DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 22 | Abril 2022

LA PROTECCIÓN DE DATOS EN LAS RELACIONES LABORALES

Í N D I C E

LA PROTECCIÓN DE DATOS EN LAS RELACIONES LABORALES

	Página
Introducción	**2**
Aspectos generales	**3**
Base de licitud	**4**
Derechos de protección de datos	**5**
Sistemas internos de denuncias	**7**
Protección de la privacidad de las víctimas de acoso y violencia de género	**8**
Material complementario y noticias	**10**

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"SE RECONOCE EL DERECHO A LA INTIMIDAD EN EL USO DE DISPOSITIVOS DIGITALES Y FRENTE AL USO DE DISPOSITIVOS DE VIDEOVIGILANCIA Y GEOLOCALIZACIÓN, ASÍ COMO A LA DESCONEXIÓN DIGITAL".

INTRODUCCIÓN

Las entidades públicas y privadas requieren tratar datos personales de los recursos humanos necesarios para llevar a cabo su actividad. El tratamiento de datos de empleados públicos debe garantizar los principios y requisitos legales establecidos por la normativa de protección de datos vigente.

En particular, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, "LOPDGDD") establece varias disposiciones aplicables al ámbito del sector público, especialmente respecto a aquellas finalidades dirigidas a controlar el cumplimiento de las obligaciones del personal público y garantizar la integridad de los dispositivos portátiles destinados al ejercicio de sus funciones.

La LOPDGDD modifica el texto refundido de la Ley del Estatuto Básico del Empleado Público (en adelante, "EBEP") reconociendo el derecho del empleado público a la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

La Agencia Española de Protección de Datos publicó la Guía relativa a la *"Protección de datos en las relaciones laborales"* destinada a proporcionar una orientación de carácter práctico, no vinculante, que facilite a los responsables y encargados el cumplimiento de la legislación.

En el presente documento se analizarán los principales aspectos tratados en la *Guía de protección de datos en las relaciones laborales*, desde la perspectiva enfocada en su aplicación en el sector público.

"EL TRATAMIENTO DE DATOS DE LOS RECURSOS HUMANOS PUEDE ABARCAR UN AMPLIO ABANICO DE DATOS PERSONALES, INCLUIDAS CATEGORÍAS ESPECIALES DE DATOS".

ASPECTOS GENERALES

Conforme a lo dispuesto en el artículo 4.1 del Reglamento General de Protección de Datos (en adelante, "RGPD") se considera dato de carácter personal:

> *"Toda información relativa a una persona física identificada o identificable".*

Como se adelantaba en la introducción, el tratamiento de datos de los recursos humanos, ya sean referentes al sector público o en el privado, debe garantizar la privacidad y el cumplimiento de la normativa de protección de datos vigente. En particular, el tratamiento puede abarcar un amplio abanico de datos personales, incluidas categorías especiales de datos.

El artículo 9.1 RGPD establece con carácter general la prohibición de tratar categorías especiales de datos. Sin embargo, en su segundo apartado, establece una relación de supuestos en virtud de los cuales se habilita a los Responsables a tratar esta categoría de datos personales.

Uno de las excepciones a la que hace referencia la Agencia Española de Protección de Datos en la *Guía de protección de datos en las relaciones laborales* es la establecida en el artículo 9.2.b) RGPD es cuando el tratamiento:

> *"Es 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…"*

Ejemplos de categorías especiales de datos

Información relativa la situación de discapacidad de la persona trabajadora a efectos de reducciones o bonificaciones de cuotas a la Seguridad Social.

Sistema de fichaje para el control horario basado en el reconocimiento facial/huella dactilar (datos biométricos).

BASE DE LICITUD

El tratamiento de datos personales exige que el responsable del tratamiento cuente con una "base jurídica" que le legitime para ello.

En las relaciones laborales, la base jurídica principal es la ejecución del contrato de trabajo (artículo 6.1.b RGPD). En lo referente al consentimiento como base de licitud en el ámbito que nos ocupa, la AEPD establece en la Guía de Protección de Datos y Relaciones Laborales, que el consentimiento del interesado no es válido cuando se proporciona en un contexto de "desequilibrio claro entre el interesado y el responsable del tratamiento". En el ámbito público, esta imposibilidad se refleja principal y claramente en la relación profesional que vincula al personal laboral con la entidad pública:

> *Artículo 19 Ley 4/2021, de 16 de abril, de la Función Pública Valenciana*
>
> *"Es personal laboral quien […] está vinculado a cualquiera de las administraciones públicas, organismos públicos, consorcios o universidades públicas, mediante una relación profesional caracterizada por las notas de **ajenidad, dependencia**, voluntariedad y retribución.*

«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»

(Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 291).

"EL CONSENTIMIENTO DEL INTERESADO NO ES VÁLIDO CUANDO SE PROPORCIONA EN UN CONTEXTO DE DESEQUILIBRIO CLARO ENTRE EL INTERESADO Y EL RESPONSABLE DEL TRATAMIENTO".

"LA LIMITACIÓN DEL TRATAMIENTO SE BASA EN EL MARCADO DE LOS DATOS DE CARÁCTER PERSONAL CONSERVADOS CON EL FIN DE LIMITAR SU TRATAMIENTO EN EL FUTURO".

DERECHOS DE PROTECCIÓN DE DATOS

Las personas trabajadoras, en tanto son interesados en el tratamiento de datos personales, pueden ejercer los siguientes derechos frente al responsable del tratamiento:

DERECHO DE ACCESO (ART. 15 RGPD)

Independientemente de la información que se le haya proporcionado sobre el tratamiento, la persona trabajadora tiene derecho a obtener la confirmación de que se está produciendo un tratamiento de datos y, en su caso, cómo se está produciendo el mismo.

Asimismo, pueden solicitar una **copia de los datos personales** que están siendo objeto del tratamiento.

DERECHO DE RECTIFICACIÓN (ART. 16 RGPD)

Las personas trabajadoras tienen la posibilidad de exigir la rectificación de los datos inexactos que estén siendo objeto de tratamiento, así como completar aquella información de carácter personal que resulte incompleta.

DERECHO DE SUPRESIÓN (ART.17 RGPD)

Las personas trabajadoras tienen la posibilidad de exigir la supresión de los datos personales objeto del tratamiento en determinadas situaciones, tales como: cuando los datos personales no sean necesarios o la base de licitud sea el consentimiento y éste haya sido retirado.

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO (ART. 18)

Conforme a lo dispuesto en el artículo 4.3 RGPD la limitación del tratamiento se basa en "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro". Es un derecho de las personas trabajadoras cuando se dan las circunstancias establecidas en el RGPD.

"SE RECONOCE COMO DERECHO INDIVIDUAL DE LOS EMPLEADOS PÚBLICOS EL DERECHO A LA INTIMIDAD EN EL USO DE LOS DISPOSITIVOS DIGITALES Y EL DERECHO A LA DESCONEXIÓN DIGITAL".

DERECHO A LA PORTABILIDAD DE LOS DATOS (ART.20 RGPD)

Cuando la base de licitud del tratamiento sea el consentimiento o la ejecución de un contrato, la persona trabajadora tiene derecho a obtener sus datos personales en un formato o estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento.

DERECHO DE OPOSICIÓN (ART. 21 RGPD)

Si la base de licitud es la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero o una misión realizada en interés público, las personas trabajadoras podrán ejercer el derecho de oposición, salvo que se acrediten motivos legítimos que prevalezcan sobre los intereses, derechos y libertades de las personas trabajadoras o para la formulación, el ejercicio o la defensa de reclamaciones.

Además de los derechos mencionados cabe destacar la modificación del EBEP con la entrada en vigor de la disposición final decimocuarta de la LOPDGDD. Con esta modificación se reconoce como derecho individual de los empleados públicos el **derecho a la intimidad** en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como el **derecho a la desconexión digital** en los términos establecido en la legislación vigente.

En base a lo establecido en el artículo 88 LOPDGDD, el derecho a la desconexión digital tiene por objetivo garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

SISTEMAS INTERNOS DE DENUNCIAS O "WHISTLEBLOWING"

Es habitual en la práctica configurar los sistemas internos de denuncias o "*whistleblowing"* mediante la creación de buzones internos. A través de estos canales las personas trabajadoras ponen de manifiesto la comisión de actos o conductas contrarias a la ley.

En lo referente a la base de licitud de estos sistemas, la propia LOPDGDD establece que la licitud del tratamiento relativo a la implementación de sistemas de denuncias internas proviene de la existencia de un **interés público**, en los términos establecidos en el artículo 6.1.e) del RGPD. Además, la transposición en España de la Directiva (UE) 2019/1937 puede implicar una **obligación legal**.

"LA IMPLEMENTACIÓN DE SISTEMAS DE DENUNCIAS INTERNAS PROVIENE DE LA EXISTENCIA DE UN INTERÉS PÚBLICO"

El artículo 24.5 LOPDGDD establece que los principios que se recogen en sus apartados 1-4 serán aplicables a los sistemas de denuncias internas que pudieran crearse en las Administraciones Públicas. En particular, los requisitos que debe reunir un sistema de información de denuncias internas son los siguientes:

- Los empleados y terceros deberán ser informados acerca de la existencia del sistema.
- Se deberá limitar el acceso a los datos contenidos en el sistema al personal estrictamente necesario.
- Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos personales contenidos en el sistema, especialmente los referidos al persona denunciante de los hechos.
- La LOPDGDD permite sistemas de denuncias internas "anónimas".
- Debe regir el principio de limitación del plazo de conservación de los datos personales. En todo caso, transcurridos tres meses de la introducción de los datos, deberá procederse a su supresión.

Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que resulte de aplicación la obligación de bloqueo establecida en el artículo 32 LOPDGDD.

PROTECCIÓN DE LA PRIVACIDAD DE LAS VÍCTIMAS DE ACOSO Y VIOLENCIA DE GÉNERO

La información de carácter personal de las víctimas de acoso en el trabajo y de las mujeres supervivientes a la violencia de género tienen, con carácter general, la consideración de **categorías especiales de datos personales**, por lo que se exige al responsable del tratamiento una protección reforzada (Informe AEPD 149 – 2019).

En los supuestos de acoso en este ámbito, en sus distintas modalidades, el responsable del tratamiento tendrá que adoptar medidas oportunas respecto del acosador y de la persona acosada. Entre estas medidas se incluye la obligación de **proteger los datos personales.**

La puesta en marcha de procedimientos sancionadores frente al acosador no requiere del consentimiento de la persona acosada. La base de licitud en este caso sería el cumplimiento de una obligación legal (art. 6.1.c) del RGPD). Por un lado, en el sector privado, la empresa es garante de la salud y seguridad en el trabajo conforme a los artículos 4.2.d del Estatuto de los trabajadores y 14 de la a Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (LPRL). Por otro lado, en el sector público, rige lo establecido en el EBEP:

- Los funcionarios públicos y el personal laboral quedan sujeto sal régimen disciplinario establecido en el TÍTULO VII EBEP y a las normas que las leyes de Función Pública dicten en desarrollo del EBEP. (ART. 93.1 EBEP)
- Las Administraciones Públicas corregirán disciplinariamente las infracciones del personal a su servicio, sin perjuicio de la responsabilidad patrimonial o penal que pudiera derivarse de tales infracciones. (ART.94.1 EBEP)

Si el acto o conducta fuera constitutivo de delito público, todo testigo del mismo está obligado a ponerlo en conocimiento de la Justicia, del mismo modo que si se tratara de otros delitos, incluidos los leves, se cometan en el ámbito de la violencia de género.

"LA PUESTA EN MARCHA DE PROCEDIMIENTOS SANCIONADORES FRENTE AL ACOSADOR NO REQUIERE DEL CONSENTIMIENTO DE LA PERSONA ACOSADA. LA BASE DE LICITUD EN ESTE CASO SERÍA EL CUMPLIMIENTO DE UNA OBLIGACIÓN LEGAL".

"FINALIZADO EL PROCEDIMIENTO SANCIONADOR, LOS DATOS DEBEN PERMANECER BLOQUEADOS DURANTE EL PERÍODO DE PRESCRIPCIÓN DE LA SANCIÓN, O EN TANTO PUEDAN SER UTILIZADOS EN UN PROCEDIMIENTO JUDICIAL".

Se debe garantizar la confidencialidad de la información tratada y la identidad de la víctima solamente será revelada ante personas con interés en el procedimiento, no siendo en ningún caso admisible una publicidad masiva o indiscriminada sin consentimiento de la víctima, ni tampoco el acceso a los datos de personas no legitimadas. Para garantizar la confidencialidad resulta conveniente asignar un código identificativo tanto de la persona supuestamente acosada como la supuestamente acosadora, en aras de preservar la identidad de estas.

Una vez finalizado el procedimiento sancionador, los datos deben permanecer bloqueados durante el período de prescripción de la sanción, o en tanto puedan ser utilizados en un procedimiento judicial.

El bloqueo de los datos, tal y como establece el artículo 32.2 LOPDGDD, consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, salvo para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Una vez finalizado el plazo de prescripción se deberá proceder a la destrucción de los datos.

MATERIAL COMPLEMENTARIO

- Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Consulta este enlace.
- Dictamen 2/2017, sobre el tratamiento de datos en el trabajo (GT29). Consulta este enlace.
- Guía: "Protección de datos en las relaciones laborales" (AEPD). Consulta este enlace.
- Recomendaciones de la AEPD sobre la Protección de Datos como garantía en las políticas de prevención del acoso. Consulta este enlace.
- Guía: "Protección de datos y prevención de delitos". Consulta este enlace.

NOTICIAS

- **La AEPD impone una sanción de apercibimiento a un Ayuntamiento por haber infrinjido el deber de informar a sus empleados respecto al tratamiento de la huella dactilar.** La AEPD recuerda que la implantación de un sistema de control horario basado en la huella por parte del empleador debe ser informado a los empleados de manera clara, completa, conceisa y, además, haciendo referencia a las bases legales e información requerida por el artículo 13 RGPD. Asímismo, la AEPD determina qe la huella dactilar debe ser clasificada como dato biométrico. Consulta la resolución en este enlace.

- **La AEPD resuelve una consulta relativa al análisis de la cualidad de los dtos de víctima de violencia de género como merecedores de especial protección, para dispensarles o no, la protección que se establece en el artículo 9 RGPD.** La AEPD concluye que no estamos ante datos personales ordinarios, no debe obviarse que son datos sensibles que requieren mayor protección. Si bien la AEPD considera que las categorías especiales de datos deben considerarse como "numerus clausus", se deben tratar de acuerdo con la eficacia y alcance de un derecho fundamental en relación con la especial consideración que el legislador y, en su caso, los poderes públicos, otorgan al colectivo de víctimas de violencia de género. Consulta en este enlace.

- **La AEPD resuelve una consulta remitida por la Asociación Española de Compliance (ASCOM) relativa al período de conservación de los datos personales recabados a través de los canales de denuncias internos.** La AEPD hace mención al artículo 24 LOPDGDD que establece el plazo de 3 meses desde la introducción de los datos en el sistema de denuncias. Además, puntualiza que en el caso de que la denuncia pueda considerarse fundada y dé lugar a una concreta invetigación, no implica que deban suprimirse de los sistemas de la entidad, sino que únicamente procederá su supresión del concreto sistema de información de denuncias internas, pasando a integrarse en los sistemas propios del órgano de cumplimiento o, en su caso, del que tenga a su cargo la gestión de personal. Consulta en este enlace.