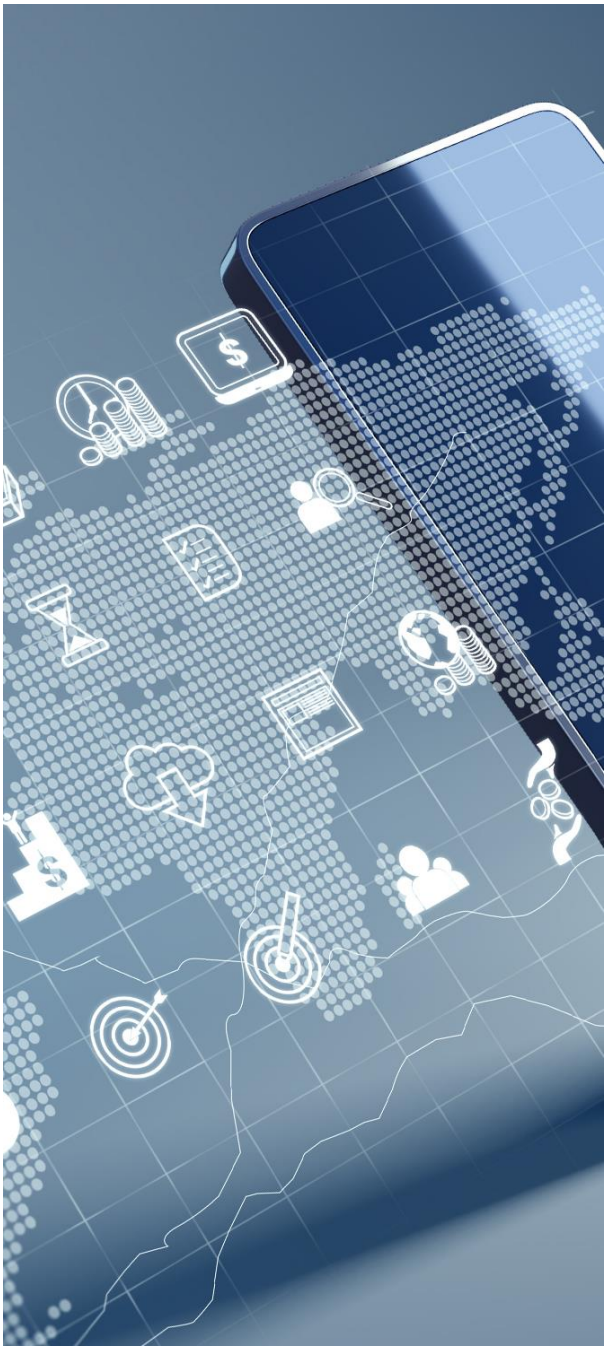
CUATRECASAS

Novedades en materia de protección de datos personales en las relaciones laborales

Legal Flash

8 de junio de 2021



La Agencia Española de Protección de Datos (AEPD) ha publicado una nueva guía sobre *Protección de datos y relaciones laborales* ("la Guía") con el objetivo de ofrecer una herramienta práctica que facilite el adecuado cumplimiento de la normativa de protección de datos por parte de las empresas.

Si bien la Guía carece de carácter vinculante, muestra el criterio que tanto la propia AEPD como posiblemente los Tribunales seguirán a la hora de resolver conflictos que se les presenten, por lo que su valor interpretativo resulta indiscutible para todas las empresas que tengan trabajadores en plantilla.

En este Legal Flash, tratamos de manera ejecutiva los 10 aspectos más relevantes y que más controversia han generado frente a la AEPD en la aplicación de la normativa de protección de datos en el ámbito de los recursos humanos y que la Guía trata de resolver.

1. Selección de personal y redes sociales

- La empresa solo puede tratar los datos personales de personas trabajadoras o candidatas obtenidas de las redes sociales, aunque el perfil en las redes sociales sea de acceso público, si tiene una base jurídica válida, el tratamiento está relacionado con fines profesionales y se demuestra su necesidad y pertinencia para el desempeño del puesto de trabajo[1].

- Por otro lado, la empresa no está legitimada para solicitar «amistad» a personas candidatas o empleadas con el objetivo de acceder a los contenidos de sus perfiles, ni tampoco para solicitar la información que estas compartan con otras personas a través de las redes sociales[2].

- Por lo que se refiere a las entrevistas de trabajo, las contestaciones de las personas candidatas no equivalen a un consentimiento para su tratamiento. Por tanto, los datos personales obtenidos por esa vía, directamente o mediante deducciones, no pueden ser objeto de tratamiento si no se dispone de una base jurídica legítima, so pena de infracción administrativa y posible vulneración de derechos fundamentales[3].

2. Colaboración entre empresas en la fase de contratación (ETT)

- Es muy habitual que, durante el proceso de selección y contratación, las empresas colaboren con otras empresas especialistas. Cuando ello sucede, el marco que regula el tratamiento de datos varía. Cuando las agencias de colocación y empresas de selección actúen por cuenta de sus clientes, siguiendo sus instrucciones, tendrán la consideración de encargadas del tratamiento de los datos personales. No obstante, cuando el contacto con las personas candidatas sea previo a disponer de ofertas de empleo concretas, y las agencias decidan la finalidad y los medios del tratamiento, sin seguir instrucciones -al menos inicialmente- de sus clientes, dichas empresas de selección actuarán como responsables del tratamiento[4].

---

[1] Un ejemplo válido sería el de una empresa que sigue el perfil de LinkedIn de un exempleado con pacto de no competencia con el objetivo de controlar su cumplimiento.

[2] *Dictamen 2/2017 del Grupo de Trabajo del Artículo 29.*

[3] Por ejemplo, preguntar en una entrevista de trabajo –y recabar el dato– acerca de si el/la candidato/a tiene intención de constituir una familia o tener hijos en el futuro podría ser considerado como un acto discriminatorio (STSJ Islas Canarias, Sala de lo social (Santa Cruz de Tenerife) de 7 de abril de 2014).

[4] Ello implica, entre otras cuestiones, que cuando las agencias actúen como encargadas, solo podrán tratar los datos de una persona candidata en particular para la ejecución del contrato con un cliente en particular de modo que, cuando se haya cubierto el puesto de trabajo para el cual fue contratada la agencia, esta deberá destruir o devolver los datos tratados.

- De igual forma las ETT serán también responsables en su calidad de empleadoras directas.

- Para la cesión de datos personales contenidos en el currículum entre empresas de un mismo grupo empresarial será necesario el consentimiento de la persona candidata.

3. Sistemas de denuncias internas o *whistleblowing*

- Estos sistemas se suelen configurar mediante la creación de buzones telemáticos internos a través de los cuales las personas trabajadoras de la compañía pueden comunicar la comisión, en su seno o en la actuación de terceros que contraten con ella, de actos o conductas contrarios a la ley o al convenio colectivo. La base jurídica para el tratamiento de los datos recogidos a través de estos sistemas de denuncias es el interés público en el sentido del artículo 6.1.e) del RGPD y de la exposición de motivos de la *Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* ("LOPDGDD").

- La Guía de la AEPD destaca el carácter primordial de informar, con carácter previo, de la existencia de estos sistemas y del tratamiento de los datos que conlleva la formulación de una denuncia, tanto a los denunciantes como a los potenciales denunciados.

- A su vez, los datos personales contenidos en estos sistemas podrán ser transmitidos a un tercero que investigue los hechos (por ejemplo, al *Data Protection Officer* de la matriz extranjera), o a una tercera compañía que investigue el hecho denunciado, realizándose una comunicación de datos de la que tanto el denunciante como el denunciado deberán ser debidamente informados.

- Las denuncias anónimas están admitidas por el artículo 24 de la LOPDGDD. Si la denuncia no fuera anónima deberá garantizarse la confidencialidad del denunciante.

- El acceso a los datos debe limitarse a quienes desarrollen las funciones de control interno y cumplimiento, o al encargado del tratamiento designado. El acceso del personal de recursos humanos a la información estará vetado, exceptuando procedimientos disciplinarios o notificaciones a la autoridad competente de hechos constitutivos de ilícitos.

- En todo caso, los datos deben suprimirse transcurridos 3 meses desde su introducción en el sistema de denuncias sin que se aplique la obligación de bloqueo, salvo que la finalidad de la conservación sea dejar evidencia del modelo de prevención de delitos.

4. Registro de jornada

- El registro de jornada en el ámbito laboral tiene su base jurídica en la obligación legal de registrar el horario concreto de inicio y finalización de la jornada de cada persona trabajadora, prevista en el artículo 34.9 del *Estatuto de los Trabajadores* ("TRLET"). La conservación del registro diario (no necesariamente de su totalización) será de 4 años, siendo válido cualquier medio de conservación, siempre que se garantice su preservación y la fiabilidad e invariabilidad de su contenido.

- La Guía parte del derecho de la persona trabajadora a ser informada sobre la existencia y el método del registro. Además, recomienda que el sistema de registro horario sea el menos invasivo posible, que no sea de acceso público ni esté situado en un lugar visible. Será necesario incluirlo en el registro de actividades de tratamiento con la posibilidad de realizar una evaluación de impacto dependiendo del número de personas trabajadoras o del concreto formato empleado para registrar la jornada.

- La confidencialidad de los datos del registro es esencial, de modo que se limita su acceso a las personas autorizadas por la Ley: personas trabajadoras interesadas, sus representantes legales y las autoridades a efectos de una investigación, como la Inspección de Trabajo y Seguridad Social o a petición judicial[5].

- Se establece explícitamente que los datos recogidos por medio del registro horario no pueden ser utilizados con finalidades distintas, como recabar la ubicación o geolocalización de una persona trabajadora, en la medida en que es un instrumento de comprobación del tiempo del trabajo y no del lugar donde se desarrolla la actividad. Asimismo, como novedad, se hace referencia a la posibilidad de realizar un registro horario a distancia para aquellas personas trabajadoras que no acudan físicamente al puesto de trabajo a través del acceso remoto a una intranet corporativa, o de aplicaciones en dispositivos digitales que deberán garantizar adecuadamente los derechos de las personas trabajadoras.

[5] Según la *Guía* del Ministerio de Trabajo sobre registro de jornada, "la permanencia a disposición no implica la obligación de entrega de copias, salvo pacto expreso en contrario, ni debe entregarse al trabajador individual copia de su registro diario, sin perjuicio de facilitar su consulta personal, ni a los representantes legales de los trabajadores, lo que no obsta, de nuevo, la posibilidad de estos últimos de tomar conocimiento de los registros de los trabajadores".

5. Registro salarial

- Al tratarse de un registro en el que no ha de constar el salario de cada persona trabajadora identificada individualmente, sino los valores medios de los salarios, los complementos salariales y las percepciones extrasalariales de la plantilla, la información se deberá tratar de manera disociada, por lo que el cumplimiento de la obligación legal prevista en el artículo 28.2 TRLET no debe implicar, en principio, un tratamiento de datos personales.

- Sin embargo, el dato disociado del registro podría convertirse en dato personal respecto de aquellas categorías o grupos profesionales con un reducido número de personas trabajadoras (por ejemplo, puestos directivos o altos cargos). Por este motivo, la Guía plantea implementar medidas de seguridad, informar del tratamiento (no del contenido del registro) y de la finalidad, así como asegurar la confidencialidad de la información compartida con los representantes legales de la plantilla[6].

- En cuanto a la consulta del registro salarial, las empresas tienen que facilitar el acceso al registro a la representación legal de la plantilla, teniendo derecho a conocer el contenido íntegro del mismo. En caso de no existir representantes legales, la persona trabajadora podrá acceder directamente al registro, si bien solo a las diferencias porcentuales que existieran en las retribuciones promediadas de hombres y mujeres, de manera desagregada, en atención a la naturaleza de la retribución y el sistema de clasificación aplicable. No se facilitarán en este supuesto los datos promediados respecto a las cuantías efectivas de las retribuciones que constan en el registro.

6. Cesión de datos a otras empresas (grupos de empresas y contratas)

- Según el *Informe AEPD 0494/2008*, los grupos de empresas no constituyen una única persona jurídica a efectos de la normativa de protección de datos, sino que cada empresa del grupo tiene personalidad jurídica propia y puede ser considerada como responsable del tratamiento de los datos.

[6] De hecho, la Guía de Uso de la *Herramienta del Análisis Cuantitativo por Sexo del Ministerio de Igualdad* señala que en aquellos casos en los que solo exista una persona en la organización con ese cargo, no debe incluirse la posición de dicha persona a efectos de publicar su salario.

- Con carácter general, la base jurídica de la comunicación de los datos entre empresas del mismo grupo podrá ser el interés legítimo (por ejemplo, centralización de actividades de carácter administrativo). Ahora bien, centralizar la información de todas las personas trabajadoras en un solo fichero al que puedan acceder todas las empresas del grupo no sería -según la AEPD- una práctica acorde con la normativa de protección de datos, salvo que se celebre un contrato como encargado del tratamiento.

- En caso de que el grupo o varias de sus empresas ocupen la posición de empleador único en la relación laboral, cuando la empresa matriz tome decisiones directamente, o bien cuando se presten servicios de forma indiferenciada entre varias empresas del grupo, la base jurídica de la comunicación de los datos podría ser el cumplimiento del contrato de trabajo.

- En caso de subcontratación, la empresa subcontratista podrá comunicar a la empresa principal los datos de su plantilla, con base en una obligación legal, derivada de la responsabilidad solidaria o subsidiaria que puede alcanzar a la empresa principal.

7. Videovigilancia

- El tratamiento de datos personales de las personas trabajadoras con fines de videovigilancia para el ejercicio de las funciones de control de los trabajadores se regula en el artículo 89 de la LOPDGDD, donde se recoge que la base jurídica reside en el TRLET, por lo que no resulta necesario recabar su consentimiento. Los sistemas de videovigilancia, con carácter general, sólo deben utilizarse cuando no sea posible acudir a otros medios que causen un menor impacto en la privacidad de las personas trabajadoras. En este sentido, los sistemas de videovigilancia para control empresarial requerirán de la existencia de una relación de proporcionalidad entre la finalidad perseguida y el modo en que se traten las imágenes y no haya otra medida más idónea.

- A su vez, la Guía concreta cómo dar cumplimiento al principio de minimización de datos en este ámbito, analizando las siguientes cuestiones:

  - el número necesario de cámaras para cumplir con la función de videovigilancia;
  - el análisis de los requisitos técnicos de las cámaras e implantación de medidas de seguridad;
  - el cumplimiento del deber de informar[7];

[7] Recientemente, el TSJ de Andalucía, en su sentencia 1146/2020, de 1 junio (*Rec. 4152/2018*), ha confirmado la nulidad del despido de un vigilante de seguridad que fue grabado a través del sistema de videovigilancia instalado por la empresa, ocultando su ubicación y existencia. En este caso, el Tribunal considera que la compañía vulneró el derecho a la intimidad del trabajador por no informar previamente de la colocación de las cámaras en el centro de control –ni individualmente ni a través de carteles en las instalaciones– ni de que estas podían ser empleadas para fines de control y sanción. Tampoco constaba la presencia de distintivos de advertencia de estar instalada la cámara.

- en el supuesto de que se capte la comisión flagrante de un acto ilícito mediante la instalación de cámaras ocultas, parece avalarse la doctrina del TEDH en el caso *López Ribalda II*, siempre que existan sospechas fundadas y exista un dispositivo informativo en lugar suficientemente visible, concretando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar derechos;
- aplicación de la normativa de protección de datos a las cámaras desactivadas (que puedan ser fácilmente activadas);
- prohibición de la instalación de cámaras en lugares destinados al descanso o esparcimiento;
- el plazo de conservación de los datos será de 1 mes, salvo cuando deban ser conservados para acreditar la comisión de actos atentatorios contra la integridad de las personas.

8. Geolocalización

La AEPD destaca la licitud de los sistemas de geolocalización aplicados a las herramientas propiedad de la empresa (vehículo, dispositivos digitales, etc.), siempre y cuando se cumplan los principios de la normativa de protección de datos y se garanticen las cautelas correspondientes.

- Con carácter previo a la implementación de estas tecnologías deberá realizarse una evaluación de impacto. A su vez, la empresa deberá asegurar que los datos recogidos sirvan a un fin específico, sin excederse de dicha finalidad concreta, sin perjuicio de que el empleado pueda desactivar el sistema cuando las circunstancias lo exijan (por ejemplo, visita médica).

- La Guía recomienda que los sistemas de seguimiento estén diseñados para registrar los datos de localización sin proporcionar todos los detalles al empleador, y confirma la ilicitud –prevista legalmente– de imponer a la persona trabajadora la obligación de proporcionar medios personales para facilitar la geolocalización (por ejemplo, el teléfono móvil).

- Otra cuestión tratada por la Guía es la de los registradores de datos de incidencias, especialmente relevante en el sector del transporte. Habrá de valorarse la existencia de medios menos invasivos, así como la aplicación de los principios propios de la de protección de datos (proporcionalidad, legitimación, etc.).

9. Seguimiento mediante detective

- La normativa laboral habilita a las empresas para adoptar medidas de control y vigilancia de muy distinta intensidad, entre las cuales se encuentra la figura del detective privado. La AEPD recuerda la necesidad de tener en cuenta las siguientes cautelas:

(i) superar el test de proporcionalidad;

(ii) no investigar de la vida íntima de las personas trabajadoras; y

(iii) no require de consentimiento.

- En relación con el informe del detective privado, únicamente se hará constar información directamente relacionada con el objeto y la finalidad de la investigación, que deberá ser conservada, al menos, durante 3 años y mantener un carácter estrictamente reservado.

10. Vigilancia de la salud

- En el campo de la vigilancia de la salud, el tratamiento de datos personales se encuentra legitimado por la existencia de una relación contractual y la obligación que tiene la empresa de cumplir con las obligaciones legales establecidas en el TRLET, la *Ley de Prevención de Riesgos Laborales* y normativa que la desarrolla.

- Además de recordar los principios de confidencialidad, información y proporcionalidad, la Guía expone que la vigilancia de la salud puede llegar a ser obligatoria conforme a la normativa aplicable, previo informe de la representación legal de los trabajadores, y sin que el convenio colectivo constituya una base legítima suficiente:

  (i) cuando el reconocimiento sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de la persona trabajadora individualmente considerada;

  (ii) cuando sea necesario verificar si el estado de salud de la persona trabajadora puede constituir un peligro para compañeros de trabajo y/o terceras personas relacionadas con la empresa;

  (iii) cuando exista una obligación legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad (enfermedades profesionales).

- El reconocimiento médico deberá vincularse a la conclusión sobre la aptitud laboral ("apto", "apto condicionado" o "no apto" para el puesto de la persona trabajadora), sin que pueda la empresa acceder a ningún otro tipo de información, como el concreto diagnóstico médico que justifica la conclusión.

- En lo relativo a la tecnología Weareable, la AEPD señala que la monitorización de datos de salud a través de dispositivos inteligentes, como pulseras o relojes, está por lo general prohibida –a menos que esté establecida por ley o reglamento–, debido a que no se entiende comprendida 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, carece de finalidad legítima y vulnera el principio de proporcionalidad.

Y ahora, ¿qué? Próximos pasos

- El cumplimiento normativo en materia de protección de datos es una cuestión de gran relevancia en el día a día de las empresas, especialmente desde que la actual normativa de protección de datos comenzó a ser directamente aplicable en mayo de 2018. Por ello, el conocimiento de las novedades legislativas y su adaptación a las relaciones laborales conlleva ventajas competitivas estratégicas en el mercado.

- Nuestro equipo de abogados especializado en cuestiones de índole laboral, protección de datos y nuevas tecnologías asesora a las empresas para garantizar el pleno entendimiento de las actualizaciones y su afectación en las relaciones laborales, para adaptar los contratos de trabajo y las políticas y procedimientos de empresa, y evitar posibles sanciones derivadas del incumplimiento del régimen legal aplicable o ante casos de brechas de seguridad.

- Si desea más información a la contenida en este Legal Flash respecto a la interpretación de la nueva Guía de la AEPD y su implementación en las relaciones laborales puede dirigirse a su contacto habitual en Cuatrecasas.