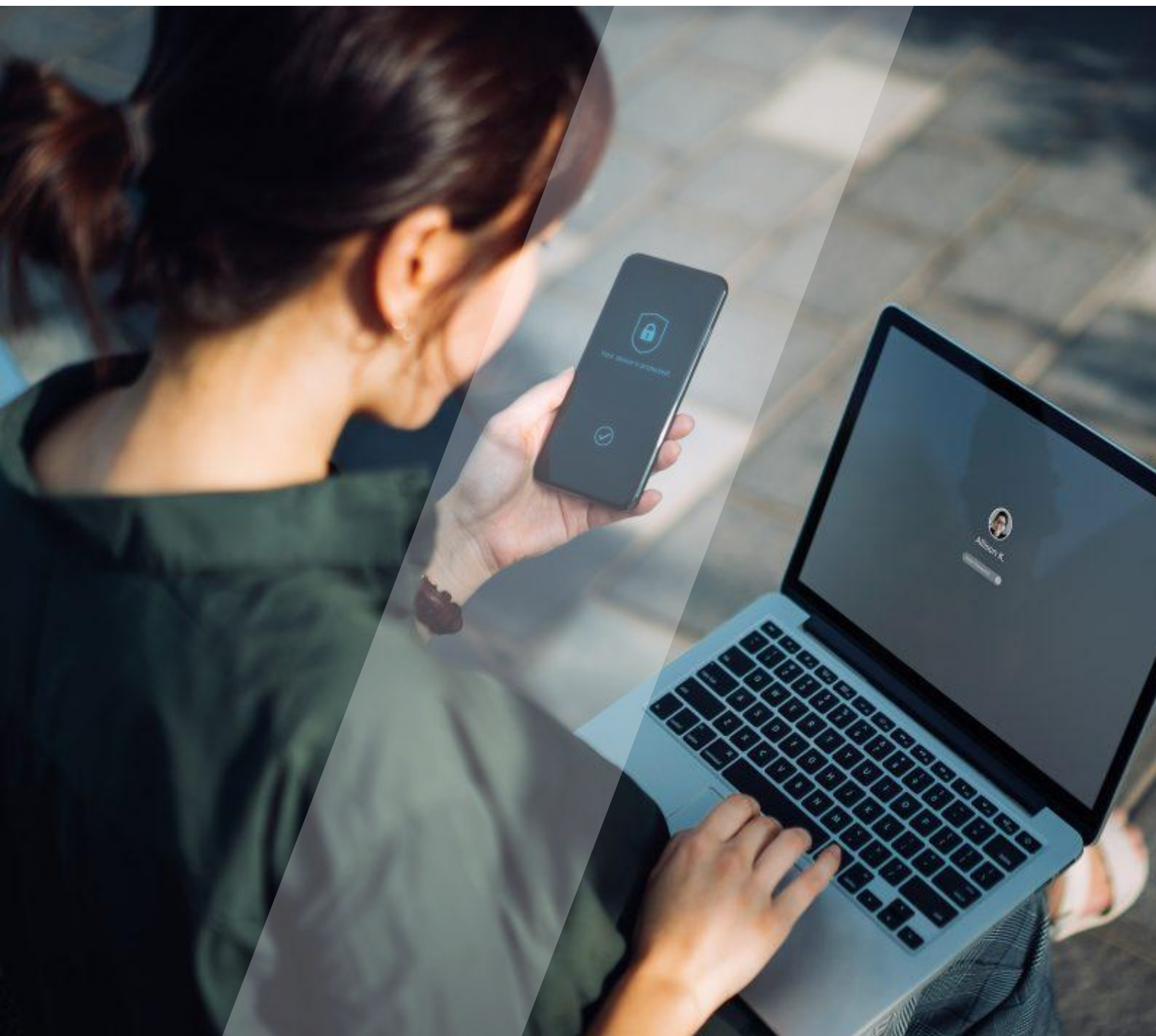




El derecho a la protección de datos en las relaciones laborales

Concepto de tratamiento de datos personales y su regulación

forv/s
mazars

La normativa de protección de datos personales ha ido adquiriendo una relevancia cada vez mayor a lo largo de los años, pasando a ser un elemento esencial y que se debe tener en cuenta en las relaciones tanto interpersonales como interprofesionales. En lo que en el presente artículo atañe, merece mencionarse el gran impacto que ello supone en las relaciones entre empresa y persona trabajadora, puesto que la totalidad de las empresas debe cumplir con dicha normativa, exponiéndose a sanciones muy graves en caso de incumplimiento.

Actualmente, la normativa fundamental y básica se encuentra recogida en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, “Reglamento general de protección de datos” o “RGPD”) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, “LOPDPGDD”).

Con carácter previo, conviene recordar que el artículo 4.2 del RGPD define el tratamiento de datos personales como *“cualquier operación o conjunto de operaciones realizadas sobre daos personales, ya sea por procedimientos automatizados o no, tales como su recogida, registro, organización, conservación, consulta, utilización, comunicación, supresión o destrucción”*. En consecuencia, **prácticamente cualquier actuación que una empresa lleve a cabo con información relativa a una persona trabajadora constituye un tratamiento de datos personales y debe ajustarse a las exigencias del RGPD.**

En primer lugar, a fin de un análisis más exhaustivo, debe identificarse a qué se refiere el concepto de tratamiento de datos personales. El artículo 4.1 del RGPD considera dato personal *“toda información relativa a una persona física identificada o identificable”*. A modo de ejemplo, se entiende como dato personal aquella (i) información asociada a una persona concreta como son su nacimiento, matrimonio, domicilio, etc; (ii) información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo; (iii) información sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre las creencias religiosas o ideologías; y (iv) nombre, apellidos, N.I.F., datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o socia, entre otros.

La protección de dichos datos se fundamenta esencialmente en el artículo 18 de la Constitución Española relativa al derecho a la intimidad familiar y personal y el derecho al honor, así como al secreto de las comunicaciones.

La tutela de la protección de datos es asumida por distintos órdenes jurisdiccionales siendo ello en el marco de la jurisdicción penal, civil, contenciosa administrativa, así como en el orden laboral siendo su singular protección el objeto de análisis en el presente artículo.

El tratamiento de los datos personales en el ámbito laboral

El tratamiento de datos personales en el ámbito laboral presenta determinadas particularidades derivadas de la propia relación entre empleador y persona trabajadora. En este sentido, el RGPD prevé que, en determinados supuestos, puedan tratarse categorías especiales de datos personales cuando dicho tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del Derecho Laboral, de conformidad con el artículo 9.2.b del RGPD.

Con carácter general, el tratamiento de datos personales en el marco de la relación laboral no requiere el consentimiento de la persona trabajadora, dado que la base jurídica que lo legitima suele encontrarse en la “*ejecución del contrato de trabajo*” (artículo 6.1.b del RGPD), el “*cumplimiento de obligaciones legales*” por parte del empleador (artículo 6.1.c del RGPD) o, en determinados supuestos, en el “*interés legítimo*” del empleador (artículo 6.1.f del RGPD). No obstante, **ello no implica que el empleador pueda tratar cualquier información sin limitación alguna, debiendo respetar en todo caso los principios de minimización, proporcionalidad y transparencia**. Asimismo, el empleador deberá siempre mantener informada a la persona trabajadora sobre el tratamiento de sus datos personales, incluyendo la finalidad, la base jurídica, los destinatarios y los derechos que le asisten.

Por tanto, el consentimiento de la persona trabajadora no constituye, como norma general, una base jurídica adecuada para legitimar el tratamiento de datos personales en el ámbito de la relación laboral, dado que el desequilibrio existente entre las partes puede impedir que dicho consentimiento sea prestado de forma libre, considerándose, en consecuencia, viciado o carente de validez. En este contexto, el tratamiento de los datos personales de las personas trabajadoras deberá fundamentarse en otras bases legitimadoras previstas en la normativa, como las mencionadas anteriormente. En consecuencia, el empleador 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 que resulten necesarios para la formalización del contrato, la gestión de la relación laboral y el cumplimiento de las obligaciones derivadas de esta.

En cualquier caso, **el empleador, deberá cumplir siempre con los deberes de seguridad, secreto y confidencialidad, así como con el principio de responsabilidad proactiva, debiendo ser capaz de demostrar el cumplimiento de las obligaciones previstas en la normativa de protección de datos**.

Asimismo, el propio RGPD permite a los Convenios Colectivos de aplicación para que puedan establecer normas específicas relativas al tratamiento de los datos personales con las personas trabajadoras.

A continuación, analizaremos cómo incide la protección de datos en casos concretos que se dan en la relación laboral entre empleador y empleado.

¿Puede la empresa conservar los datos de la persona candidata?

Una vez concluido el proceso de selección, si la persona candidata no es contratada, desaparece la base jurídica que permitía inicialmente el tratamiento de sus datos personales para dicha finalidad. Por lo tanto, la empresa no podrá conservar sus datos indefinidamente ni utilizarlos para finales distintas de aquellas para las que fueron recabados.

No obstante, la conservación del currículum y de los datos personales de la persona candidata para futuros procesos de selección podrá resultar lícita cuando exista una base jurídica que legitime dicho tratamiento. Para ello, la empresa deberá informar previamente a la persona interesada sobre esta posibilidad y, cuando corresponda, obtener su consentimiento para mantener sus datos durante un periodo adicional. Asimismo, podrá conservar determinados datos cuando exista un interés legítimo debidamente justificado, como la defensa frente a posibles reclamaciones derivadas del proceso de selección, siempre que dicha conservación sea necesaria y proporcional.

En ausencia de una base jurídica válida, la empresa deberá proceder a la supresión de los datos personales y, en su caso, al bloqueo de aquellos datos que deban conservarse para hacer frente a posibles responsabilidades legales, respetando en todo caso el principio de limitación del plazo de conservación previsto en el artículo 5.1.e) del RGPD.

¿Puede la empresa publicar los datos de productividad de sus empleados?

La publicación de datos relativos a la productividad de las personas trabajadoras constituye un tratamiento de datos personales, y, por tanto, deberá contar con una base jurídica que lo legitime, así como respetar los principios de proporcionalidad, minimización y limitación de la finalidad previstos en el RGPD.

En aquellos supuestos en los que la empresa pretenda fundamentar dicho tratamiento en su interés legítimo, conforme al artículo 6.1.f del RGPD, deberá realizarse la correspondiente ponderación entre los intereses perseguidos por el empleador y los derechos e intereses de las personas trabajadoras afectadas.

Para ello, deberán valorarse, entre otros, los siguientes aspectos:

- (i) la satisfacción de los intereses legítimos en virtud del artículo 6.1 f) del RGPD.
- (ii) La apreciación de la “necesidad” de tratamiento exige una ponderación entre los intereses del empleador y de la persona trabajadora.
A modo de ejemplo, el abono de un complemento de productividad y la publicación de los datos de rendimiento para dotar de transparencia el proceso y motivar a las personas trabajadoras a obtener mejores resultados podría constituir un interés legítimo.
- (iii) La publicidad de datos de productividad no puede ser indiscriminada, sino que debe limitarse su publicación a las personas trabajadoras de la empresa y, en ningún caso a personas distintas.
- (iv) La publicación debe realizarse del modo que resulte menos perjudicial para la persona trabajadora.
- (v) Debe garantizarse que los datos de productividad publicados no pueden ser utilizados para futuros tratamientos con una finalidad incompatible de aquella que motivó su recogida.

Divulgación de datos médicos de la persona trabajadora

Los datos relativos a la salud de las personas trabajadoras constituyen una categoría especial de datos personales conforme al artículo 9 del RGPD, por lo que su tratamiento requiere una protección reforzada y únicamente podrá realizarse cuando concurra alguna de las excepciones previstas en dicha normativa.

En el ámbito laboral, el tratamiento de datos de salud puede resultar necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en materia laboral y de Seguridad Social.

En la actualidad, derivado de la problemática que plantea el incremento de las bajas médicas de índole laboral en España, se plantea también el problema relativo a la notificación de los datos relativos a las situaciones de salud de la persona trabajadora, concretamente, de la notificación de los partes médicos sobre la incapacidad temporal.

A raíz del Real Decreto 1060/2022, de 27 de diciembre, por el que se regulan determinados aspectos de la gestión y control de los procesos por incapacidad temporal, se eliminó la obligación de que la persona afectada traslade a la empresa los partes médicos de baja, confirmación y alta. Actualmente, corresponde al Instituto Nacional de la Seguridad Social o a las entidades competentes remitir telemáticamente a la empresa la información necesaria para la gestión de la situación de incapacidad temporal.

No obstante, **dicha comunicación debe limitarse a los datos estrictamente necesarios para la gestión administrativa de la incapacidad temporal**, sin incluir información relativa al diagnóstico, motivo médico o cualquier otro dato de salud que no resulte imprescindible para dicha finalidad.

En este sentido, en la Sentencia de la Audiencia Nacional de 16 de noviembre de 2022 (Rec. 270/2022) se declaró la nulidad del sistema de remisión de partes de baja, al no ser proporcionado, puesto que en el mismo había que rellenar una serie de campos como: tipo de baja, duración fecha de inicio y expedición del parte y el motivo, extremos estos que no eran necesarios conforme a la legalidad vigente.

Por lo tanto, la empresa deberá garantizar que cualquier tratamiento de datos médicos de las personas trabajadoras se limite a la finalidad para la que fue autorizado, evitando acceder o divulgar información sanitaria que exceda de las necesidades propias de la relación laboral.

¿Cómo incide la protección de datos en cuanto al uso de cámaras de videovigilancia en el lugar de trabajo?

La imagen de una persona constituye un dato personal, ya que identifica o hace identificable a una persona. En este sentido, **la instalación de cámaras, con finalidades como la seguridad, el control laboral, el acceso a zonas restringidas captando la matrícula del coche y la imagen del conductor, o incluso la monitorización de una UVI, supondría un tratamiento de datos de carácter personal y, en consecuencia, resultaría de aplicación la normativa de protección de datos.**

Cada vez más, las empresas optan por establecer medidas de videovigilancia con el fin de controlar a sus empleados y, dicha actuación se fundamenta en el artículo 20.3 del Estatuto de los trabajadores, en el que se establece que se permite al empresario adoptar las medidas de vigilancia y control que estime oportunas para verificar el cumplimiento de las obligaciones laborales, siempre respetando la dignidad de la persona trabajadora.

Para la implantación de dichas medidas de control por parte del empresario deben respetarse los derechos mínimos de las personas trabajadoras y, los derechos a la protección de datos. Para ello, debe realizarse un test de proporcionalidad valorando si la medida de control cumple con (i) el juicio de idoneidad (ii) el juicio de necesidad y (iii) el juicio de proporcionalidad. Superado dicho test, se podrá adoptar la medida, pero cumpliendo con el derecho a la protección de datos. A estos efectos, el empleador debe:

- a. Debe informar a las personas trabajadoras sobre la finalidad del tratamiento de datos, y por tanto sobre la existencia y propósito de la medida de control.
- b. No puede recabar más datos de los estrictamente necesarios.
- c. No está legitimado para utilizar los datos con finalidades distintas del control empresarial.
- d. Estas cautelas se extienden también a cualquier otro medio de control que suponga tratamiento de datos personales.

En estos casos pues, **es imprescindible que la empresa informe a las personas trabajadoras y, en su caso, a sus representantes, con carácter previo, y de forma expresa, clara y concisa, acerca la imposición de cámaras de videovigilancia.**

Sin embargo, la norma permite que, en caso de flagrancia de una conducta ilícita, el deber de información se tenga por efectuado mediante la colocación en lugar visible, de un distintivo, que advierta sobre la existencia del sistema, su responsable y los derechos derivados del tratamiento de los datos.

En este sentido cabe mencionar la Sentencia del TEDH en el caso *Barbulescu v. Rumanía*, en la que se examina la compatibilidad de la vigilancia encubierta con el artículo 8 del Convenio Europeo de Derechos Humanos, en la que se alcanza la siguiente conclusión: *“si bien no puede aceptar que la mínima sospecha de robos u otras irregularidades cometidas por los empleados, pueda justificar la instalación de un sistema de videovigilancia encubierta por parte del empleador, la existencia de sospechas razonables de que se habían cometido graves irregularidades, y el alcance de los robos constatados en el presente asunto, pueden parecer una justificación seria”*. Se concluye pues, que en aquellos casos en los que existan sospechas razonables de la comisión de irregularidades por parte de los empleados justificaría la instalación de sistemas de videovigilancia.

Finalmente, respecto al plazo de conservación de las imágenes, el art. 22.3 de la LOPDGDD establece que podrán conservarse durante un plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

¿Y respecto del uso de sistemas de geolocalización?

Para que la geolocalización sea lícita, debe superar el examen de proporcionalidad y subsidiariedad, utilizándose únicamente cuando no existan alternativas menos invasivas. En esta línea, la Audiencia Nacional se pronunció señalando que una empresa no puede implantar el seguimiento de forma generalizada a toda su plantilla si las funciones del puesto no lo justifican, ni tampoco puede obligar a una persona trabajadora a poner su propio teléfono móvil al servicio de esta vigilancia. Asimismo, los principios de minimización y limitación de la finalidad prohíben que los datos se desvíen del objetivo para el que fueron recogidos; si el sistema nace para cumplir con el registro de la jornada laboral, es ilegal rastrear la ubicación del empleado minuto a minuto, debiendo limitarse exclusivamente a fichar las horas de inicio y fin.

El gran conflicto surge cuando la tecnología se instala en herramientas propiedad de la empresa, como los vehículos corporativos. Aunque el empresario argumente que vigila su patrimonio y no a la persona, la realidad es que el rastreo del objeto conlleva inevitablemente el control de la persona trabajadora, lo que exige salvaguardas drásticas. Las empresas están obligadas a informar de manera expresa, clara e inequívoca sobre estos dispositivos, e incluso a realizar evaluaciones de impacto previas si la tecnología es nueva. Además, este control tiene una barrera temporal infranqueable: la jornada laboral.

Los Tribunales han dejado claro que el poder de vigilancia de la empresa se apaga cuando termina el horario de trabajo.

Por ello, si se permite el uso privado del vehículo, se debe garantizar el derecho a la desconexión mediante sistemas que permitan desactivar el GPS o que solo se activen de forma excepcional ante alertas de robo.

Las consecuencias de no cumplir con la Ley de Protección de Datos

El incumplimiento de la normativa de protección de datos puede tener importantes consecuencias económicas, legales y reputacionales para las empresas. En este sentido, **el artículo 83 del RGPD prevé sanciones administrativas que pueden alcanzar los 20 millones de euros o, tratándose de una empresa, el 4% del volumen de negocio anual global del ejercicio financiero anterior, optándose por la cuantía de mayor importe. Estas sanciones pueden ir acompañadas de otras medidas correctivas impuestas por autoridad de control, como apercibimientos, limitaciones del tratamiento o la obligación de adoptar medidas para adecuarse a la medida.**

En España, la autoridad encargada de velar por el cumplimiento de la normativa es la Agencia Española de Protección de Datos (AEPD). Para determinar la cuantía de una sanción, la AEPD tiene en cuenta diversos factores, entre ellos la naturaleza, gravedad y duración de la infracción, el número de personas afectadas, el grado de responsabilidad del responsable del tratamiento, la intencionalidad o negligencia, las medidas adoptadas para paliar los daños y el nivel de cooperación con la autoridad de control.

Para ello, el cumplimiento de la normativa de protección de datos no debe entenderse únicamente como una obligación legal, sino como un elemento esencial para garantizar una gestión responsable de la información personal y reforzar la confianza de las personas trabajadoras en la organización.

Conclusiones

Como se ha podido observar, la protección de datos en el entorno laboral se ha convertido en una obligación de gran relevancia para las empresas. **Pese a que el contrato de trabajo permite ciertos márgenes de control sin necesidad del consentimiento expreso de la persona trabajadora, este poder nunca es absoluto, debiendo respetarse en todo caso todos los derechos que le protegen, entre ellos especialmente el derecho a la protección de datos.**

La clave de todo radica en la proporcionalidad y la transparencia. Cuando se discute la viabilidad de instalar cámaras, revisar los datos de productividad o de activar sistemas de geolocalización, la empresa está obligada a informar siempre de forma clara y a buscar la opción que resulte menos invasiva para la persona trabajadora. Además, conviene recordar que el poder de vigilancia de la dirección termina en el mismo instante en el que finaliza la jornada laboral.

Saltarse estos límites e ignorar las normativas del RGPD o la LOPDGDD expone a las organizaciones a un riesgo financiero y reputacional inasumible, con multas que pueden alcanzar los 20 millones de euros. En conclusión, respetar la privacidad de la plantilla ya no es solo una exigencia legal, sino la única vía para garantizar una gestión empresarial segura, justa y eficiente.

Natalia Murillo Sorroche

Abogada laboralista en Forvis Mazars

natalia.murillo@forvismazars.com

Agustina Pardo

Privacy consultant en Forvis Mazars

agustina.pardo@forvismazars.com

Forvis Mazars es la marca de la red Forvis Mazars Global (Forvis Mazars Global Limited), una red mundial de servicios profesionales. La red opera bajo una única marca en todo el mundo, con sólo dos miembros: Forvis Mazars, LLP en Estados Unidos y Forvis Mazars Group SC, una asociación internacional integrada que opera en más de 100 países y territorios.

Las entidades de la red Forvis Mazars en España prestan servicios de auditoría & assurance, asesoramiento fiscal, legal, financiero, consultoría, outsourcing y sostenibilidad a través de 900 profesionales en 8 oficinas.

Visita forvismazars.com/es para conocer más.

