



LA PROTECCIÓN DE DATOS EN LAS RELACIONES LABORALES

Basado en la Guía AEPD (mayo 2021)



Índice

Concepto de tratamiento de datos personales	3
Base jurídica del tratamiento de datos personales	3
Información del tratamiento de datos personales	5
Derechos de protección de datos en el ámbito laboral	6
Principio de minimización	6
Deberes y obligaciones. Secreto y seguridad	7
Delegado/a de protección de datos	7
Transferencias internacionales de datos	8
Selección y contratación	9
Acceso a datos de otras personas candidatas	9
Desarrollo de la relación laboral	10
Datos biométricos	11
Sistema interno de denuncias - whistle blowing	12
Registro de jornada	12
Registro de salarios	12
Ayudas y acción social	13
Derechos de conciliación y corresponsabilidad	13
Seguros de vida y pensiones	14
Cesión de datos en grupos de empresas	14
Transmisión de empresas	15
Subcontratación	15
Protección de datos a víctimas de violencia de género y acoso	16
Extinción de la relación laboral	18
Cesión de datos de personas exempleadas a empresas de recolocación	18
Descuento de la cuota sindical	18
Control empresarial y protección de datos	19
Control de acceso	19
Vídeo vigilancia	19
Geolocalización	20
Tecnología weareable	20
Control por falta de asistencia por baja por contingencia profesional o común	21
Detectives privados	21
Tratamiento de datos por la RLT	22
Publicación de datos en tabloneros de anuncios	23
Comunicaciones de datos por mail	23
Periodos de consultas legalmente previsto	23
Vigilancia de la salud	24
Relación entre la empresa y el servicio de prevención	25

Concepto de tratamiento de datos personales



DATO PERSONAL (DP)	TRATAMIENTO	CATEGORÍA ESPECIAL DE DP
“Toda información relativa a una persona física identificada o identificable” (art. 4.1 RGPD)	Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registr o, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción (art. 4.2 RGPD).	Aquellas que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física y los datos relativos a la salud o datos relativos a la vida sexual u orientación sexual de la persona. (Art. 9.1 RGPD). Con carácter general el tratamiento de categorías especiales de datos personales está prohibido, salvo excepciones (art.9.2 RGPD).

Base jurídica del tratamiento de datos personales

El tratamiento de datos personales no puede realizarse por una razón de oportunidad, por la fácil obtención de estos o por si acaso en el futuro pudieran ser de utilidad, sino que exige que el responsable del tratamiento cuente con una «base jurídica» que le legitime para ello (conforme al art. 6.1 y art. 9.2 RGPD).

Art. 6.1 RGPD (bases jurídicas generales)

- a. El interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos.
- b. El tratamiento es necesario para la **ejecución de un contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas pre-contractuales.
- c. El tratamiento es necesario para el cumplimiento de una **obligación legal** aplicable al responsable del tratamiento.
- d. El tratamiento es necesario para proteger **intereses vitales** del interesado o de otra persona física.
- e. El tratamiento es necesario para el cumplimiento de una misión realizada en **interés público** o en el **ejercicio de poderes públicos** conferidos al responsable del tratamiento.
- f. El tratamiento es necesario para la satisfacción de **intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Art. 9.2 RGPD (bases jurídicas de excepción de la prohibición de tratamiento de datos de categoría especial).

El apartado 1 (prohibición de tratamiento de datos personales) no será de aplicación cuando concorra una de las circunstancias siguientes:

- a. La persona interesada dio su **consentimiento explícito** para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado (pero el art. 9.1 de la LOPDGD prohíbe el tratamiento de datos, aun con consentimiento del afectado, cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, a fin de evitar situaciones discriminatorias).
- b. El tratamiento es necesario para el **cumplimiento de obligaciones y el ejercicio de derechos específicos de la persona responsable del tratamiento o de la persona interesada en el ámbito del Derecho laboral y de la seguridad y protección social**.
- c. El tratamiento es necesario para **proteger intereses vitales** de la persona interesada o de otra persona física, en el supuesto de que la persona interesada no esté capacitada, física o jurídicamente, para dar su consentimiento;
- d. El tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, **por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical**.
- e. El tratamiento se refiere a datos personales que **la persona interesada ha hecho manifiestamente públicos**.
- f. **El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial**.
- g. El tratamiento es necesario **por razones de un interés público** esencial, sobre la base del Derecho de la Unión o de los Estados miembros.
- h. El tratamiento es necesario para **finés de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social**.
- i. El tratamiento es necesario **por razones de interés público en el ámbito de la salud pública**, como la protección frente a amenazas transfronterizas graves para la salud, o para **garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios**.
- j. El tratamiento es necesario con **finés de archivo en interés público, fines de investigación científica o histórica o fines estadísticos**.

El tratamiento de datos de las personas trabajadoras por parte del empleador es lícito:

1. Cuando sea necesario para la **ejecución de un contrato** en el que la persona interesada es parte o para la aplicación a petición de éste de medidas pre-contractuales (art. 6.1.b RGPD). La empresa podrá tratar datos como el nombre y los apellidos de las personas trabajadoras, su fecha de nacimiento, su sexo, su nacionalidad, su formación previa o cualesquiera otros imprescindibles para formalizar el contrato y ejecutar el trabajo.
2. «Para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento» (art. 6.1.c RGPD). Esta base jurídica permite el tratamiento de datos cuando sea necesario para cumplir las exigencias impuestas por la ley (por ejemplo, cotización a la Seguridad Social, obligaciones tributarias, registro de jornada, información y consulta con los representantes de las personas trabajadoras, etc.) o por un convenio colectivo.
3. La satisfacción de **intereses legítimos** perseguidos por la persona responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales de la persona interesada que requieran la protección de datos personales (art. 6.1.f RGPD). (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29: «En caso de que un empresario pretenda invocar un interés legítimo, la finalidad del tratamiento debe ser legítima; el método elegido o la tecnología específica deben ser necesarios, proporcionados y aplicados de la manera menos intrusiva posible, y el empresario deberá poder demostrar que se han adoptado las medidas adecuadas para garantizar un equilibrio con los derechos y libertades fundamentales de los trabajadores») ejemplo: datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica.
4. Excepcionalmente: protección de **intereses vitales** del afectado o de otra persona física.

- **Dictamen 2/2017** sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del art. 291) «Es muy poco probable que el **consentimiento** constituya una base jurídica para el tratamiento de datos en el trabajo, a no ser que los trabajadores puedan negarse sin consecuencias adversas [...] Salvo en situaciones excepcionales, los empresarios tendrán que basarse en otro fundamento jurídico distinto del consentimiento, como la necesidad de tratar los datos para su interés legítimo. Sin embargo, un interés legítimo en sí mismo no es suficiente para primar sobre los derechos y libertades de los trabajadores».
- **STS 21.09.2015 (Rec. 259/2014)**: A lo que exclusivamente nos oponemos es que en el contrato de trabajo se haga constar -como específica cláusula/tipo- que el trabajador presta su «voluntario» consentimiento a aportar los referidos datos personales y a que la empresa los utilice en los términos que el contrato relata, siendo así que el trabajador es la parte más débil del contrato y ha de excluirse la posibilidad de que esa debilidad contractual pueda viciar su consentimiento a una previsión negocial referida a un derecho fundamental, y que dadas las circunstancias -se trata del momento de acceso a un bien escaso como es el empleo- bien puede entenderse que el **consentimiento** sobre tal extremo **no es por completo libre y voluntario**.

Información del tratamiento de datos personales



DEBER DE INFORMAR

A las personas trabajadoras de forma concisa, transparente, inteligible y de fácil acceso con lenguaje claro y sencillo.

Se recomienda información por capas (**cláusulas informativas en documentos de captación de datos, correos electrónicos, avisos legales, carteles, etc + link al aviso legal Protección de Datos de la web**).

La inclusión de cláusula informativa en el contrato o mediante un anexo es un medio adecuado para cumplir con el derecho de información.



PLAZOS

Momento en el que se recaben los datos.

Si los datos no se obtienen del afectado, plazo máximo de un mes o con antelación a su uso.

La información no equivale a consentimiento

La empresa debe informar sobre nuevos tratamientos de datos posteriores al nacimiento relación laboral

Derechos de protección de datos en el ámbito laboral

1.- Derecho de Acceso (art. 15 RGPD).

2.- Derecho de Rectificación (art. 16 RGPD).

3.- Derecho de Supresión (art.17 RGPD). Se puede exigir supresión:

- Cuando los datos ya no sean necesarios.
- Cuando se haya retirado el consentimiento para su tratamiento.
- Cuando el tratamiento sea ilícito.
- Cuando la persona se oponga al tratamiento y no sea necesario para la ejecución y cumplimiento del contrato de trabajo.
- Por obligación Legal. Procedimiento de supresión:
 - a. Concreción periodo de uso y fin de la finalidad de uso.
 - b. Periodo de conservación de datos.
 - c. Periodo de bloqueo (los datos no pueden manipularse ni alterarse).

4.- Derecho a la limitación del Tratamiento (art. 18 RGPD).

- Inexactitud de datos personales.
- Ilícitud del tratamiento por el empleador.
- Datos no necesarios para el tratamiento.
- Oposición al tratamiento.

5.- Derecho a la portabilidad de datos (art. 20 RGPD).

6.- Derecho de oposición (art. 21 RGPD).

7.- Derecho a no ser objeto de decisiones individuales automatizadas (art.22 RGPD).

Principio de minimización

- La persona empleadora NO está legitimada para conocer cualquier tipo de dato personal bajo el pretexto de la relación contractual.
- El **principio de minimización** de datos exige que los datos personales sean adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que son tratados.
- Son datos personales **necesarios**: Nombre, sexo, DNI, NASS, nacionalidad, discapacidad, fecha de nacimiento.
- Son datos **no imprescindibles**: nombre usuario redes, cesión derechos de imagen...
- Se deberán **ponderar su necesidad** con respecto a la realización del contrato: domicilio, email, número de teléfono o cuenta bancaria.



Deberes y obligaciones. Secreto y seguridad

El art. 5 LOPDGDD

- Deber de confidencialidad (por ejemplo, mantener las mesas de trabajo limpias de documentación).
- Secreto Profesional.

Es necesaria una Política de Gestión de personas:

- Definición de los perfiles de acceso.
- Definición de procedimientos de formación.

Recomendaciones:

- Diseñar las funciones y responsabilidades de los miembros de RRHH.
- Formar a las personas de RRHH.
- Advertir y formar a otras personas que pudieran tener contacto con datos.
- Consultar dudas con carácter previo al delegado/a de protección de datos.

Delegado/a de protección de datos

Art. 39 RGPD (funciones del Delegado de Protección de Datos):

- **Informar y asesorar** a las y los empleados que se ocupen del tratamiento de las obligaciones que les incumben.
- **Supervisar** el cumplimiento de la normativa de Protección de Datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el **asesoramiento** que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y **supervisar** su aplicación.
- **Cooperar** con la autoridad de control (Agencia Española de Protección de Datos)
- Actuar como **punto de contacto** de la autoridad de control para cuestiones relativas al tratamiento y realizar **consultas**.
- Desempeñar sus funciones prestando la debida atención a los **riesgos** asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.



Transferencias internacionales de datos

Tienen tal consideración, las transmisiones de datos personales fuera del Espacio Económico Europeo (EEE), ya constituyan una comunicación de datos a otros responsables del tratamiento, en cuyo caso exportador e importador son responsables del tratamiento, ya tengan por objeto la prestación de servicios por un encargado del tratamiento establecido fuera del EEE. En este último caso el exportador puede ser un responsable o un encargado del tratamiento y el importador de los datos un encargado o subencargado del tratamiento.

El RGPD ha venido a simplificar el régimen de transferencias internacionales:

- Con el RGPD, se suprime la obligación de notificar a la AEPD las transferencias de datos a países que disponen de una decisión de adecuación, o si se realizan en aplicación de alguna de las excepciones previstas en el art. 49 del RGPD, salvo cuando, dada su singularidad, las transferencias son realizadas por un responsable del tratamiento por motivos legítimos e imperiosos y siempre que, además, se cumplan el resto de los requisitos que se exigen en el art. 49.1 párrafo segundo del RGPD.
- Se suprime también, con carácter general, la obligación de obtener la autorización previa de la AEPD cuando las transferencias se basen en la aportación de garantías adecuadas, que sólo será necesaria cuando las garantías aportadas para la transferencia se recojan en un contrato que no se ajuste al clausulado tipo aprobado por la Comisión Europea, o adoptado por una autoridad de control y aprobado también por la Comisión Europea, o cuando las garantías se incluyan en acuerdos administrativos para transferencias entre autoridades u organismos públicos.

Por tanto, las transferencias internacionales de datos se podrán realizar sin necesidad de autorización de la Autoridad de Control:

- a. Cuando tengan por destinatario una entidad establecida en alguno de los países o territorios declarados de nivel adecuado de protección por la Comisión Europea
- b. Cuando se aporten garantías adecuadas por las que los afectados cuenten con derechos exigibles y acciones legales efectivas mediante:
 - Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
 - Normas corporativas vinculantes para el caso de compañías multinacionales.
 - Cláusulas contractuales tipo adoptadas por la Comisión Europea, o por una autoridad de control y aprobadas por la Comisión Europea.
 - Un código de conducta, o un mecanismo de certificación.
- c. Cuando se diera alguna de las circunstancias excepcionales previstas en el art. 49 del RGPD, como el consentimiento explícito del afectado, o cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del tratamiento.

Requerirán la autorización previa de la AEPD cuando las garantías adecuadas se aporten mediante:

- Cláusulas contractuales específicas
- Acuerdos administrativos entre las autoridades u organismos públicos

De las transferencias internacionales de datos se ha de informar a los afectados e incluirlas en el registro de actividades de tratamiento (arts. 13 y 30 RGPD).



Selección y contratación

- El tratamiento de datos durante el proceso de selección **no exige el consentimiento**.
- Es conveniente disponer de **impresos tipo** para recabar currículos y tener procedimiento para su entrega.
- Si el currículo es remitido por el interesado: **procedimiento** de información de su **recepción**.
- La empresa es **responsable de la custodia de la documentación** entregada por el candidato
- Solo se han de recabar los **datos estrictamente necesarios (minimización y limitación de la finalidad)**.
- **Son datos personales las impresiones o valoraciones subjetivas que se realicen en el proceso de selección.**
- El candidato no está obligado a permitir a la empleadora la **indagación en redes sociales** ni durante el proceso de selección ni durante la ejecución del contrato:
 - El empleador no puede tratar los datos recabados en redes sociales.
 - Principio de **proporcionalidad, intervención mínima y derecho de información**.
- Las respuestas de la entrevista de trabajo no suponen a una autorización tácita al tratamiento de datos.
- Las **ETTs** serán las responsables del tratamiento de los datos de la persona puesta a disposición.
- No es admisible que la utilización de **algoritmos** produzca discriminación.
- Se ha de contemplar la intervención humana si la persona lo solicita, y un cauce para que el candidato manifieste su opinión y pueda impugnar la decisión.

Datos especialmente sensibles

1.- Reconocimientos médicos:

- Idoneidad para el empleo futuro.
- Cumplir requisitos medicina preventiva.

2.- Pruebas psicotécnicas o psicológicas:

- Consentimiento.
- Proporcionalidad.

La persona candidata podrá acceder a:

- Los resultados del proceso y conocer los criterios de selección.
- Pero **no tendrá acceso a los datos del resto de personas candidatas**.

Concluido el periodo de selección

- Si la **persona candidata no es seleccionada** se ha de **recabar consentimiento para un futuro tratamiento de los datos** (base de datos para futuras vacantes).
- En caso contrario se ha de destruir el curriculum y proceder a la supresión y bloqueo de los datos personales.

Acceso a datos de otras personas candidatas

- En general, la empresa empleadora no puede difundir datos personales de una persona trabajadora entre sus compañeros sin el consentimiento del afectado, pero la sentencia del TSJUE 19/04/2012: Derecho a conocer la información oportuna para realizar una reclamación al considerar que ha existido discriminación en el acceso al empleo o la promoción profesional.
- Concurrencia competitiva; derecho a conocer información sobre cualificación profesional de otros candidatos y, en particular, de quienes han obtenido mayor valoración.
- Compatible con la protección de datos:
 - No requiere el consentimiento de los afectados.
 - Principio de minimización de datos (no debe proporcionarse al solicitante un currículum completo de las otras personas candidatas, sino limitado a la formación, experiencia profesional y los datos estrictamente relevantes para formalizar la reclamación. No deberá permitirse el acceso como regla general a la siguiente información: nombre, fotografía, dirección postal o de correo electrónico.
 - Principio de finalidad.
 - Los datos han de ser disociados.
- Dependiendo de la finalidad de la reclamación podrá acceder a datos concretos como edad, raza o sexo.

Desarrollo de la relación laboral

- Los datos han de ser: **Adecuados, pertinentes y limitados**.
- Se debe **informar** a las personas de los **cambios** que afecten al tratamiento de sus datos.
- **No** hay que recabar **datos superfluos o excesivos** que impliquen el conocimiento de información adicional no necesaria para el desarrollo de la actividad.
- Hay que aplicar el **principio de proporcionalidad** en el tratamiento de datos.
- **Principio de minimización**.

1.- Identificación de personas ante clientes

- Exigencia de tarjetas identificativas con nombre y apellidos con cautelas:
 - Actividades cara al público o por razones de seguridad.
 - Información mínima imprescindible para facilitar identificación.
- Podrían utilizarse fotografías sin necesidad de consentimiento respetando el principio de limitación de la finalidad.

2.- Publicación de datos de actividad

- Ponderación entre el interés legítimo y la lesión de los derechos e intereses de los afectados:
 - Base jurídica.
 - Ponderación de los intereses.
 - La publicación no puede ser indiscriminada.
 - Debe de realizarse del modo menos perjudicial.
 - No puede ser utilizada para futuros tratamientos.

3.- Nóminas

- No debe figurar información superflua o adicional (por ejemplo, mención filiación sindical).
- Recomendación: que no figure la cuota sindical como tal en nomina por el acceso que pudieran tener a la nomina terceros para otras utilidades.

4.- Categorías especiales de datos personales

- El tratamiento de categorías especiales de datos personales **está prohibido con carácter general**.
- Será lícito (art. 9.2 RGPD):
 - Si media consentimiento*.
 - Cuando sean necesarios para la perfección y desarrollo de la actividad laboral.
 - Cuando sea efectuado en el ámbito de su actividad legítima.
 - Cuando sean datos manifiestamente públicos.
 - Cuando sean necesarios para formular reclamaciones.
 - Fines de medicina preventiva o laboral, evaluación de la capacidad laboral de la persona trabajadora.

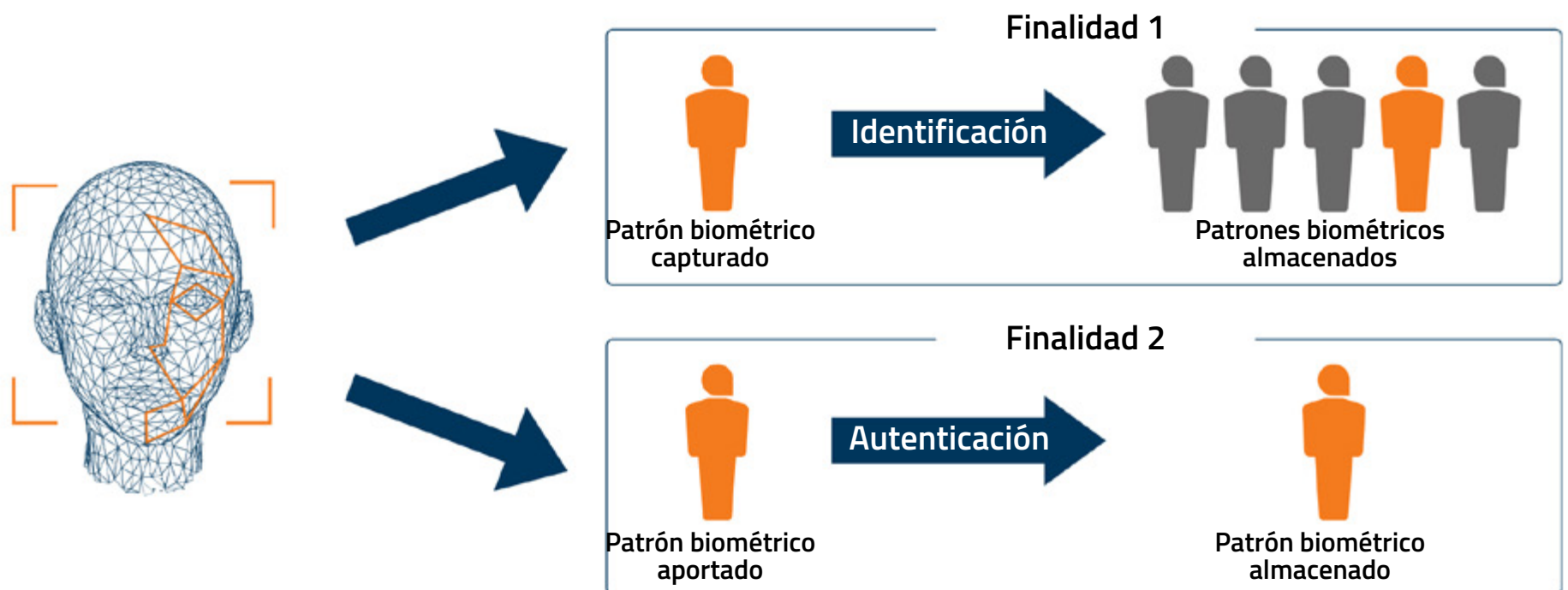
**Pero hay datos que no pueden tratarse ni con consentimiento – art. 9.1 LOPDGDD: ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.*

No existe legitimación para exigir datos sobre:

- Afiliación sindical
- Ideología política
- Creencia religiosa
- Orientación sexual

Datos biométricos

- Solo constituirán una categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física.
- Diferencia entre verificación o **autenticación** (uno a uno) biométrica e **identificación** (uno a varios).
- Solo tienen la consideración de categoría especial los casos en los que se trate de identificación no en los casos de verificación/autenticación.
- Potestad del empresario (art. 20.3 ET).



Garantías:

- La persona trabajadora debe ser informado.
- Las empresas fabricantes han de incorporar en el sistema la protección de datos (borrados automáticos).
- Plantillas biomédicas.
- Almacenamiento.
- No reutilizables para otra finalidad.
- Mecanismo basado en tecnologías de cifrado.
- Supresión cuando decaiga la finalidad de su recogida.
- Evaluación de impacto.



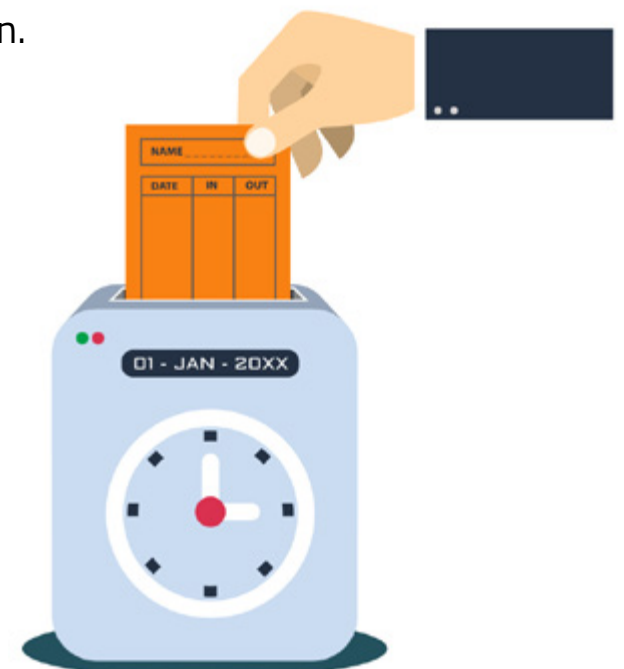
Sistema interno de denuncias - whistle blowing

- Tanto las personas denunciantes como las denunciadas deben tener constancia de la existencia del sistema y del tratamiento de los datos (conocimiento Individual o colectivo)
- Principio de proporcionalidad.
- Principio de limitación de la finalidad.
- Acceso al compliance officer o la persona encargada del tratamiento.
- El departamento de RRHH solo accederá a los datos en el caso de procedimiento disciplinario.
- Los datos solo se conservarán (en el sistema o herramienta de denuncias) durante el tiempo necesario para la investigación, en todo caso 3 meses.



Registro de jornada

- Art. 34.9 ET: horario de inicio y fin de jornada. 4 años de plazo conservación.
- Se trata de tratamiento de datos al permitir identificar a la persona.
- Hay que tener en cuenta:
 - Tiene que ser lo menos invasivo posible.
 - Base jurídica y obligación legal.
 - Se puede transmitir a la Inspección de Trabajo.
 - Derecho de información y todos los derechos de LOPD.
 - Incluido en registro de actividades del tratamiento.
 - Evaluación de impacto.
 - Principio minimización.
 - No puede tener acceso público ni ser visible terceros
 - La empresa empleadora es la responsable de tratamiento.
 - El único fin es el control de jornada, principio de finalidad.



Registro de salarios

- Art. 28.2 ET Obligación legal.
- No justifica el tratamiento de datos.
 - Valores medios de salarios
- Datos disociados no personales (podrían ser personales en casos de pocas personas).
 - Se aplican medidas de seguridad, obligación de informar y confidencialidad.
- No se contempla un derecho a la información, ni al ejercicio de los derechos de acceso, rectificación, oposición y supresión al no ser un tratamiento de datos personales.
- La consulta al registro está regulada por ley.



Ayudas y acción social

- La base jurídica del tratamiento: el contrato de trabajo y el convenio colectivo/pactos de empresa.
- La persona trabajadora tienen derecho a ser informada sobre protección de datos.
- La RLT (representación legal trabajadores): art. 64.7 b) ET derecho a participar en la gestión o tramitación de la ayuda social de la empresa y, por ello, a acceder a un listado de las personas trabajadoras beneficiarias de la acción social en el ejercicio de las funciones representativas.
- Principio de minimización de los datos.
- En cuanto a la publicidad de la concesión:
 - Cuando no sea de concurrencia competitiva se individualiza.
 - Cuando es concurrencia competitiva las personas solicitantes podrán conocer los resultados con los datos estrictamente necesarios (no página web ni tablón público).
 - Si nos encontramos con categorías especiales de datos (por ejemplo, ayuda discapacitados) se ha de anonimizar (la publicidad de la concesión de la ayuda no ha de permitir la identificación de la persona afectada).



Derechos de conciliación y corresponsabilidad

- El tratamiento de datos personales de la persona trabajadora por parte de la empresa es necesario para la concesión y gestión de solicitudes relativas a la suspensión del contrato (suspensión y excedencias, arts. 45 a 47 del ET), permisos (art.37 del ET) y modificaciones de jornada (art. 34.8 del ET), que tienen como finalidad la articulación de derechos de conciliación de la vida laboral, personal y familiar. En muchos supuestos, el ejercicio de estos derechos implica el tratamiento de datos personales de un tercero, como hecho causante de los mismos.
- Base jurídica: el contrato de trabajo y el convenio/pactos de empresa.
- Puede implicar el tratamiento de categoría especial de datos al hacer referencia el permiso, por ejemplo, a datos de salud de familiares.
- La posibilidad del tratamiento de datos de categoría especial art. 9.2.b) RGPD, pudiendo los convenios establecer garantías al respecto.
- Principio de minimización de los datos.



Seguros de vida y pensiones

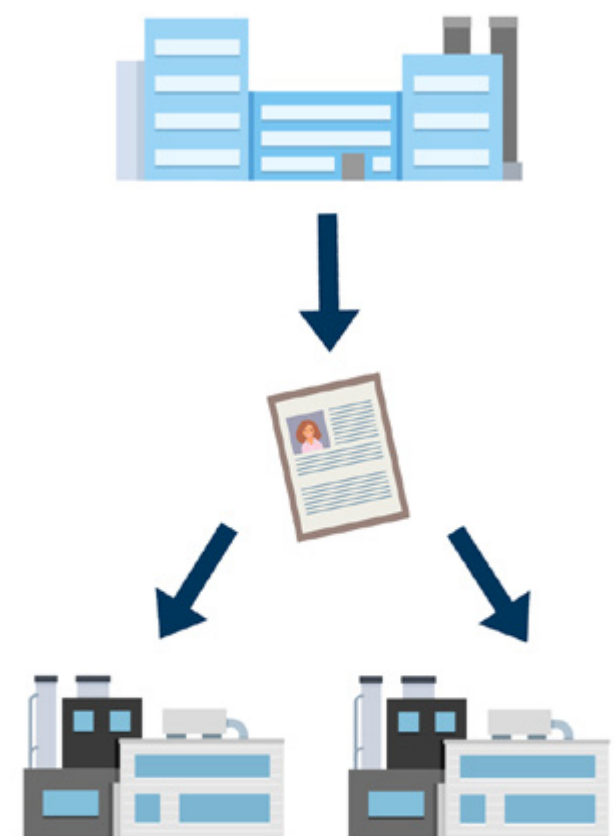
- Base jurídica: el contrato de trabajo y el convenio/pactos de empresa.
- La empresa puede realizar diferentes tipos de tratamiento:
 - Comunicación de los datos de identificación y contacto a la compañía aseguradora.
 - Recogida de datos vinculados al contrato.
- En todo caso es necesario informar a la persona.
 - En el contrato de trabajo.
 - Información específica.
- Puede existir datos de familiares o personas relacionadas con la persona trabajadora: principio de minimización y limitación de la finalidad.
- Debe definirse el procedimiento de captación de datos personales.
- Se recomienda la cesión de los datos a la compañía, dejando en sus manos la realización e otras gestiones e informando previamente a la persona.



Cesión de datos en grupos de empresas

- El RGPD menciona expresamente a los grupos de empresas en varios pasajes:
 - Designación de un único delegado de protección de datos para todas las empresas del grupo (art. 37.2). El RGPD alude a los grupos de empresas.
 - Consulta previa a la autoridad de control (art. 36).
 - Contenido de las normas corporativas vinculantes (art. 47).
 - Comunicación de datos entre las empresas del grupo (art. 88).
- Con carácter general, la comunicación de los datos entre empresas del mismo grupo exigirá acreditar un interés legítimo*, bien del responsable del tratamiento, o bien del tercero al que se comunican los datos.
- Pero, no es acorde al derecho a la protección de datos una organización interna de un grupo empresarial que centralice la información de todas las personas trabajadoras en un solo fichero, de modo que quien acceda al mismo pueda comprobar datos de las personas trabajadoras de las distintas empresas sin los filtros pertinentes, salvo que se celebre un contrato como encargado del tratamiento.

**Cuando se produce una prestación de servicios indiferenciada en varias empresas del grupo, la comunicación de datos entre esas empresas resulta lícita, porque es necesaria para el cumplimiento ejecución del contrato de trabajo. Pero la comunicación de esos datos debe respetar el principio de minimización y no pueden ser utilizados con una finalidad incompatible.*



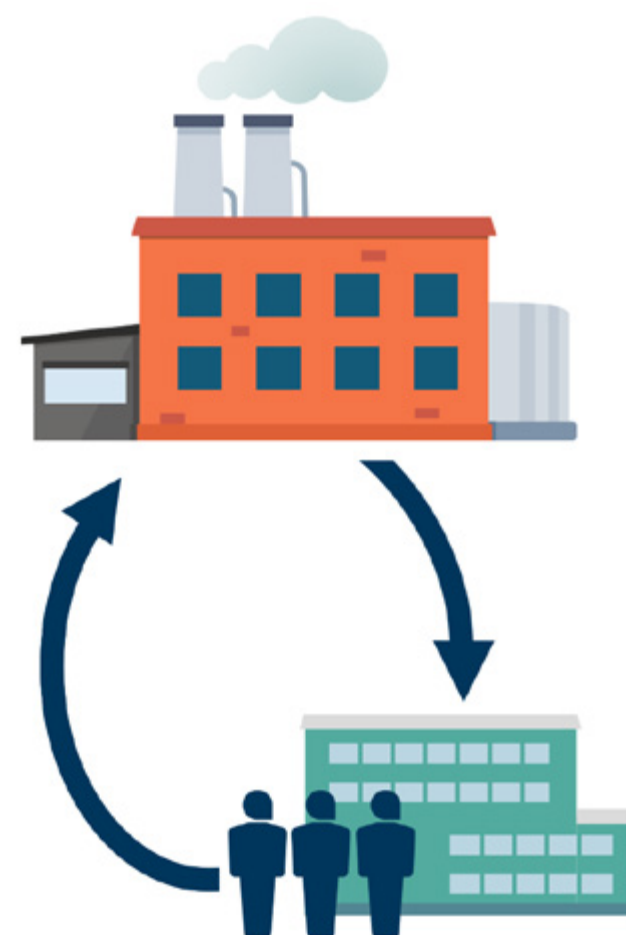
Transmisión de empresas

- En estos casos la comunicación de datos no requiere consentimiento de los afectados en supuestos de subrogación empresarial.
- La base jurídica no es el consentimiento de la persona trabajadora, sino la obligación establecida en el art. 44 del ET, el convenio colectivo o el pliego de cláusulas, según los casos.
- La nueva empresa empleadora tiene derecho a conocer y tratar datos personales de las personas trabajadoras imprescindibles para la ejecución y mantenimiento del contrato.
- La cesión de datos no es lícita si la persona trabajadora rechaza la subrogación y decide permanecer en la empresa cedente.
- Las personas trabajadoras y sus representantes legales deben ser informados de la cesión de datos.



Subcontratación

- Art. 42 ET (responsabilidad solidaria empresa principal/contrata) por las deudas salariales y de Seguridad Social contraídas por las empresas contratistas y subcontratistas durante la vigencia de la contrata.
- Art. 168 LGSS: Responsabilidad subsidiaria en materia de prestaciones de Seguridad Social.
- El cumplimiento de esas obligaciones legales (art. 6.1.c) del RGPD), puede exigir la comunicación de datos personales de las personas trabajadoras entre el empleador principal y otras empresas de la cadena de contratas.
- Dos supuestos:
 - Momento previo a la contratación.
 - Momento posterior respecto de la responsabilidad solidaria.
- A la obligación de comprobar, previamente a la contratación, que las empresas subcontratadas se encuentran al corriente en el pago de cuotas a la Seguridad Social de las personas empleadas en la contrata por parte del empleador principal, se añade la posibilidad de comprobar que el subcontratista ha cursado su afiliación y alta en la Seguridad Social. Esta legitimación alcanzaría a los documentos de cotización y nóminas de las personas trabajadoras.
- Al tener responsabilidad solidaria o subsidiaria, dependiendo del caso, no exige consentimiento la comunicación de datos.
- Las nóminas pueden contener datos de categorías especiales en este caso la legitimación estaría en el art. 9.2.b) en relación con 6.1.c) RGPD.
- Principio de minimización.



Protección de datos a víctimas de violencia de género y acoso

Los datos personales relativos a las víctimas de acoso en el trabajo y a las mujeres supervivientes a la violencia de género, y en particular su identidad, tienen, con carácter general, la consideración de categorías especiales de datos personales y, en todo caso, son datos sensibles que exigen una protección reforzada (Informe AEPD 149 - 2019).

Violencia de género

El empleador podrá conocer y tratar los datos de una trabajadora vinculados a la condición de mujer superviviente a la violencia de género cuando así resulte necesario para el cumplimiento de las obligaciones legales pertinentes; modificación del tiempo de trabajo, traslado, reordenación del tiempo de trabajo, suspensión o extinción del contrato, bonificaciones por contratos de interinidad para sustituir a las trabajadoras supervivientes a la violencia de género.

En tales casos:

1. El tratamiento de datos personales sólo procede cuando la trabajadora solicita ejercitar un derecho reconocido por esa condición de superviviente a la violencia de género, o cuando la empresa empleadora tiene un interés legítimo y siempre que dicha condición se haya comunicado voluntariamente por parte de la trabajadora. Por ejemplo, comunicación a la entidad gestora a efectos de aplicar reducciones en las cuotas de cotización a la Seguridad Social.
2. La empresa empleadora no podrá exigir más datos que la acreditación de la condición de mujer superviviente a la violencia de género.
3. La empresa no podrá tratar esos datos con una finalidad distinta de la establecida en las leyes.
4. La condición de superviviente a la violencia de género no será revelada por el empleador sin consentimiento de la trabajadora si no es exigencia para el cumplimiento de las obligaciones correspondientes.
5. La documentación de la empresa debe evitar la expresión "superviviente a la violencia de género" y sustituirla por un código o referencia que no permita que terceros puedan asociar con la superviviente esa condición.
6. Una vez concluida la relación laboral debe procederse al bloqueo/supresión de los datos.
7. La RLT únicamente podrán conocer la identidad de la superviviente a la violencia de género cuando sea imprescindible para el ejercicio de sus labores de representación.
8. La empresa debe informar a la superviviente a la violencia de género sobre el tratamiento de datos y sobre el ejercicio de los derechos de acceso, rectificación, oposición y supresión.
9. A diferencia de las situaciones de acoso, la superviviente a la violencia de género sí puede ejercitar el derecho de supresión en cualquier momento

Los datos personales de las mujeres supervivientes de violencia de género deben ser objeto de tratamiento con mucha cautela, pues cabría incluso incurrir en delito por un tratamiento inadecuado.



Acoso

En supuestos de ACOSO en el ámbito laboral, la empresa deberá adoptar las medidas oportunas de protección de los datos personales respecto del acosador, pero también de la persona acosada.

A tener en cuenta:

1. La puesta en marcha de procedimientos sancionadores en la empresa frente al acosador no requiere del consentimiento de la persona acosada. La base jurídica es el cumplimiento de una obligación legal (art. 6.1.c) RGPD): Obligación de la empresa ligada a su posición de garante de salud y seguridad en el trabajo, conforme a los artículos 4.2.d) del ET y 14 de la Ley Prevención de Riesgos Laborales (LPRL). La empresa está obligada a prevenir e identificar las prácticas de acoso y a erradicar, en su caso, las situaciones de acoso en la empresa.
2. En la investigación sobre lo sucedido sólo se podrá solicitar a la persona acosada información pertinente para el esclarecimiento de los hechos.
3. Los datos de la víctima obtenidos durante la investigación no se podrán utilizar para una finalidad distinta a la del procedimiento sancionador, sin perjuicio de las restantes obligaciones legales que incumben a la empresa (como la obligación de poner los hechos en conocimiento de la Justicia en caso de tratarse de un delito público).
4. La empresa debe garantizar la confidencialidad. La identidad de la víctima sólo será revelada ante las personas con interés en el procedimiento, no siendo admisible una publicidad masiva o indiscriminada sin consentimiento de la víctima, ni tampoco el acceso a los datos de personas no legitimadas. Deberá asignarse un código identificativo tanto a la persona supuestamente acosada como a la supuestamente acosadora, con objeto de preservar la identidad de estas.
5. La víctima debe prestar su consentimiento para declarar o testificar en los procedimientos sancionadores frente al acosador.
6. Una vez concluido el procedimiento sancionador, los datos deben ser bloqueados durante el período de prescripción de la sanción, o en tanto puedan ser utilizados en un procedimiento judicial.
7. La identidad de la víctima de acoso no deberá constar en ningún documento que se utilice con finalidad distinta a la sanción a la persona acosadora. Tampoco debería figurar el acoso como razón para la adopción de medidas correctoras en el puesto de trabajo.
8. La RLT únicamente podrán conocer la identidad de la víctima de acoso si es imprescindible para el ejercicio de sus labores de representación.
9. La empresa debe informar a la persona acosada y a la supuestamente acosadora sobre el tratamiento de datos y sobre el ejercicio de los derechos de acceso, rectificación, oposición y supresión. No obstante, el derecho de supresión no puede ser ejercitado si la empresa decide sancionar al acosador, pues en tal caso la base jurídica del tratamiento no es el consentimiento, sino el cumplimiento de una obligación legal y la ejecución del contrato de trabajo, en el que se incluye el ejercicio de la potestad sancionadora.
10. Cuando la persona acosada ha recibido asistencia sanitaria derivada de esa situación, los datos médicos constituyen datos personales de categoría especial que sólo pueden ser objeto de tratamiento con una finalidad vinculada al acoso. Por ejemplo, prueba en el proceso sancionador frente al acosador.
11. La cesión de los datos de la víctima requiere su consentimiento, salvo previsión legal en contra.



Extinción de la relación laboral

- La carta de despido puede contener datos personales y de terceros siempre que se cumpla el principio de finalidad
- Se implementarán medidas para que a la carta no puedan tener acceso terceros que no estén legitimados.
- A la finalización de la relación laboral se deberá proceder al bloqueo de los datos (No obstante, el tratamiento de datos tras la extinción del contrato podría ser admisible si existe otra base jurídica, como sucederá si la empresa empleadora demuestra un interés legítimo)
- En el caso de que se quiera contactar con la persona en un futuro se deberá recabar su consentimiento.



Cesión de datos de personas exempleadas a empresas de recolocación

- Las empresas que lleven a cabo un despido colectivo que afecte a más de 50 personas trabajadoras deben ofrecer a los afectados un plan de recolocación externa a través de empresas autorizadas (art. 51.10 del ET).
- La comunicación de datos entre la empresa que procede al despido y la empresa de recolocación es un tratamiento de datos que no exige el consentimiento de la persona trabajadora, pues la base jurídica es el cumplimiento de una obligación legal.
- En todo caso, la persona trabajadora tiene derecho a recibir la información de la empresa sobre ese tratamiento de datos y a ejercer los derechos de acceso, rectificación o supresión.
- No obstante, ese tratamiento debe respetar el principio de minimización de datos, por lo que sólo han de proporcionarse los datos imprescindibles para efectuar el ofrecimiento, como la identidad y una forma de contacto. El tratamiento de otros datos que puedan ser necesarios para desarrollar el plan de recolocación será lícito una vez que la persona trabajadora haya aceptado participar en el mismo.

Descuento de la cuota sindical

- El art. 9.1 del RGPD prohíbe el tratamiento de datos personales que revele la afiliación sindical. No obstante, el art. 9.2 del RGPD contiene excepciones respecto de esa prohibición: la recogida en su apartado d), dentro de las actividades legítimas del sindicato, y siempre con el consentimiento de la persona afiliada, el sindicato puede proceder a la comunicación del dato de afiliación a la empresa a efectos del descuento de la cuota sindical.
- En el preámbulo de la LOPDGDD se aclara que es lícito el tratamiento de datos personales por parte de la empresa relativo a la afiliación sindical con la finalidad de descuento de la cuota sindical.
- El tratamiento de datos sobre la afiliación sindical por el empleador es lícito cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo (art. 9.2.b RGPD).
- La empresa procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de éste (art. 11.2 de la LOLS).

Control empresarial y protección de datos

- Legitimación: Art. 20.3 ET
- La implantación de medidas de control exige realizar un test de proporcionalidad:
 - Susceptible de conseguir el objetivo propuesto (idoneidad).
 - Es necesaria.
 - Proporcional.
- Superado el test se implantará respetando la LOPD:
 - Deber de información sobre la finalidad del tratamiento de datos.
 - Se implementaran medidas para que a la carta no puedan tener acceso terceros que no estén legitimados.
 - Principio minimización de datos.
 - Principio de finalidad.

Control de acceso

- No necesita consentimiento de la persona trabajadora para establecer controles de acceso.
- Base jurídica: el contrato de trabajo.
- Se han de evitar sistemas invasivos de derechos fundamentales si existen otras posibilidades.
- Datos Biomédicos.



Vídeo vigilancia

- La imagen es un dato personal.
- Finalidad: control laboral versus seguridad de instalaciones y personas.
- Pueden tratarse las imágenes para el control de las personas:
 - La base jurídica el contrato y el art. 20.3 ET.
 - Solo se utilizará cuando no haya otro medio (menor impacto y proporcionalidad).
 - Principio de minimización:
 - Sólo las cámaras necesarias.
 - Requisitos técnicos de las cámaras (zoom o cámaras domo"
 - Los monitores de grabación solo deberán ser visualizados por los encargados de grabación.
- Información expresa, clara, concisa de la medida personas y RLT.
- Comisión de un delito detectado con la cámara.



- No se aplica la normativa protección de datos a cámaras simuladas.
- Prohibidas en lugares destinados al descanso (vestuarios, aseos, comedores, etc.)
- Se han de implantar medidas de seguridad acorde al riesgo.
- Subcontratas: El tercero se convierte en encargado de tratamiento.
- Suspensión de los datos: 1 mes desde la captación, salvo que tuvieran que ser conservados por la comisión de un ilícito.
- Art. 89 LOPDGDD limita la utilización de grabación de sonidos en el lugar de trabajo (proporcionalidad, intervención mínima).

Geolocalización

- El Art. 90 LOPDGDD lo posibilita
- Base jurídica: el contrato de trabajo
- Información expresa, clara, concisa de la medida personas y RLT.
- Información a las personas sobre el derecho de acceso, rectificación, limitación de tratamiento y supresión.
- Principios de minimización y limitación de finalidad.
- Principio de proporcionalidad.
- La geolocalización se puede aplicar a las herramientas y no a las personas. En los vehículos, en principio es lícito, pero también implica la geolocalización de la persona. Cautelas en este caso:
 - Evaluación de impacto, proporcionalidad y subsidiaridad.
 - Los datos deben tratarse con un fin específico no uno amplio.
 - Se deben limitar los fines específicos
 - Quien utilice herramientas con geolocalización debe ser informada sobre el seguimiento y la finalidad de su utilización.
 - No es lícito que la persona facilite su operativo para facilitar la geolocalización (teléfono móvil).
 - Hay que acreditar un fin legítimo, proporcionalidad y minimización.



Tecnología weareable

La monitorización por la empresa de datos de salud de sus personas trabajadoras (dada la relación desigual entre empresas y personas trabajadoras y la naturaleza sensible de los datos de salud, las personas trabajadoras no son verdaderamente «libres» para consentir) a través de dispositivos inteligentes, como pulseras o relojes, está, por lo general, prohibida, a menos que esté establecida por ley o reglamentariamente, ya que:

- No se enmarca en la vigilancia de la salud propia de la prevención de riesgos laborales.
- Supone el tratamiento de una categoría especial de datos (salud) sin una base jurídica.
- No cuenta con una finalidad legítima.
- Vulnera el principio de proporcionalidad, porque conlleva una monitorización permanente y permitiría al empleador acceder a datos de salud específicos, y no exclusivamente a la valoración sobre la aptitud de la persona trabajadora para desempeñar el trabajo.

Incluso si el empleador utiliza a un tercero para recopilar los datos de salud, el tratamiento seguiría siendo ilícito, salvo que se acreditase un interés legítimo, una finalidad específica, una monitorización proporcional, o bien que se garantizase la anonimización completa de los datos.



Control por falta de asistencia por baja por contingencia profesional o común

El art. 20.4 ET posibilita al empresario realizar controles médicos a los trabajadores cuando se abonan complementos de I.T. Las características de estos controles son:

- Tratamiento de datos de salud, categoría especial de datos.
- Base jurídica: contrato de trabajo y ET
- No se pueden conocer los detalles concretos del diagnóstico/reconocimiento médico. Sólo si está o no en condiciones psicofísicas para reincorporarse la trabajo.
- La incorporación de datos de salud a un fichero con datos personales para controlar absentismo se estima desproporcionada.
- STS 481/2018, de 25 de enero, se puede subcontratar con una empresa el control.
- La empresa puede elaborar estadísticas de absentismo (datos disociados) la RLT tiene derecho a conocerlos.

Detectives privados

El art. 20.3 ET posibilita su utilización.

- Hay que realizar test de proporcionalidad.
- No requiere el consentimiento del tratamiento.
- Prohibido investigar la vida íntima en sus domicilios u otros lugares privados.
- Informe del detective:
 - Información relacionada con el objeto y finalidad de la investigación.
 - Conservación 3 años las imágenes y sonidos grabados.
 - Las investigaciones privadas tendrán carácter reservado.
 - Su actividad deberá adecuarse al RGPD y LOPDGDD.



Tratamiento de datos por la RLT

El cumplimiento de las obligaciones y el ejercicio de los derechos de los representantes de las personas trabajadoras permiten el tratamiento de datos personales de las personas trabajadoras sin el consentimiento de éstas. No obstante, este tratamiento cuenta con una serie de límites:

- Sólo podrán ser objeto de tratamiento los datos necesarios para el ejercicio de esas funciones de representación.
- No es admisible el tratamiento de datos privados de la persona trabajadora, como el número de teléfono o domicilio personal.
- Sí se puede dar la identificación de las personas trabajadoras que ocupan cada puesto de trabajo con nombre y apellidos (STS 572/2018 de 7 de febrero, Sala de lo Social) y la dirección de correo electrónico corporativo.
- La copia básica del contrato contendrá todos los datos del contrato a excepción del número del DNI, el domicilio, el estado civil y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 mayo (RCL 1982, 1997), pudiera afectar a la intimidad personal.
- Respecto del absentismo, la empresa deberá informar sobre las causas y consecuencias de las bajas por incapacidad temporal (IT), pero no de las patologías médicas concretas de las personas trabajadoras que, por otra parte, tampoco debería conocer la empresa.
- Los datos no podrán ser utilizados con finalidades distintas a las del ejercicio de las tareas representativas.
- Siempre que los representantes de las personas trabajadoras hagan uso de los medios proporcionados por la empresa para el ejercicio de sus funciones, se les considerarán aplicables las políticas de seguridad de la entidad, tanto para el trabajo en los locales de la entidad, como en situación de movilidad o teletrabajo. Al tratarse de funciones distintas de las que llevan a cabo como usuarios en la empresa, tendrían que recibir perfiles específicos para acceder a los sistemas de información para el ejercicio de su acción representativa y recibir la formación adecuada para su manejo.
- Como responsables del tratamiento en el desarrollo de su acción representativa, deberán cumplir las medidas de seguridad aplicables y, en particular, en el caso de que se produzca una brecha de seguridad que afecte a los tratamientos de datos de carácter personal realizados en el desempeño de sus funciones, tendrán que cumplir con los requisitos relativos a la notificación de quiebras de seguridad a la autoridad de control y, dependiendo de su alcance, a los afectados. En cualquier caso, deberán comunicarlo de forma inmediata a la empresa en la que desempeñen sus funciones.
- Los convenios colectivos, en los términos previstos en el art. 64.9 del ET, podrían ser base jurídica para la lícita cesión de datos personales a los representantes de las personas trabajadoras. - art. 88.1 del RGPD –
- El tratamiento de datos requiere cumplir la obligación de informar a las personas trabajadoras.
- Los representantes deben respetar la confidencialidad de esos datos.



Publicación de datos en tableros de anuncios

Las notas publicadas en tableros de anuncios (o en portales electrónicos/intranet, etc) que contienen datos personales: su publicación constituye tratamiento de datos que puede comportar el acceso de terceros.

Aspectos a tener en cuenta:

- La persona responsable es quien sube materialmente la información al tablón.
- Solo los usuarios legitimados deben tener acceso al tablón.
- Los tableros siempre en la intranet(interno) no en internet(externo).
- Muy presente el principio de minimización.
- Limitación de acceso a terceros no autorizados.



Comunicaciones de datos por mail

- Una dirección de correo es un dato personal.
- Se dará acceso al correo corporativo y los envíos se han de realizar de forma proporcional sin que afecte a la actividad.
- Aspectos a tener en cuenta:
 - Uso de procedimientos automatizados (listas de distribución sin acceso a mails personales).
 - La comunicación de datos se limitara a los estrictamente necesarios (minimización).
 - El dato se utilizará para la finalidad para que fue comunicado.
 - La RLT obligada a cumplir con la RGPD y LOPDGDD.
 - La RLT deberá respetar el derecho de oposición (salvo en el supuesto de elecciones sindicales, momento en el cual prevalece la libertad sindical respecto del derecho a la protección de datos).

Periodos de consultas legalmente previsto

- Se tiene una base jurídica Convenio, ET.
- El periodo de consultas es una negociación y la norma exige que la empleadora proporcione a la RLT la información pertinente para conocer y valorar la situación.
- Esta información puede contener datos personales por lo que regirá el principio de minimización.
- Ambas partes garantizaran la confidencialidad.
- Las personas trabajadoras tienen derecho a los datos que han llevado a la decisión empresarial.

Vigilancia de la salud

Reconocimiento médico vinculado a la aptitud laboral de la persona trabajadora del que se derivan datos necesarios para la ejecución del contrato de trabajo.

- Existe un problema en la legitimación de la empresa y los delegados de prevención en el acceso de datos de salud.
- El acceso es muy limitado, solo apto o no apto.
- Pueden darse excepciones donde se requiera conocer más datos (adaptación de equipos y puestos) en estos casos principio de minimización (datos estrictamente necesarios).
- El consentimiento no es base jurídica no se tiene completa libertad para consentir.
- El convenio tampoco es base jurídica.
- Los delegados de prevención pueden acceder a la información necesaria para el ejercicio de sus funciones.
- Finalidad de control y datos estrictamente necesarios.
- Los delegados de prevención deberán respetar el sigilo profesional (art. 65.2 ET y 37.7 LPRL). Confidencialidad de la información.
- El derecho de información de los Delegados de Prevención tiene la misma extensión que la potestad informativa de la autoridad laboral.
- La investigación del accidente es parte de la evaluación y el resultado debe ser conocido por los Delegados de Prevención.
- Art.39.2 b) LPRL permite conocer al Comité de Seguridad y Salud cuantos documentos e informes relativos a las condiciones de trabajo sean necesarios para el cumplimiento de sus funciones.
- El RGPD permite el tratamiento de datos de la persona interesada sin consentimiento en situaciones de interés público en el ámbito de salud pública y en el cumplimiento de obligaciones legales (por ejemplo, pandemia Covid19).



Relación entre la empresa y el servicio de prevención

La relación entre la empresa y el servicio de prevención requerirá un tratamiento de datos, en concreto comunicaciones de datos relativos a las personas trabajadoras, que no exigen el consentimiento de éstas porque la base jurídica es una obligación legal, la prevención de riesgos laborales.

La condición de responsable del tratamiento varía según se trate de un servicio de prevención propio, ajeno o mancomunado:

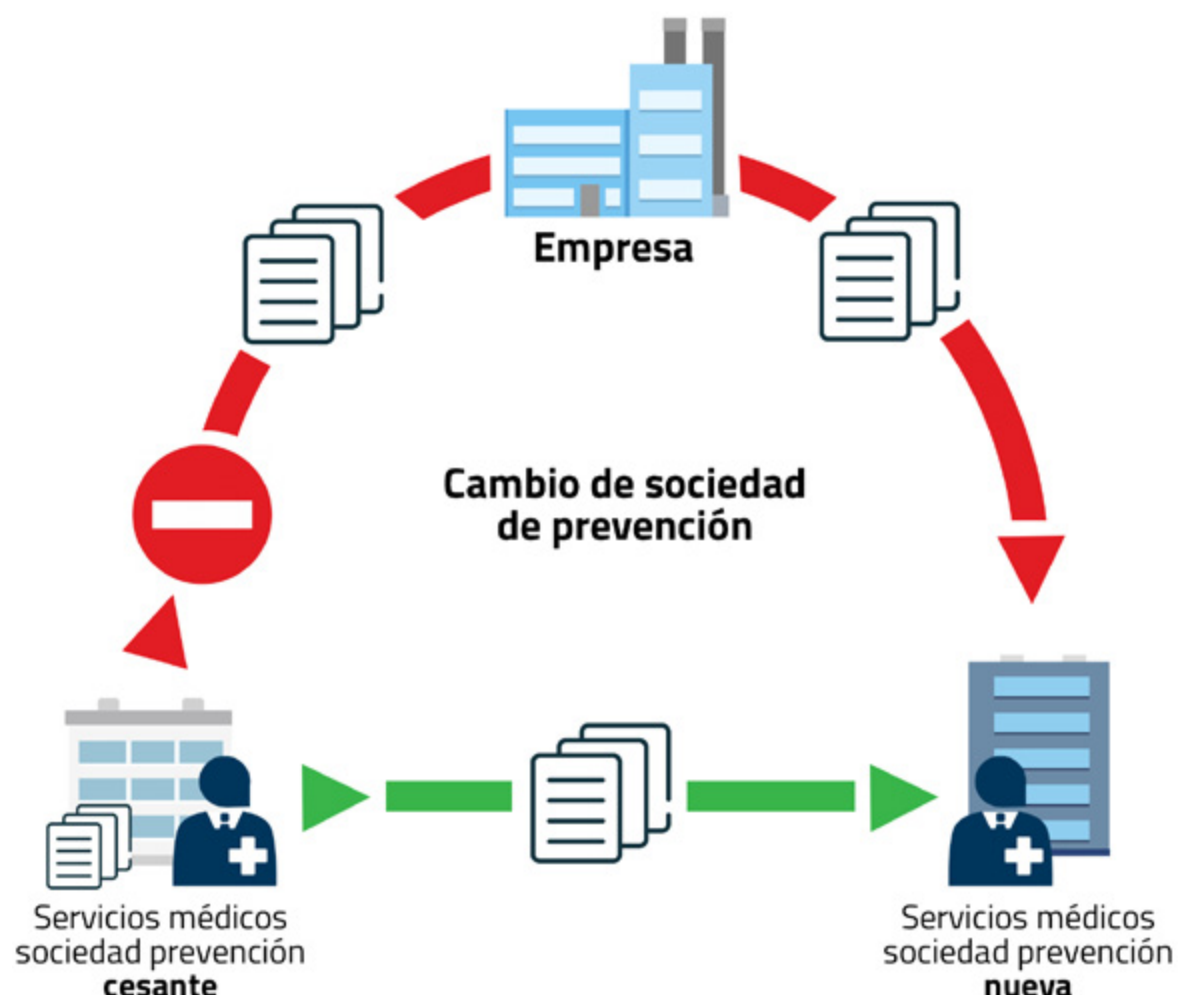
- Si se trata de un servicio propio, la empresa será responsable del tratamiento. En caso de servicio de prevención propio existirán en el seno de la empresa distintos perfiles y facultades de acceso a datos de salud.
- En el caso de servicio de prevención ajeno, éste será el responsable del tratamiento. En estos supuestos existe una total separación entre la empresa y el servicio de prevención. El servicio de prevención ajeno deberá limitarse a comunicar al empleador la condición de apto o no apto de la persona trabajadora o, en su caso, la necesidad de acometer adaptaciones o mejoras para reducir o eludir los riesgos. Cualquier otra comunicación de datos al empleador exige un interés legítimo del empleador.
- Los servicios de prevención mancomunados tendrán la consideración de servicios propios de las empresas que los constituyan si no tuviera personalidad jurídica independiente. Si el servicio mancomunado tiene personalidad jurídica propia, se considera como un servicio de prevención ajeno y, por tanto, responsable del tratamiento.

La confidencialidad debe garantizarse plenamente y, por ello, los sistemas de información para la gestión de servicios de prevención deberán implementar sistemas de registro o logs, a los efectos de verificar que los accesos se corresponden únicamente al personal habilitado y debidamente autorizado. Deberán definirse de modo muy preciso los perfiles de acceso y las funciones de cada uno de los usuarios.

Cambio en el servicio de prevención

Cuando se produce un cambio en el servicio de prevención, la comunicación de los datos relativos a la vigilancia de la salud de las personas trabajadoras a la nueva entidad, sería un supuesto de comunicación de datos previsto en el artículo 23.1 de la LPRL, en relación con el art. 30.3, derivada de la obligación de puesta a disposición del nuevo servicio y de la obligación de mantenimiento de la historia clínico-laboral (art. 37.3.c) del Real Decreto 39/1997 (Reglamento de los Servicios de Prevención).

- La comunicación debe producirse directamente entre los servicios médicos de las empresas de prevención involucradas. Nunca procede que el servicio de prevención que cesa entregue los datos al empleador para que éste se los haga llegar al nuevo servicio de prevención.
- La persona trabajadora tiene derecho a ser informada.
- El servicio de prevención que cesa no debe proceder a la supresión de los datos inmediatamente, pues tiene obligación de conservación, en los términos previstos en la normativa laboral que resulte de aplicación.





mutualia
