCESO POR CUENTA DE TERCEROS, CESIÓN DE DATOS Y TRANSFERENCIA INTERNACIONAL DE DATOS)

Dentro de este supuesto hemos de distinguir tres tipos de flujos:

- a) Cesión. Para poder ceder los datos de una persona se ha de contar en todo caso con el consentimiento del interesado y que la cesión responda a finalidades legítimas entre el cedente y el cesionario de los datos. No obstante hay cesiones que debido a que están autorizadas por una Ley están exceptuadas de dicho consentimiento. Algunos ejemplos característicos de cesiones que se producen dentro del ámbito de un departamento de recursos humanos son:
 - i. A la Agencia Tributaria
 - ii. Tesorería General de la Seguridad Social
 - iii. Instituto Nacional de Empleo
 - iv. En el supuesto de que se traten datos derivados de la realización de reconocimientos médicos, los datos del trabajador (habitualmente nombre y apellidos) son cedidos para la identificación de la persona que va a realizar las pruebas.
 - v. Entidades de seguros (vida, jubilación, accidentes...etc)
- b) Acceso por cuenta de terceros. Es frecuente que las empresas tengan externalizados determinados servicios relacionados con el departamento de recursos humanos. Por ejemplo la gestión de la nóminas, la seguridad....etc En estos casos los datos a pesar de que sena tratados por un tercero son responsabilidad de la empresa para la que los empleados trabajan, no obstante y dado que la gestión de dichos datos es realizada por otra compañía se articula un medio para garantizar en primer lugar los datos de los trabajadores así como para limitar las responsabilidades que pudieran surgir de un mal uso de los datos. Estas prestaciones de servicios se regulan en el artículo 12 de la LOPD que obliga a la

formalización de un contrato entre ambas empresas estableciéndose asimismo en dicho artículo el contenido mínimo que debe comprender.

- c) Son frecuentes también las transferencias internacionales de datos que suelen producirse como consecuencia de la cesión de los datos de los trabajadores a la matriz (sita en un país extranjero) o como consecuencia de la ubicación de los sistemas de información donde se albergan los datos personales fuera del territorio español.

Los requerimientos legales en relación con el flujo de datos en empresas pertenecientes al un mismo grupo empresarial está creando dificultades por la necesidad en muchos supuestos de articular numerosos contratos, es por ello, que desde hace tiempo se está trabajando en buscar una serie de protocolos que permitan garantizar la protección de los datos de carácter personal de los trabajadores al mismo tiempo que faciliten o más bien no dificultan con demasiados trámites burocráticos la realización de determinadas comunicaciones entre empresas pertenecientes a un mismo grupo.

5. DERECHOS DE ACCESO, RETIFICACIÓN, CANCELACIÓN U OPOSICIÓN A LOS DATOS

Realmente en cuanto a los derechos de los interesados el ejercicio de los derechos no presenta muchas novedades si bien que los datos no pueden proceder a cancelarse hasta que no finalice la relación que les une a la empresa.

Otro supuesto que puede ser destacado es el ejercicio del derecho de oposición que se ejerce cuando los empleados se oponen a determinados tratamientos que efectúa la empresa con sus datos personales. Por ejemplo el caso de un trabajador que se incorpora en una empresa que edita una revista y por el mero hecho de estar en nómina recibe dicha revista; en este caso, se debe distinguir dos tratamientos totalmente distintos el de la gestión de la nóminas y el envío de la revista, el primero de ellos es necesario para el mantenimiento de la relación laboral mientras que el segundo no lo es, por tanto el trabajador puede oponerse al tratamiento de los datos para el envío de la revista y que la empresa los mantenga exclusivamente para confección de la nómina.

6. MEDIDAS DE SEGURIDAD

El artículo 9 LOPD establece que para proteger los datos deben adoptarse una serie de medidas técnicas y organizativas para proteger la confidencialidad, integridad y confidencialidad de los datos personales. Estas medidas deben quedar comprendidas en el documento de seguridad que debe poseer toda entidad que trate datos de carácter personal. Las medidas de seguridad podrán ser de nivel básico, medio o alto en función del tipo de datos que se traten.

7. DEBER DE SECRETO

El artículo 10 LOPD establece el deber de secreto para todas las personas que intervengan en el tratamiento de datos, por tanto toda persona perteneciente al departamento de Recursos Humanos queda sujeto a este deber incluso tras finalizada la relación que le une a la entidad.

En conclusión y como se puede desprender del contenido del presente artículo sin duda el departamento de recursos humanos de una compañía tiene una trascendencia fundamental en orden al cumplimiento por parte de la entidad, de la normativa de protección de datos de carácter personal dado que en el mismo se contienen una gran parte de los datos personales existentes en una empresa.

Jesús Sánchez Echeverría
Director de Áudea, Seguridad de la Información, S.L.

