MOORE

LEGAL Y COMPLIANCE

GUÍAS PUBLICADAS DE LA AEPD

Este trimestre la AEPD ha publicado 2 guías:

- Guía publicada el 18 de mayo de 2021: Guía de Protección de datos y relaciones laborales (https://www.aepd.es/es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf)
- Guía publicada el 29 de junio de 2021: Guía de Gestión del riesgo y evaluación de impacto en tratamientos de datos personales (https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf)

Guía sobre Protección de datos y relaciones laborales

Esta guía ha sido elaborada por la Agencia con la participación tanto del Ministerio del Trabajo y Economía Social como de la patronal y organizaciones sindicales. La aplicación del Reglamento General de Protección y la Ley Orgánica de Protección de Datos y garantía de los derechos digitales (LOPDGDD) ha supuesto una serie de **cambios** tanto en lo relativo a los derechos de las personas trabajadoras como en la recogida y el uso de sus datos por parte de los empresarios.

Asimismo, la guía también aborda temas que se plantean cada vez con mayor frecuencia, como la consulta por parte del empleador de las **redes sociales** de la persona trabajadora, los sistemas internos de denuncias (**whistleblowing**), el **registro de la jornada laboral**, la protección de los datos de las **víctimas de acoso** en el trabajo o de las **mujeres supervivientes a la violencia de género** o el uso de la **tecnología wearable** como elemento de control. Mediante su guía no vinculante la AEPD pretende dar una serie de orientaciones a los responsables del tratamiento de datos personales y a las personas o entidades encargadas de este.

Trasladamos a continuación los principales aspectos:

- **Selección de personal:** Utilizando como base jurídica el art. 6.1.b) del RGPD, la Agencia indica una serie de **cautelas** en el tratamiento de datos personales durante la fase previa a la contratación, es decir, en el proceso de selección:
  - ✓ Principios de minimización y limitación de la finalidad.
  - ✓ Modelo tipo para el currículo.
  - ✓ Anuncio o convocatoria pública del puesto ofertado.
  - ✓ El deber de información y conservación mientras persista el tratamiento de los datos del afectado. Una vez concluido el proceso de selección, si la persona candidata no es contratada, desaparece la base jurídica para el tratamiento de datos, por lo que sería necesario su consentimiento para un futuro tratamiento.
  - ✓ La empresa es responsable de la custodia de la documentación entregada por la persona candidata.

- **Selección de personal y redes sociales: L**as personas no están obligadas a permitir que el empleador indague en sus perfiles de redes sociales, ni durante el proceso de selección ni durante la ejecución del contrato.

Aunque el perfil en las redes sociales de una persona candidata a un empleo sea de acceso público, el empleador no puede efectuar un tratamiento de los datos obtenidos por esa vía si no cuenta para ello con una base jurídica válida y para ello será necesario informar de ello a la persona trabajadora y demostrar que dicho tratamiento es necesario y pertinente para desempeñar el trabajo.

Por otro lado, la Agencia aclara que la empresa no está legitimada para solicitar 'amistad' a las personas candidatas para que éstas proporcionen acceso a los contenidos de sus perfiles.

- **Sistemas internos de denuncias o whistleblowing:** la Agencia considera que la información tanto a los denunciantes como a los potenciales denunciados reviste un carácter primordial. La LOPDGDD admite sistemas de denuncias anónimas y, en caso de que la denuncia no sea anónima, la confidencialidad de la información del denunciante debe quedar a salvo y no debe facilitarse su identificación al denunciado. Además, el personal con funciones de gestión y control de recursos humanos sólo podrá acceder a dichos datos en caso de procedimientos disciplinarios, sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo

- **Registro de jornada obligatorio y Geolocalización:** para el registro de jornada, la Agencia recomienda que se adopte el sistema menos invasivo posible y este no puede ser de acceso público ni estar situado en un lugar visible. Asimismo, los datos de ese registro no pueden utilizarse para finalidades distintas al control de la jornada de trabajo, como comprobar la ubicación. Por ejemplo, en el caso de una persona trabajadora itinerante cuyo registro de jornada se realiza por geolocalización, el registro no puede ser utilizado para verificar dónde se encuentra en cada momento si no que únicamente debe utilizar para comprobar el tiempo de trabajo.

- **Protección de la privacidad de las víctimas de acoso en el trabajo y de las mujeres supervivientes a la violencia de género:** La AEPD determina que sus datos personales y en particular su identidad, tienen, con carácter general, la consideración de **categorías especiales de datos personales** y, en todo caso, son datos sensibles que exigen una **protección reforzada**. Así, recoge que deberá asignarse un código identificativo tanto a la persona supuestamente acosada como a la acosadora, con objeto de preservar la identidad de estas. Además, el empleador podrá conocer y tratar los datos de una trabajadora vinculados a la condición de mujer superviviente a la violencia de género cuando resulte necesario para el cumplimiento de las obligaciones legales pero, en todo caso, la documentación de la empresa debe incluir un código que no permita que terceros puedan asociar esa información con la trabajadora.

- **Tecnología wearable.** La AEPD indica que 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 reglamentariamente, dado que no se enmarca en la vigilancia de la salud propia de la prevención de riesgos laborales, supone el tratamiento de una categoría especial de datos (salud) sin una base jurídica, no cuenta con una finalidad legítima y vulnera el principio de proporcionalidad, dado que conlleva una monitorización permanente y permitiría al empleador acceder a datos de salud específicos, y no exclusivamente a la valoración sobre la aptitud para desempeñar el trabajo.

Guía de Gestión del riesgo y evaluación de impacto en tratamientos de datos personales

El documento, dirigido a responsables, encargados de tratamientos y delegados de protección de datos (DPD), ofrece una **visión unificada de la gestión de riesgos y de las evaluaciones de impacto en protección de datos**, y facilita la integración de la gestión de riesgos en los procesos de gestión y gobernanza de las entidades.

El RGPD establece que las organizaciones que tratan datos personales deben realizar una gestión del riesgo con el fin de establecer las medidas que sean necesarias para garantizar los derechos y libertades de las personas. Además, para los casos en los que los tratamientos impliquen un **riesgo alto** para la protección de datos, el Reglamento **dispone que esas organizaciones están obligadas a realizar una Evaluación de Impacto en Protección de Datos (EIPD) para mitigar esos riesgos**.

Para los casos de alto riesgo la Guía incorpora las orientaciones necesarias para realizar la EIPD y, en su caso, la consulta previa a la que se refiere el artículo 36 del RGPD, que establece que el responsable debe consultar a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto sigue ofreciendo un riesgo residual alto o muy alto tras haber tomado medidas. No obstante, la guía es aplicable a cualquier tratamiento con independencia de su nivel de riesgo.