Protección de datos y Prevención de Riesgos Laborales

CCOO comisiones obreras de Aragón

GOBIERNO DE ARAGON

Indice

La protección de datos de carácter personal

Los derechos fundamentales son aquellos inherentes al ser humano, que pertenecen a toda persona en razón a su dignidad.

Dentro de estos derechos fundamentales adquiere especial relevancia, además de las libertades públicas, el derecho individual de las personas físicas, y especialmente de su honor, intimidad, privacidad personal y familiar, por lo que todo lo concerniente a sus datos personales deben ser garantizados y protegidos.

Por datos de carácter personal se entiende cualquier información referida a personas físicas (no jurídicas) identificadas o identificables (el interesado).

Se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente.

Se consideran datos de carácter personal, entre otros, el nombre y apellidos, dirección, teléfono, DNI, número de la Seguridad Social, fotografías, firmas, correos electrónicos, datos bancarios, edad y fecha de nacimien to, sexo, nacionalidad y datos de localización.

Datos considerados como categorías especiales o especialmente protegidos son aquellos que revelen origen étnico o racial, opiniones políticas o religión, datos relativos a la vida sexual o a la orientación sexual, condenas o infracciones penales, la identidad física, los relativos a la ideología, afiliación sindical, religión, creencias, situación económica, relaciones sociales de dicha persona, etc. y en especial los datos genéticos y los relativos a la salud física o mental.

Normativa relativa a la protección de datos

Para proteger los derechos fundamentales se han promulgado una serie de leyes y normas encaminadas a regular y conseguir que la utilización de datos personales se realice con las garantías suficientes que

impidan el abuso de los derechos individuales. La Constitución Española de 1978 fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Actualmente, las normas que rigen la protección de datos son:

1. El Reglamento General de Protección de Datos (RGPD). Es el texto de referencia europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Al ser una normativa europea es de obligado cumplimiento de todos los estados miembros, por lo que cualquier organización, organismo, instituciones, empresa de la Unión Europea que manejen información personal de cualquier tipo, deberán acogerse a ella. Este Reglamento incluye a aquellas empresas no europeas, cuando trabajen con información personal de residentes europeos.
2. La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales de 6 de diciembre tiene por objeto:
    a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.
    b) Garantizar el derecho fundamental de las personas físicas a la protección de datos personales; amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.
    c) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

La protección de datos en el ámbito laboral

Esta normativa es de especial relevancia en lo que respecta al tratamiento de los datos personales en las empresas, tanto de trabajadores, como de usuarios, clientes, proveedores, etc. Se refiere, por tanto, a la protección a todos los empleados propios de la empresa, a terceras empresas y a cualquier persona indifvidual que puedan ser susceptibles de ver lesionados sus derechos y libertades como consecuencia del uso de sus datos.

Por otra parte, obliga a todas aquellas personas físicas o jurídicas que manejen datos de clientes, usuarios o visitantes, empleados, proveedores, etc. ya sea en soporte informático o en papel, a cumplir una serie de principios generales, entre los que se encuentran:

- Calidad de los datos. Se deben recopilar y tratar los mínimos datos necesarios para el tratamiento. Sólo se podrán recoger cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Se deben evitar los datos considerados especialmente protegidos, como los relativos a la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual, etc. Además, no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.
- Limitación de la finalidad del tratamiento. Es decir, que los tratamientos se realicen para unas finalidades concretas.
- Limitación del plazo de conservación de los datos personales. Es decir, bloquear y/o destruir los datos en plazo de tiempo determinado.
- Transparencia en cuanto a la información proporcionada a los interesados sobre el tratamiento de sus datos personales.
- Responsabilidad proactiva en el uso de medidas de seguridad y políticas ante brechas de seguridad en los sistemas utilizados por las empresas en el tratamiento de los datos personales.

- Exactitud y veracidad de los datos personales que se manejan.
- Deber de confidencialidad. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de éste, estarán sujetas al deber de confidencialidad y obligados a guardar el secreto profesional, incluso una vez finalizada la relación con la empresa o con el responsable o encargado del tratamiento.
- Comunicación o cesión de datos. Los datos de carácter personal sólo podrán ser comunicados o cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas de quien los cede y a quien se les cede, siendo imprescindible que los trabajadores sean informados de esta cesión y el destino de la misma. La posibilidad de que se contrate a una empresa externa para que preste un servicio (gestoría, asesoría, empresas de prevención de riesgos laborales, subcontratas, etc.) es muy habitual y si bien es cierto que no se requiere el consentimiento concreto para dicha cesión, esta debe hacerse en base a un contrato de encargado de tratamiento.
- El interés legítimo. Se presume, salvo prueba en contrario, la prevalencia del interés legítimo del responsable para el tratamiento de los datos profesionales de las personas físicas que presten servicios en una empresa, así como el respecto de los datos de los empresarios individuales y de los profesionales liberales.
- Consentimiento del afectado. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado. El consentimiento deberá ser una manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el uso de sus datos personales. Para ello se deberá de especificar de manera clara la finalidad para la que se autoriza el uso de los datos, no pudiendo hacerse uso de dichos datos para otros fines que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

El consentimiento exigido no será preciso cuando la cesión está autorizada en una ley o cuando se trate de datos recogidos de fuentes accesibles al público.

Agentes que intervienen en el tratamiento de datos

En el Reglamento se refuerzan las figuras internas que protegen los datos, obligando a las empresas afectadas por la normativa en materia de protección de datos de carácter personal, a determinar cuáles son los responsables y encargados de establecer las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo.

- Responsables de Tratamiento (RT). Aquella persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, decide sobre los fines y medios del tratamiento de datos. Esta capacidad de decisión incluye la creación, contenido, finalidad y uso del tratamiento. En otras palabras, decide por qué llevar a cabo el tratamiento y el cómo hacerlo.
- Encargados de Tratamiento (ET). Los encargados de tratamiento serán las personas físicas o jurídicas que hacen un tratamiento por cuenta de un responsable.
- El delegado de protección de datos (DPD). Es el encargado de velar por que se cumpla el RGPD. Establece el derecho de acceso y derecho a la portabilidad de los datos, así como los derechos al olvido, de corrección y de oposición, la protección de datos desde el diseño y la protección de datos por defecto. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

Los responsables y encargados determinarán las medidas técnicas y organizativas apropiadas que se deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con lo recogido en la normativa. En

particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere el Capítulo IV del citado Reglamento.

Derechos de los afectados

Las personas físicas o jurídicas que manejen datos están obligadas a cumplir con una serie de principios que garanticen el derecho de los afectados:

- Transparencia e información al afectado. Cuando los datos personales del afectado sean obtenidos por el responsable del tratamiento deberá de dar cumplimiento del deber de información a la persona afectada de forma sencilla e inmediata. Dicha información deberá contener como mínimo: la identidad del responsable del tratamiento o de su representante, la finalidad del tratamiento y las categorías de datos objeto de tratamiento.
- Derecho de acceso a los propios datos personales.
- La persona afectada tiene derecho también a ser informada de los fines del tratamiento de sus datos, del plazo de conservación, de los derechos que se pueden ejercer, de las garantías existentes en caso de transferencia internacional y de la existencia de decisiones automatizadas (incluida la elaboración de perfiles) y también el derecho a obtener una copia de los datos.
- Derecho de rectificación si los datos son inexactos o incompletos.
- Derecho de supresión (derecho al olvido). Si los datos se tratan de forma ilegal o ya no son necesarios para la finalidad con que se recogieron, incluidos los datos en las búsquedas de internet, en servicios de redes sociales o servicios equivalentes.
- Derecho a la limitación del tratamiento, es decir, a solicitar que se suspenda el tratamiento si existen controversias sobre su exacti-

tud, o si se ha ejercitado el derecho de oposición al tratamiento. Mientras se verifica la legitimación, se deben conservar los datos, evitando su supresión, por ser necesarios para el interesado para la formulación, ejercicio o defensa de reclamaciones.

- ◊ Derecho a la portabilidad de los datos para poder cambiar o transmitirlos a otro responsable si es técnicamente posible en un formato estructurado y de uso común.
- ◊ Derecho de oposición al tratamiento cuando por la situación personal debe cesar el tratamiento o para oponerse a un uso posterior con fines de prospección comercial (marketing directo), investigación científica o histórica, o fines estadísticos (salvo que quien trate los datos acredite un interés legítimo).
- ◊ Derecho a no ser objeto de decisiones individuales automatizadas, decisiones sin intervención humana que produzcan efectos jurídicos al interesado, incluida la elaboración de perfiles que produzcan efectos jurídicos sobre él o tengan efectos negativos para la persona afectada.
- ◊ Derecho a que se anule el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos o el tipo de actividad de aquel a quien se pretenden comunicar.
- ◊

Organismos de control

Son organismos públicos que actúan de manera independiente y cuya responsabilidad es la proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento de sus datos y de facilitar la libre circulación de los mismos en la Unión Europea si así lo solicitara.

Dichos organismos son:

- Supervisor Europeo de Protección de Datos (SEPD). Es el encargado de supervisar y garantizar el tratamiento de datos personales por las instituciones y organismos comunitarios. Asesora a las instituciones y a organismos comunitarios y a los titulares de los datos en las cuestiones relacionadas con el tratamiento de los datos personales.
- Agencia Española de Protección de Datos (AEPD). Es la encargada de controlar a nivel estatal la aplicación del RGPD y del resto de la normativa de protección de datos.
- Agencias Autonómicas de Protección de Datos. Estas Agencias son las encargadas del control respecto de los ficheros de datos de carácter personal creados o gestionados por las CCAA y por la Administración Local de su ámbito territorial. No todas las CCAA disponen de estas Agencias. La Comunidad Autónoma de Aragón no dispone todavía de esta Agencia.

Sanciones

Además de las obligaciones, conviene hacer una llamada de atención sobre el régimen de responsabilidades y sanciones previsto por el texto europeo en caso de incumplir lo dispuesto en él. Las empresas son las responsables de las infracciones realizadas en el manejo de los datos recogidos y violar el derecho fundamental a la protección de datos puede traducirse en multas muy elevadas.

El sistema de sanciones que establece el RGPD permite un amplio margen de actuación por los Estados Miembros en este marco. La Ley Orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, de acuerdo con la diferenciación que el RGPD establece al fijar la cuantía de las sanciones.

Protección de Datos y Prevención de Riesgos Laborales

La Ley 31/1995 de Prevención de Riesgos Laborales obliga a la empresa a realizar una serie de actividades preventivas para garantizar unas condiciones de trabajo seguras y saludables. La gestión de la prevención de riesgos laborales en las empresas requiere, por tanto, la utilización de documentos diversos y el tratamiento de datos personales como la identificación, generación, almacenamiento, acceso, intercambio, etc., tanto del personal propio como del perteneciente a otras empresas subcontratas u otros organismos.

La normativa sobre protección de datos incide en todos los aspectos de la actividad laboral, pero muy especialmente en la Prevención de Riesgos Laborales.

A continuación, se hace un breve repaso sobre aquellos aspectos más relevantes a tener en cuenta en la prevención de riesgos laborales para dar cumplimiento a la normativa protección de datos de carácter personal.

Datos personales tratados en la gestión de la Prevención de Riesgos Laborales

Son muchos y muy variados los documentos que se manejan en la Prevención de Prevención de Riesgos que requieren la recogida, tratamiento y almacenamiento de datos de carácter personal (informes sobre investigación de accidentes, informe de Vigilancia de la Salud, personas asistentes a cursos de formación y sus certificaciones o títulos, informes de las evaluación específicas de riesgos, trabajadores designados en responsabilidades en el Plan de Emergencia o Autoprotección, nombramientos de delegados de prevención, actas de constitución y reunión del Comité de Seguridad y Salud, contrato de trabajo de los técnicos del Servicio de Prevención, registros de participación y consulta con los Delegados de Prevención, intercambio de datos sobre los trabajadores

en la coordinación de actividades empresariales, registros de entrega de EPI's o equipos de trabajo, certificados de aptitud, registros de información de trabajadores de proveedores y contratistas, actas de reuniones de coordinación de actividades empresariales, etc.).

Con la entrada en vigor del nuevo Reglamento General de Protección de Datos (RGPD) se produce una profunda modificación respecto a la protección y privacidad de los datos.

Por tanto, se exigirá a las organizaciones públicas y privadas un mayor compromiso de conocimiento en la gestión de los datos y su necesaria integración en los protocolos de cumplimiento recogidos en la normativa.

Tal y como se recoge en la normativa de Protección de Datos Personales y garantía de los derechos digitales, las personas físicas o jurídicas que manejen estos datos están obligados a cumplir con los principios de:

- Calidad, recopilando y manejando exclusivamente los datos imprescindibles, adecuados, pertinentes para el tratamiento o finalidad que se pretende.
- Limitar el plazo de conservación de los datos personales. Es decir, destruir los datos cuando estos ya no sean necesarios en el proceso de prevención.
- Informar de manera clara a los interesados sobre el tratamiento de sus datos personales.
- Utilizar datos exactos y veraces.
- Deber de confidencialidad de los responsables y encargados del tratamiento de los datos.
- Información al interesado cuando sus datos sean cedidos a terceros.
- Consentimiento en los casos requeridos.
- La toma de datos personales relativos a la vigilancia y control de la salud de los trabajadores solo se llevarán a cabo por personal sanitario con competencia técnica, formación y capacidad acreditada.

El artículo 9 del Reglamento General de Protección de Datos establece la prohibición del tratamiento de datos personales calificados como "especialmente sensibles" cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnica o los relativos a la salud física o mental, a no ser que estén amparados en una norma con rango de ley.

En esta categoría se incluyen: los informes de accidentes de trabajo y/o enfermedades profesionales, la evaluación de riesgos específica de personal especialmente sensible (minusvalía, embarazo, menores), certificados de porcentaje de discapacidad requeridos en las adaptaciones de puesto de trabajo, el listado de personal especialmente sensible, etc.

Agentes que intervienen en la gestión de los datos de prevención

La Ley Oorgánica de Protección de Datos (LOPD) define el tratamiento de datos como "Todas aquellas operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". Es decir, el tratamiento de datos es un proceso por el cual éstos sirven al fin para el cual fueron recopilados, teniendo en cuenta que este tratamiento comprende su uso, desde el momento de su recogida hasta el momento de su cancelación. Por otra parte, el Reglamento General de Protección de Datos (RGPD) recoge la obligación de nombrar la figura del delegado de protección de datos.

La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, impone a la empresa la realización de un conjunto de actividades cuyo fin último es evitar o disminuir los riesgos derivados del trabajo. Para la realización de dichas actividades, así como para la recopilación y gestión de los datos de prevención que entran en juego, el empresario está obligado a contratar un Servicio de Prevención que puede ser propio, ajeno o mancomunado, dependiendo del modelo organizativo elegido.

Tanto la LPRL como el RGPD regulan las obligaciones, responsabilidades y las acciones concretas de los agentes que intervienen en el tratamiento de datos personales.

Los agentes que gestionan de una u otra forma datos son:

Con carácter general, las autoridades públicas y algunas empresas deberán de contar con la figura del delegado de protección de datos (DP).

- **Delegado de protección.** Es la persona designada por el responsable de tratamiento de datos. Es el encargado de velar por que se cumpla el RGPD.

  Entre sus funciones se encuentran:

  1. Establecer, el derecho de acceso y derecho a la portabilidad de los datos, así como los derechos al olvido, de corrección y de oposición.
  2. La protección de datos desde el diseño y la protección de datos por defecto.
  3. Actuará también como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos y podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

En lo que se refiere a la gestión de la Prevención de Riesgos Laborales (PRL), se consideran Responsables de Tratamiento los siguientes agentes:

- **El empresario.** Se considera el Responsable de Tratamiento de datos (RT). El empresario es quien tiene la capacidad para aplicar las medidas técnicas y organizativas adecuadas de protección de datos, así como las políticas de prevención de riesgos a poner en marcha en la empresa. Es, por tanto, quien tiene las mayores obligaciones respecto de los tratamientos de datos sobre los que decide. Al Responsable de Tratamiento le corresponden los siguientes deberes:

    1. Llevar a cabo un análisis de riesgos de los tratamientos específicos que lleva a cabo para determinar las medidas adecuadas.
    2. Iniciar la protección de datos desde el diseño y por defecto.
    3. Tomar las medidas oportunas para atender los derechos del interesado.
    4. Elaborar y mantener actualizado el Registro de Actividades de Tratamiento (RAT).
    5. Notificar las violaciones de seguridad de los datos a la autoridad de control y, en su caso, comunicación al interesado.
    6. De la cesión de datos a terceros.
    7. Designar un Delegado de Protección de Datos, en su caso.

- **Los Servicios de Prevención.** Se consideran también agentes Responsables del tratamiento de datos. Entre otras funciones tienen:

    1. El diseño, aplicación y coordinación de la Planificación de la Actividad Preventiva, y Plan de Prevención.
    2. La evaluación de riesgos laborales en relación a la Ergonomía, Seguridad, Higiene Industrial, Ergonomía y Psicosociología, en coordinación con la Unidad de Vigilancia de la Salud.
    3. Determina las prioridades en la adopción de medidas preventivas, en función del tipo de riesgo identificado.

4. Vigila la eficacia de las medidas preventivas implantadas.
5. Forma e informa a los trabajadores, a través de diferentes medios, web del Servicio de Prevención, información escrita, presencial, e-mail, etc.
6. Elabora, actualiza e implanta los planes de emergencia mediante diferentes actuaciones, como los simulacros de alarma y evacuación.
7. Elabora y custodia la documentación de carácter médico y deberá tener a disposición de la autoridad sanitaria la documentación relativa a la práctica de los controles de la vigilancia de la salud
8. Realiza las propuestas de adaptación de puesto de trabajo.

◊ **Las Mutuas de accidentes de trabajo y enfermedades laborales.** Se consideran, junto con los Servicios de Prevención, los responsables del tratamiento de datos. Las Mutuas colaboradoras con la Seguridad Social son responsables de la elaboración de informes médicos de los trabajadores con fines propios y del tratamiento y custodia de los datos de dichos informes.

◊ **Comité de Seguridad y Salud y delegados de prevención.** Se consideran también agentes de gestión de datos. Para el desempeño de estas competencias, la LPRL en su artículo 39.2 confiere a los Comités de Seguridad y Salud (CSS) la facultad para acceder a la información y registros que pueden contener datos personales como:

1. En la realización de visitas, conocer directamente la situación relativa a la prevención de riesgos en el centro de trabajo.
2. Cuantos documentos e informes relativos a las condiciones de trabajo sean necesarios para el cumplimiento de sus funciones, así como los procedentes de la actividad del servicio de prevención, en su caso.
3. Los informes de los daños producidos en la salud o en la integri-

dad física de los trabajadores, al objeto de valorar sus causas y proponer las medidas preventivas oportunas.

4. La relación de accidentes de trabajo y daños sufridos por los trabajadores, como son los informes de siniestralidad y otros indicadores de accidentabilidad. En cuanto a los datos individuales de accidente o enfermedad profesional concretos se garantizará el uso de códigos, seudónimos u otro sistema con objeto evitar que por los datos se pueda identificar a la persona.

◊ **Auditoría.** Es un instrumento de gestión que persigue reflejar la imagen fiel del sistema de prevención de riesgos laborales de la empresa, valorando su eficacia y detectando las deficiencias que puedan dar lugar a incumplimientos de la normativa vigente para permitir la adopción de decisiones dirigidas a su perfeccionamiento y mejora.

La auditoría llevará a cabo un análisis sistemático, documentado y objetivo del sistema de prevención.

Los resultados de la auditoría deberán quedar reflejados en un informe que la empresa auditada deberá mantener a disposición de la autoridad laboral competente y de los representantes de los trabajadores.

Registro de las actividades de tratamiento

El Responsable de Tratamiento de datos (RT) o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento a que se refiere el artículo 30 del Reglamento General de Protección de Datos.

El registro deberá estar organizado en torno a conjuntos estructurados de datos; deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cesión de datos a empresas de prevención de riesgos laborales

En el caso de producirse un traslado de la documentación relativa a la Vigilancia de la Salud entre los servicios sanitarios y los servicios de prevención se informará a los interesados. Puede darse en el caso de cambio de Servicios de Prevención Ajenos por finalización de relación contractual o cuando un Servicio de Prevención subcontrata algún servicio específico.

Dicha transferencia de datos sanitarios está legitimada, por ser necesaria para el cumplimiento de la obligación de la Vigilancia de la Salud dentro de la relación laboral, pero no elimina el deber de información de tal transferencia a los interesados.

Desde el punto de vista de tratamiento de datos personales, la protección de los intereses vitales de las personas físicas corresponde en el ámbito de la salud a las distintas autoridades sanitarias de las diferentes administraciones públicas, las cuales podrán adoptar las medidas necesarias para salvaguardar a las personas en situaciones de emergencia sanitaria.

Por otra parte, el empresario deberá garantizar que la autoridad sanitaria disponga de la documentación relativa a la práctica de los controles de la vigilancia de la salud del artículo 22 de la LPRL.

El deber de custodia exige que se adopten medidas propias de la seguridad de la información como son la identificación, clasificación y codificación de los activos, gestión y control de accesos de los usuarios, política de contraseñas, políticas de copias de seguridad o el cifrado de archivos, entre otras, de manera que se garanticen las tres dimensiones de la seguridad de la información: la disponibilidad, la integridad y la confidencialidad.

No será necesario recabar el consentimiento de los trabajadores para comunicar sus datos a las Mutuas o las Sociedades de Prevención por la excepción de la obligación legal.

Los datos personales también podrán estar a disposición de Organismos Públicos de control, como por ejemplo la Inspección de Trabajo o Tribunal de Justicia.

El principio de responsabilidad proactiva

El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

La protección de datos en situaciones de pandemia (COVID-19)

El Reglamento General de Protección de Datos del Parlamento Europeo, (RGPD), dispone de herramientas suficientes que legitiman el tratamiento de datos personales y reconoce que, en situaciones excepcionales como una epidemia, la base jurídica de los tratamientos puede ser múltiple, basada tanto en el interés público como en el interés vital del interesado u otra persona física.

Por tanto, la protección de datos personales en situaciones como la presente, en que existe una emergencia sanitaria de alcance general, no debería utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades, especialmente las sanitarias, en la lucha contra la pandemia.

En situaciones excepcionales como la actual pandemia, en cuanto al derecho a la protección de datos personales, se deben compatibilizar y ponderar en primer lugar los intereses y derechos del bien común y el control de la pandemia.

La Agencia Española de Protección de Datos, en relación con los tratamientos de datos resultantes de la actual situación derivada de la extensión del virus COVID-19, aclara que la normativa de protección de datos personales es un derecho fundamental, por lo que se está aplicando en su integridad, eso sí, se está poniendo en práctica lo que recoge el RGPD en lo referente a situaciones de fuerza mayor, como es el caso de una pandemia.

Por tanto, la base jurídica en la que se basa la utilización de datos en caso de pandemia es:

- Misión realizada en interés público.
- Intereses vitales del interesado u otras personas físicas.

Se considera de interés público cuando el uso de los datos es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

Se entiende de interés vital cuando la utilización de datos personales van dirigidos a proteger a todas aquellas personas susceptibles de ser contagiadas en la propagación de una epidemia, lo que justificaría, desde el punto de vista del uso de datos personales, en la manera más amplia posible, por cuanto los intereses vitales de dichas personas físicas habrán de ser salvaguardados y ello es reconocido por la normativa de protección de datos personales.

La protección de datos puede y debe quedar supeditada al interés público y el interés vital de evitar una propagación incontrolada del virus, intentando, en la medida de lo posible, respetar la privacidad

de los interesados de acuerdo con las exigencias legales.

La ley General de Salud Pública contempla la posibilidad de adoptar medidas adicionales en caso de riesgo de transmisión de enfermedades.

Por lo tanto, en materia de riesgo de transmisión de enfermedades, epidemia, crisis sanitarias, etc., la normativa aplicable ha otorgado "a las autoridades sanitarias de las distintas Administraciones públicas" las competencias para adoptar las medidas necesarias previstas en dichas leyes cuando así lo exijan razones sanitarias de urgencia o necesidad.

Corresponde por ello a la autoridad sanitaria la adopción de las medidas oportunas encaminadas a la prevención y gestión de la enfermedad, así como los criterios y el uso de los datos personales.

Ante la situación social y sanitaria de pandemia en relación con el COVID-19, la Agencia Española de Protección de Datos (AEPD) publicó el 12 de marzo de 2020 un informe en el que analiza la situación actual con el objetivo principal de que la protección de datos no resulte un impedimento en la lucha contra la pandemia.

La protección de datos en el ámbito de las empresas en lo referente al COVID-19

En el Ámbito Laboral, según la Ley de Prevención de Riesgos Laborales, la empresa tiene la obligación de promover una cultura de prevención de riesgos laborales. En esta situación de emergencia el empleador debe anteponer su rol de vigilancia y control de salud de todos sus trabajadores; esto quiere decir que está facultado para verificar sí el estado de salud de sus trabajadores puede constituir un peligro para ellos mismos o para el resto del personal. Asimismo, tiene la obligación de mantener el lugar de trabajo libre de riesgos sanitarios, por lo que estaría justificada la solicitud de información a los empleados y visitantes externos sobre síntomas o factores de riesgo sin necesidad de pedir su consentimiento explícito.

Por tanto, los empresarios podrán tratar, de acuerdo con dicha norma-

tiva y con las garantías que establecen, los datos de sus empleados necesarios para garantizar la salud de todos sus empleados, lo que incluye igualmente al resto de empleados distintos del interesado, para asegurar su derecho a la protección de la salud y evitar contagios en el seno de la empresa y/o centros de trabajo.

En base a las medidas adoptadas por Autoridad de Control española, en relación con el Derecho Laboral y la Ley de Prevención de Riesgos Laborales y medicina laboral, se establecen una serie de normas referentes a los datos a los que la empresa puede tener acceso, su finalidad y los requisitos para el tratamiento de dichos datos.

El Tratamiento de Datos Personales Sensibles debe:

- Responder al principio de proporcionalidad, ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.
- Limitarse exclusivamente a preguntar por visitas a países de alta prevalencia del virus y en el marco temporal de incubación de la enfermedad las últimas 2 semanas, o si se tiene alguno de los síntomas de la enfermedad.
- Los datos personales que vayan a ser tratados deben ser veraces, exactos y adecuados respecto de la finalidad para la que fueron recopilados. Los resultados deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.
- El empleador, como titular o responsable del tratamiento, está obligado a guardar confidencialidad respecto de la información compartida por sus trabajadores (artículo 17 de la Ley de Protección de Datos Personales).
- La recogida de datos estará siempre limitada a la finalidad que se persigue (en este caso, salvaguardar los intereses vitales/esenciales de las personas físicas).
- Deben brindar a los usuarios medidas de seguridad y un estricto respeto del principio de proporcionalidad del tratamiento de los

datos. Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

- Que la conservación de los datos tenga un fin y caducidad. Debe finalizar una vez se haya superado la pandemia.
- El interesado debe estar informado sobre cualquier extremo relacionado con sus datos personales (identificación del responsable, qué datos se van a tratar, para qué finalidades...).

Respecto a los reconocimientos médicos, aun en estado de pandemia, continúa vigente:

- Los reconocimientos médicos serán obligatorios cuando sea imprescindible para verificar si el estado de salud del trabajador puede constituir un peligro para sí mismo, para otros trabajadores, o para otras personas relacionadas con la empresa, como es actualmente la situación de pandemia.
- Se garantizará el derecho a la intimidad y a la dignidad del trabajador. La información médica será confidencial, sólo se tratará por el personal médico y las autoridades sanitarias; el trabajador deberá de ser informado de los resultados y estos resultados no podrán ser utilizados con fines discriminatorios.
- Al empresario únicamente se le facilitará un informe sobre la aptitud del trabajador para el desarrollo de las tareas de su puesto y, en su caso, sobre la necesidad de adopción de medidas adaptativas de protección y prevención en el puesto de trabajo. El empresario deberá conservar dicha información y la documentación acreditativa de la práctica de los controles de salud.
- Se establecerán protocolos médicos y se seguirá un criterio de proporcionalidad en base a los factores de riesgo inherentes al puesto, a fin de optar por las pruebas médicas que causen menos molestias a los trabajadores.
- La confidencialidad de datos, como decíamos anteriormente, es un derecho fundamental recogido en nuestra Constitución que

sigue siendo plenamente aplicable.

De todo lo anterior deducimos que ahora más que nunca, los principios contenidos en el artículo 5 del Reglamento General de Protección de Datos son imprescindibles para su tratamiento, especialmente el de "limitación de la finalidad" y el de "minimización de datos", y no deberá confundirse la conveniencia con la necesidad.

La Agencia Española de Protección de Datos, con motivo de la pandemia de la COVID-19 ha elaborado una guía sobre las preguntas más frecuentes que se plantean ante esta situación.

¿Tiene el empresario derecho a conocer si algún trabajador puede estar infectado?

Si, siempre de acuerdo con la normativa sanitaria, laboral y de prevención de riesgos laborales, y con las garantías que estas establecen, los empresarios pueden tratar los datos del personal necesarios para garantizar su salud y adoptar los planes de contingencia propios o medidas impuestas por las autoridades competentes. Esta información puede ser obtenida mediante preguntas al personal, limitándose exclusivamente a:

1. Saber si la persona trabajadora ha sido diagnosticada como contagiada.
2. Saber si la persona trabajadora está sujeta a cuarentena.
3. Quedan prohibidos los cuestionarios de salud que sean extensos y detallados o con preguntas que no guarden relación con la finalidad mencionada.
4. Las preguntas deberán limitarse a las visitas a países de riesgo no más allá de las últimas dos semanas (correspondiente al período aproximado de incubación de la COVID-19), sin permitirse cuestionarios de salud, extensos y detallados o con preguntas no guar-

den relación con la finalidad mencionada. De nuevo es necesario el respeto a los principios de finalidad y proporcionalidad.

¿Pueden los empresarios tratar la información de si las personas trabajadoras están infectadas de coronavirus?

Sí, en aplicación de lo establecido en la normativa sanitaria, laboral y, en particular, de prevención de riesgos laborales, los empleadores podrán tratar, de acuerdo con dicha normativa y con las garantías que establecen, los datos del personal necesarios para garantizar su salud y adoptar las medidas necesarias por las autoridades competentes, lo que incluye igualmente asegurar el derecho a la protección de la salud del resto del personal y evitar los contagios en el seno de la empresa y/o centros de trabajo que puedan propagar la enfermedad al conjunto de la población.

La empresa podrá conocer si la persona trabajadora está infectada o no para diseñar, a través de su servicio de prevención, los planes de contingencia que sean necesarios o que hayan sido previstos por las autoridades sanitarias.

¿Se puede transmitir información de un compañero afectado al resto del personal?

Sí, aunque se permite trasladar dicha información, esta no deberá identificar a la persona afectada a fin de mantener su privacidad. Sin embargo, si la finalidad de proteger la salud de los trabajadores no puede conseguirse sin identificar al afectado o su divulgación es requerida a la empresa por parte de las autoridades competentes, podría proporcionarse tal información identificativa respetando los principios de finalidad y proporcionalidad.

¿Se pueden tratar datos de salud de trabajadores relacionados con el coronavirus?

Sí, siempre que su finalidad sea la de cumplir con las decisiones que adopten las autoridades competentes sobre la pandemia de coronavirus. Siempre bajo los principios del RGPD.

¿Pueden transmitir esa información al personal de la empresa?

Esta información debería proporcionarse sin identificar a la persona afectada a fin de mantener su privacidad, si bien podría transmitirse a requerimiento de las autoridades competentes, en particular las sanitarias.

¿Es necesario requerir el consentimiento del trabajador contagiado, para el tratamiento de sus datos?

No, no resulta necesario que el trabajador otorgue su consentimiento expreso. Las bases que legitiman dicho tratamiento se derivan de la necesaria protección de los intereses vitales del resto de empleados, e incluso del interés público.

¿Puede una entidad comunicar a sus trabajadores que existe un empleado que ha dado positivo o con sintomatología relacionada con esta enfermedad?

La respuesta es sí, pero con limitaciones. Dicha comunicación ha de hacerse, si fuese posible, sin especificar la identidad de la persona contagiada. Si no resulta objetivamente posible o las autoridades sanitarias lo indicasen expresamente, se podría proporcionar la identificación del contagiado.

¿El trabajador está obligado a comunicar al empleador cualquier cuarentena preventiva o la afectación por el coronavirus?

Los trabajadores que, tras haber tenido contacto con un caso de coronavirus, pudieran estar afectados por dicha enfermedad y que, por aplicación de los protocolos establecidos por las Autoridades Sanitarias competentes, se ven sometidos al correspondiente aislamiento preventivo para evitar los riesgos de contagio derivados de dicha situación hasta tanto se disponga del correspondiente diagnóstico, deberán informar a su empleador y al servicio de prevención o, en su caso, a los delegados de prevención (Ley de Prevención de Riesgos Laborales). La persona trabajadora en situación de baja por enfermedad no tiene obligación de informar sobre la razón de la baja a la empresa. Sin embargo, este derecho individual puede ceder frente a la defensa de otros derechos como el derecho a la protección de la salud del colectivo de trabajadores en situaciones de pandemia, art. 29.2. 4º de la LPRL.

¿Tiene el trabajador la obligación de informar a la empresa del motivo de su baja laboral?

Si bien es cierto que por regla general no es obligatorio que el trabajador informe sobre la razón de su baja, dadas las especiales circunstancias el trabajador podría estar obligado a comunicar tal circunstancia en favor de la protección de la salud de sus compañeros, así como de toda la población si las causas de su baja son por contagio del COVID-19 o sospechas de ello.

¿Puede el empresario tomar la temperatura a trabajadores?

Si, se podrán llevar a cabo tomas de temperatura de trabajadores, recomendablemente por parte del personal sanitario, siempre con el fin de contener la propagación del coronavirus, limitándose a tal finalidad y sin extenderse a otras distintas, no manteniéndose los datos por más tiempo del necesario.

¿El personal de seguridad puede tomar la temperatura a los trabajadores con el fin de detectar casos coronavirus?

No, verificar si el estado de salud de las personas trabajadoras cuando puede constituir un peligro para ellas mismas, para el resto del personal, relacionadas con la empresa constituye una medida relacionada con la Vigilancia de la Salud de los trabajadores que, conforme a la Ley de Prevención de Riesgos Laborales, resulta obligatoria para el empleador y debería ser realizada por personal sanitario.

¿Puede el empresario proporcionar los datos personales de salud a otras entidades?

No, los datos personales de salud recogidos por razones de interés público, solo podrán proporcionarse a organismos relacionados con la salud, nunca se deben de facilitar a terceros, como empresarios, compañías de seguros o entidades bancarias, etc., que traten los datos personales con otros fines.

La confidencialidad de datos es un derecho fundamental recogido en nuestra Constitución que sigue siendo plenamente aplicable incluso en esta situación de emergencia sanitaria, y aplicándose íntegramente los principios contenidos en el art.5º RGPD.

En el supuesto de que el trabajador o la trabajadora considere que no se respetan dichos principios configurados como garantías a priori, o se vulnera su derecho a la protección de sus datos, deberá iniciar acciones tendentes a restablecer el derecho fundamental presuntamente lesionado.

Para ello, recomendamos:

- ◊ Consultar con el sindicato para ser asesorado/a.
- ◊ Recurrir a la Inspección de Trabajo.
- ◊ Recurrir a la vía judicial.