

Teletrabajo y protección de datos en el ámbito digital

Si tu organización ha mantenido el teletrabajo, te damos algunas claves que debes tener en cuenta para proteger adecuadamente los datos personales tanto de las personas trabajadoras que realizan teletrabajo como de tus clientes y/o proveedores.



La situación excepcional derivada de la pandemia de la COVID-19 hace ya más de un año puso sobre la mesa de toda clase de organizaciones la urgente necesidad de un cambio no programado en los modelos de negocio tradicionales. Una de las más importantes fue la puesta en marcha de políticas del teletrabajo. En cuestión de pocas semanas fue necesario tomar decisiones a corto plazo y hacer uso intensivo de accesos remotos, plataformas online y virtualizando las relaciones laborales. Lo que se presuponía temporal se ha quedado, cuanto menos de forma parcial, en buena parte de las entidades, dando paso a un nuevo modelo económico que forma parte de la digitalización.

Al inicio de periodo de confinamiento en 2020, la AEPD facilitó una serie de recomendaciones dirigidas a los responsables del tratamiento para que adaptaran los tratamientos en régimen de teletrabajo al cumplimiento del Reglamento General de Protección de Datos (RGPD). Distintos organismos como el CCN o el INCIBE comenzaron a dar pautas y consejos para fomentar un entorno de trabajo ciberseguro. Por su parte, el Gobierno aprobó el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia que, tras ser convalidado por el Congreso de los Diputados, acaba de incorporarse a nuestro ordenamiento jurídico como Ley 10/2021, de 9 de julio, de trabajo a distancia, con cambios mínimos respecto a su redacción original.

Sin embargo, ante una nueva dimensión de la forma de trabajar, las soluciones que se adoptaron en su momento con urgencia y a corto plazo, deben ser revisadas. Para alcanzar una resiliencia económica y operativa se requiere una estrategia, una planificación y un cambio cultural dentro de la organización que garantice su sostenibilidad en el tiempo.

Teletrabajo y protección de datos en el ámbito digital

Esto exige la implementación de un enfoque estructurado y coherente para mejorar la capacidad del responsable para identificar, de forma proactiva, los riesgos de sus procesos, evaluarlos y gestionarlos.

Desde el ámbito de las competencias de la AEPD, esta gestión hay que aplicarla desde la perspectiva de la protección de datos, lo que se ajusta perfectamente al modelo de cumplimiento del RGPD.

En el contexto del teletrabajo **los sujetos de los datos cuyos derechos y libertades deben estar garantizados son tanto los propios empleados de la organización como las personas físicas con las que esta se relaciona** y de las que se tratan datos personales en el contexto de su actividad de negocio. En ese sentido, es necesario garantizar la conformidad con el RGPD en ambas dimensiones, atendiendo a las circunstancias particulares que determina cada uno de ellos.

En el caso del tratamiento de datos de las personas trabajadoras que realizan teletrabajo, cuando este suponga un tratamiento adicional de datos con respecto al que venía realizándose en el ámbito presencial, se ha de respetar el principio de licitud, por lo que, para los distintos tratamientos que se realicen con causa de esta modalidad de trabajo a distancia, habrá de considerarse:

- **La voluntariedad del trabajo a distancia (artículo 5 de la [Ley 10/2021, de 9 de julio, de trabajo a distancia](#)).**
- **La no aplicabilidad del consentimiento como base jurídica recurriendo, según el tratamiento específico, a otras más adecuadas:**
 - **Tratamiento legitimado por la existencia de una relación contractual** (artículo 6.1.b) con relación al art. 20.3 del [Estatuto de los Trabajadores](#), que establece la facultad del empresario para ejercer el poder de dirección y control, siempre con observancia del principio de proporcionalidad.
 - **Satisfacción del interés legítimo del empleador, siempre que frente a este no prevalezcan los intereses o los derechos y libertades fundamentales del trabajador** (artículo 6.1.f), cuestión que ha de evaluarse a través de una “prueba de ponderación o contrapeso” que no debe confundirse con una EIPD.
 - **El cumplimiento de obligaciones legales** (artículo 6.1.c), **como es el caso de la obligación del empleador de establecer un registro de jornada**, establecida en el artículo 34.9 del Estatuto de los Trabajadores. Este se impone con una finalidad específica, favorable al

Teletrabajo y protección de datos en el ámbito digital

trabajador, tal y como se reitera en diversos apartados del Preámbulo del **RD-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo**. Debe valorarse si el registro va a usarse al único efecto de lo previsto en el artículo 34.9 del ET o si también se va a usar como medida de control por el empresario, atendiendo a las circunstancias concretas en que vaya a desarrollarse el trabajo a distancia. En ese caso, será necesario informar al trabajador de la doble finalidad.

- **El levantamiento de la prohibición del tratamiento de categorías especiales de datos.** Por ejemplo, los datos biométricos dirigidos a la identificación unívoca del trabajador solo podría quedar amparado bajo el artículo 9.2.b del RGPD cuando sea 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, en la medida en que así lo autorice el Derecho o un convenio colectivo con arreglo a Derecho que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.
- **El respeto de los derechos relacionados con el uso de dispositivos en el ámbito laboral** como son, entre otros, el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral y el derecho a la desconexión digital.

En cuanto a los tratamientos ya en curso y que son el objeto de la actividad de negocio propia del responsable, no se requiere la existencia de una base jurídica diferente de la que ya lo legitimaba cuando venía desarrollándose de manera presencial, no suponiendo los medios empleados una modificación de la legitimación de los mismos.

No obstante, no debe perderse de vista que la existencia de una base de legitimación no exime del cumplimiento del resto de principios de tratamiento recogidos en el artículo 5 del RGPD que se desarrollan a lo largo de todo el articulado de la norma, debiendo tenerse en cuenta que la modificación de los medios habilitados para el acceso y el tratamiento de los datos con causa de la situación de teletrabajo sí que puede generar la necesidad de introducir mayores garantías en la aplicación de dichos principios.

El Reglamento establece un modelo de cumplimiento basado en el concepto de tratamiento de datos con un enfoque dirigido a tratamientos, un enfoque dirigido a la **gestión del riesgo** que para

Teletrabajo y protección de datos en el ámbito digital

los derechos y libertades de los individuos representa el tratamiento de los datos, y en la implementación de modelos de gestión y gobernanza (políticas de protección de datos) orientadas a garantizar y demostrar la adecuación de los tratamientos en función de su naturaleza, ámbitos, contexto, fines y los riesgos para los derechos y libertades de los interesados.

Por lo tanto, cuando se plantea la implementación de procesos en la entidad en régimen de teletrabajo, hay que ir más allá de la simple elección y puesta en marcha de una herramienta o solución tecnológica. Hay que tomar decisiones para gestionar el cambio en la naturaleza del tratamiento y la forma en la que se implementa, reevaluar los nuevos riesgos introducidos y tratarlos adecuadamente para minimizar su posible impacto, pues ya [el Dictamen 2/2017 del Grupo de Trabajo del Artículo 29 respecto al tratamiento de datos en el ámbito laboral](#) advertía de que el trabajo a distancia suponía un riesgo adicional para los derechos y libertades, tanto de los trabajadores como de los sujetos de los datos que estos trataban.

Para la **gestión del riesgo** para los derechos y libertades la AEPD ha publicado guías, ayudas y herramientas dirigidas a apoyar a los responsables en esta tarea, sin que ello suponga que dicho material de soporte pueda sustituir a las obligaciones del responsable, sus decisiones y actuaciones. No cabe aplicar automatismos, limitarse a *checklists* o plantillas predefinidas, ni trasladar los resultados obtenidos sin que haya una valoración crítica y adecuación al caso concreto y particular del responsable. Por tanto, se hace necesario:

- **Implementar políticas de protección de datos, en particular, para la aplicación de los principios y derechos de protección de datos.**
- **Aplicar una gestión de riesgos para los derechos y libertades.**
- **Aplicar los principios de protección de datos desde el diseño, identificando los nuevos requisitos y rediseñando los procesos de teletrabajo, aplicándolo a las herramientas empleadas, aumentando la transparencia y el control sobre los datos, etc.**
- **Aplicar los principios de protección de datos por defecto, configurando correctamente las aplicaciones para minimizar los datos personales tratados.**
- **Implementar medidas de seguridad efectivas, orientadas a proteger los derechos y libertades.**
- **Y, por último, implementar políticas de gestión de brechas de datos personales, con el propósito de ser, de nuevo, más resilientes y efectivos.**

Teletrabajo y protección de datos en el ámbito digital

En estos meses de trabajo a distancia se han visto señales de problemas de sostenibilidad en algunas implementaciones de la digitalización que han de ser urgentemente revisadas si queremos avanzar hacia una digitalización resiliente y sostenible en la que los derechos y libertades de los ciudadanos queden garantizados.

Puede ampliar información sobre protección de datos y privacidad en el teletrabajo en el sitio web [Innovación y Tecnología](#) de la Agencia española de protección de datos, así como en sus blog:

- [Brechas de seguridad: Ransomware y gestión del riesgo](#)
- [Brechas de seguridad: el correo electrónico y las plataformas de productividad online](#)
- [Privacidad de grupo](#)
- [Gobernanza y política de protección de datos](#)
- [Protección de datos y seguridad](#)
- [La protección de datos en las relaciones laborales](#)

Publicado el 19 DE JULIO DE 2021 por la AEPD.
