Nota Informativa

Sobre las recomendaciones y medidas a adoptar para proteger los datos personales en las situaciones de movilidad y el teletrabajo en el contexto del COVID-19

13 de abril de 2020

Recomendaciones de la AEPD para proteger los datos personales en situaciones de movilidad y teletrabajo

En línea con nuestra nota informativa de 19 de marzo sobre las recomendaciones de seguridad para el teletrabajo realizadas por el Centro Criptológico Nacional y por la Agencia Europea de Ciberseguridad, consideramos acertado resumir las recomendaciones de seguridad que ha emitido la Agencia Española de Protección de Datos ("**AEPD**") en su nota técnica "Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo". Las recomendaciones incluyen las medidas que han de adoptar los responsables de tratamiento y sus empleados o colaboradores para el tratamiento de datos personales.

En primer lugar, la AEPD señala que es indispensable disponer de una planificación previa para el teletrabajo. Sin embargo, en situaciones de emergencia como la actual, es posible la adopción de medidas provisionales, sin perjuicio de que, cuando la situación de emergencia se alargue sea necesario realizar una adecuación de la implementación de medidas para el teletrabajo de los empleados.

En este sentido, la AEPD propone un bloque de seis recomendaciones destinadas a los responsables de tratamiento, que deben adaptarse a la actividad económica que desarrollan, siendo las siguientes:

- Definir una política específica de protección de la información para las situaciones de trabajo en remoto, la cual disponga de las necesidades y riesgos particulares en aquellos casos en los que se accede a información corporativa desde espacios que no estén bajo el control de la empresa.

- Utilizar soluciones informáticas de teletrabajo que ofrezcan garantías suficientes.

- Limitar el acceso a la información, creando niveles de acceso en función de las tareas que realicen los empleados de la organización, así como restringir la entrada desde determinados dispositivos o en función de la ubicación desde la que se accede.

- Revisar de forma periódica los equipos, servidores y demás dispositivos utilizados para el trabajo en remoto, instalando las actualizaciones pertinentes para que estén adaptados a la política de teletrabajo de la empresa. En el caso de que los empleados utilicen sus dispositivos

particulares, puede ser necesario restringir su acceso únicamente a la información que sea considerada como menos crítica.

- Seguimiento de los accesos realizados a la red corporativa desde el exterior, identificando aquellos comportamientos anormales con el objetivo de evitar la propagación de *malware* y el uso y acceso no autorizados. En todo caso, esta facultad de monitorización tiene que ser puesta en conocimiento de los empleados con carácter previo a su implementación, sobre todo, si la misma es usada para verificar el cumplimiento de sus obligaciones laborales.

- Las brechas de seguridad tienen que ser puestas en conocimiento de la AEPD y de los interesados, en su caso.

- Las medidas adoptadas en las políticas de privacidad y seguridad tienen que emanar del análisis de riesgos realizado con carácter previo, el cual ha de ponderar la proporcionalidad entre los beneficios obtenidos por el trabajo en remoto y el impacto que éste puede tener.

- La política de teletrabajo tiene que prever los procedimientos internos para la correcta provisión y auditoría de los dispositivos utilizados para el trabajo en remoto.

Asimismo, la AEPD propone una serie de medidas dirigidas a los empleados o colaboradores del responsable de tratamiento, que en el desempeño de sus funciones traten datos personales. Así, la AEPD insta a que estas recomendaciones se incluyan en las políticas internas del responsable de tratamiento, haciendo especial referencia a los siguientes aspectos:

- Los empleados tienen que respetar la política de protección de datos implementada por la organización para el trabajo en remoto. Así, corresponde al responsable del tratamiento facilitar las guías y recomendaciones que deben cumplir.

- Proteger de forma adecuada los dispositivos y cuentas utilizadas para la prestación de los servicios en remoto. En este caso, es recomendable establecer contraseñas robustas y diferentes para cada cuenta, así como tener claves de acceso distintas para las cuentas personales y profesionales.

- Los empleados tienen que tomar todas las precauciones pertinentes para garantizar la protección de la información que estén tratando, salvaguardando en todo caso, la confidencialidad. Por ello, es recomendable evitar el uso de papel y tener precaución a la hora de destruirlo, así como también cerrar la sesión cuando se deje desatendido el equipo para evitar la intrusión por parte de terceros.

- Guardar toda la información generada en la nube corporativa que disponga la organización, evitando guardarla de forma local en los propios dispositivos.

- Comunicar de forma inmediata cualquier tipo de anomalía o brecha de seguridad al responsable de tratamiento o al Delegado de Protección de Datos que pueda afectar la información y los datos de carácter personal tratados

En definitiva, la AEPD establece unas recomendaciones generales que tienen por objetivo garantizar la seguridad de la información y de los datos de carácter personal tratados en el contexto del teletrabajo. Habida cuenta de la situación provocada por el COVID-19, que ha obligado a numerosas empresas a tener que adoptar dicha modalidad de trabajo para garantizar su continuidad económica y adaptarse a un modelo de trabajo que no tenían previamente establecido ni previsto, resulta adecuado aprovechar esta oportunidad para rediseñar y completar las políticas internas de seguridad y tratamiento de la información que incluya la digitalización de las funciones laborales.

Esperamos que la información sea útil y de su interés. Desde Andersen Tax & Legal hemos creado un equipo multidisciplinar para atender todas las cuestiones que puedan surgir sobre este aspecto o en relación con el COVID-19.

Puede descargar las recomendaciones de la Agencia Española de Protección de Datos desde aquí.

Para más información, puede contactar con:

Isabel Martínez | Director en el área de Privacy, IT & Digital Business
isabel.martinez@andersentaxlegal.es