SENSIBILIZACIÓN DEL PERSONAL

NORMATIVA VIGENTE EN MATERIA DE PROTECCIÓN DE DATOS · LOPDGDD Y RGPD (UE) 2016/679

Los empleados son el motor de cualquier compañía, los que hacen posible su funcionamiento. Si los trabajadores no están concienciados sobre sus responsabilidades en materia de protección de datos, es muy probable que se produzcan fallos que pueden poner en peligro a la empresa. Es necesario que los empleados estén formados e informados, así como que conozcan sus obligaciones y sus derechos.

PRINCIPIO RESPONSABILIDAD ACTIVA

También conocido como "accountability". No hay suficiente con cumplir la normativa, sino que se debe poder demostrar.

01

OBLIGACIONES Y DERECHOS DE LOS EMPLEADOS

Los empleados deben conocer sus obligaciones y derechos en materia de Protección de Datos.

02

COMUNICADO INTERNO Y COMPROMISO DE CONFIDENCIALIDAD

Estos documentos establecen las obligaciones en seguridad y las directrices a seguir por el personal.

03

PLANES DE FORMACIÓN CONTINUA

Los trabajadores deben estar formados e informados. La formación debe actualizarse periódicamente.

04

LIMITACIÓN ACCESOS USUARIOS Y CONTROL

La empresa debe garantizar la limitación y el control de acceso a los datos personales tratados.

05

EMPLEADOS, PIEZA PRINCIPAL DE LA ENTIDAD

El personal debe ser consciente sobre sus responsabilidades para evitar fallos que pongan en peligro a la compañía.

06

EVITAR POSIBLES SANCIONES

El RGPD incrementó la cuantía de las sanciones, representando un impacto brutal en la economía de cualquier empresa.

07

01 CUMPLIMIENTO DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA "ACCOUNTABILITY"

Una de las principales novedades que introdujo el Reglamento General de Protección de Datos (RGPD) fue el principio de responsabilidad activa (accountability). Este principio insta a que el Responsable del Tratamiento de datos aplique medidas técnicas y organizativas para poder garantizar y demostrar a terceros que el tratamiento de datos personales se hace conforme al Reglamento.

Es decir, no hay suficiente con cumplir con la normativa, sino que también hay que demostrarlo. Para hacerlo, las empresas deben tomar una serie de medidas, tales como:

- Nombrar un Delegado de Protección de Datos.
- Aplicar las medidas de protección de datos desde el diseño, y por defecto.
- Tener un registro de las actividades de tratamiento.
- Efectuar un análisis de riesgo.
- Realizar una evaluación de impacto.
- Notificar brechas de seguridad a la autoridad competente (AEPD).

Estas medidas deberán ser revisadas y actualizadas en todo momento por el Responsable del Tratamiento.

02 INFORMACIÓN SOBRE LAS OBLIGACIONES Y DERECHOS DE LOS EMPLEADOS

La protección de datos afecta a los empleados de una doble forma: con obligaciones y con derechos. Todos los trabajadores deben ser conscientes y estar informados de ambas cuestiones.

OBLIGACIONES

En referencia a las obligaciones, estas repercuten a aquellos empleados que durante el desempeño de su trabajo procesan datos personales. En este sentido, solamente pueden gestionar datos personales de acuerdo con las responsabilidades que le han sido definidas, haciéndolo de la forma fijada por la empresa y de acuerdo con lo establecido en el RGPD. Además, estos empleados deberían recibir formación específica en esta materia.

DERECHOS

En cuanto a los derechos, los empleados pueden saber cómo se procesan sus datos personales: qué información tiene la compañía sobre ellos, para qué la utiliza (fines), dónde se almacena, quién accede a estos datos, la cesión de datos que se hace a empresas colaboradoras (mantenimiento informático, gestorías, etc.). En cualquier momento, los trabajadores pueden solicitar el acceso a esta información. Asimismo, la empresa debe notificarles cualquier cambio que afecte al tratamiento de sus datos personales e informarles de cómo se pueden ejercer los derechos de acceso, rectificación, cancelación, oposición, portabilidad o derecho al olvido.

Se debe tener en cuenta que estos derechos son vigentes en las tres fases de cualquier relación laboral entre un empleado y una compañía: antes (currículums), durante y después (extrabajadores).

En relación a los derechos, también deben tenerse en cuenta otras cuestiones:

VIDEOVIGILANCIA

La empresa está obligada a informar a los empleados de forma expresa y concisa de la instalación de cámaras de videovigilancia en el lugar de trabajo. El tratamiento de las imágenes deberá estar siempre dentro del marco legal, de manera que debe existir una relación de proporcionalidad entre la finalidad perseguida y el modo en el que se tratan las imágenes. Además, la LOPDGDD introduce expresamente la prohibición de instalar cámaras en zonas de ocio y descanso de los trabajadores.

GEOLOCALIZACIÓN

El control por geolocalización debe realizarse por una necesidad legítima, por ejemplo, para coordinar el transporte y distribución de mercancías. En el caso de que la compañía instale GPS en los vehículos de empresa para conocer la ubicación de sus empleados durante la jornada laboral, se deberá informar previamente a los trabajadores de que se controlarán sus desplazamientos, indicando la finalidad del control y el sistema utilizado. No será necesario pedir el consentimiento

DESCONEXIÓN DIGITAL

La LOPDGDD también introduce el concepto de desconexión digital, estableciendo que los empleados tienen derecho a desconectar de cualquier dispositivo digital durante sus periodos de descanso del trabajo o de vacaciones. La finalidad es garantizar la intimidad de los trabajadores y mejorar la conciliación personal y familiar.

03 COMUNICADO INTERNO Y COMPROMISO DE CONFIDENCIALIDAD

Los Responsables y Encargados del Tratamiento de datos, así como todas las personas que intervengan en cualquier fase de éste, están sujetos al deber de confidencialidad al que se refiere el artículo 5.1.f del RGPD. Para ello firmarán un Compromiso de Confidencialidad y un Comunicado Interno en el que se establecen las directrices a seguir por el personal para el tratamiento de los datos durante el desarrollo de sus tareas dentro de la empresa.

En estos documentos se recogen las principales obligaciones en materia de seguridad sobre datos de carácter personal, incluyendo la prohibición expresa de instalar cualquier tipo de aplicación en los equipos informáticos y la utilización de los recursos informáticos y no informáticos para otras finalidades diferentes de las estrictamente derivadas del desarrollo de su actividad laboral. Asimismo, también se compromete a mantener el deber de confidencialidad sobre todos los datos tratados y de no comunicar esta información a ninguna persona o entidad sin la autorización pertinente, excepto en aquellos casos en los que sea necesario para dar el debido cumplimiento a sus obligaciones o por habérsele requerido por mandato legal o de la autoridad competente.

Aquellos empleados que no respecten o no cumplan con el tratamiento de datos personales tal y como se recoge en el Comunicado Interno y en el Compromiso de Confidencialidad, se enfrentan a un proceso disciplinario formal. Además, la sustracción o revelación de información propiedad de la compañía puede ser una acción constitutiva de ilícito penal de acuerdo con el artículo 197 del Código Penal.

04 PLANES DE FORMACIÓN CONTINUA

La ley obliga explícitamente a que los empleados de cualquier compañía estén formados e informados en materia de protección de datos personales. Además, estos conocimientos deberán actualizarse de forma periódica, incorporando todos aquellos nuevos procedimientos y posibles nuevos requerimientos.

Con una buena formación, los trabajadores sabrán proteger la información de tipo confidencial, así como comprenderán y se concienciarán sobre sus obligaciones en el tratamiento de los datos personales. Sin embargo, no todos los empleados necesitan tener el mismo conocimiento sobre la normativa y debería adaptarse la formación a las tareas que desempeña cada uno. Es de especial importancia que estén formados aquellos empleados que trabajen en atención al cliente, análisis de datos, recursos humanos, informática y telecomunicaciones o equipos jurídicos, entre otros.

FORMACIÓN CURSOS CONVERSIA

En Conversia ofrecemos el curso de Privacidad y gestión de la información, especialmente indicado para aquellos empleados que, por su labor, gestionan datos de carácter personal en cualquiera de los roles que ocupen actualmente o en un futuro.

Al finalizar el curso, el alumno habrá adquirido los conocimientos suficientes en relación al uso de datos personales, para gestionar con eficacia un amplio abanico de situaciones posibles que afectan al desarrollo de sus tareas en la empresa. Su capacitación y concienciación le permitirán actuar de manera adecuada conforme a los requerimientos legales en esta materia (RGPD y LOPDGDD).

FORMACIÓN IN COMPANY

En Conversia diseñamos acciones formativas personalizadas destinadas al personal de la entidad, para tratar los puntos esenciales de la normativa de Protección de Datos y orientada a las distintas áreas y aspectos que los consultores de Conversia consideran críticos. Estas formaciones se pueden impartir en formato presencial o semipresencial, adaptándonos siempre a las necesidades de cada empresa.

05 LIMITACIÓN ACCESOS "USUARIOS" Y CONTROL

La compañía debe garantizar en todo momento que los datos de carácter personal almacenados cumplen con los tres pilares fundamentales de la seguridad de la información: integridad, disponibilidad y confidencialidad. Para ello debe garantizar la limitación y el control de acceso a los datos personales que trata. Asimismo, los empleados deben velar para cumplir con este objetivo. Para hacerlo, se deben tener en cuenta:

- La información sensible o crítica, tanto en papel como en medios informáticos extraíbles, debe mantenerse almacenada en ubicaciones con un sistema de control de acceso, al que solamente tendrá acceso el personal autorizado.

- En cuanto a almacenamiento físico, la empresa debe instalar mecanismos de control de acceso para el personal autorizado en las áreas que contienen datos de carácter personal, así como en aquellas zonas en que estén los recursos que los tratan. Cuando se requieran servicios de mantenimiento de terceros dentro de las instalaciones, se proporcionará al personal externo el acceso a las áreas requeridas con la misma supervisión y control que el personal interno. Además, deberá llevarse un registro.

- En cuanto a equipos informáticos, cada usuario deberá contar con un identificador único y una contraseña. El Responsable de Privacidad es el encargado de dar de alta los identificadores de los usuarios y permitirles o no el acceso al tratamiento de datos personales en función de la actividad que desempeñen. Cuando un usuario deje la organización (temporalmente o indefinidamente) se deberá inhabilitar o eliminar el ID. Además, la compañía deberá mantener un registro general de todos los derechos de acceso a sistemas de información y servicios concedidos a los identificadores.

- Los empleados deberán bloquear los equipos informáticos mediante contraseña cuando no los estén utilizando, con el fin de impedir la visualización de datos protegidos.

- Sacar los dispositivos fuera de los emplazamientos de trabajo puede conllevar riesgos para la información confidencial y los datos personales. Sin embargo, existen determinadas situaciones en las que es necesario hacerlo para realizar labores propias del trabajo desempeñado. En estos casos, el empleado debe contar con la previa autorización por parte de la dirección, que se encargará de proteger esta información. En caso de pérdida o robo de un dispositivo, se deberá notificar inmediatamente como una incidencia de seguridad.

- La empresa debe encargarse de mantener los equipos actualizados para evitar la entrada de software malicioso, así como realizar copias de seguridad de la información para poderla recuperar si esta se viera comprometida.

06 EMPLEADOS, PIEZA PRINCIPAL DENTRO DE LA ENTIDAD PARA EL TRATAMIENTO DE DATOS PERSONALES

Sin duda, los empleados son el motor de cualquier compañía, los que hacen posible su funcionamiento. Si los trabajadores no están concienciados sobre sus responsabilidades en materia de protección de datos, es muy probable que se produzcan fallos que pueden poner en peligro a la empresa. Por este motivo, desde la dirección deberá asegurarse de que el personal conoce los procedimientos de seguridad implementados para proteger los datos personales que tiene la compañía, ya sean de clientes, proveedores, socios, de los propios empleados, etc.

Se debe tener en cuenta que son los empleados los que trabajan directamente con los datos y que muchas de las vulneraciones y consiguientes sanciones se producen por el desconocimiento de las obligaciones legales por parte de los trabajadores. El Responsable del Tratamiento debe velar por implantar estas buenas prácticas en materia de protección de datos

Cualquier organización debe fijar una serie de medidas básicas para proteger la privacidad y los datos personales, medidas que los trabajadores deben tener totalmente interiorizadas: procedimientos para el uso de dispositivos portátiles fuera de la oficina, memorias USB encriptadas con documentación que contenga datos personales, reutilización de papel que haya sido impreso con información privada, etc.

07 EVITAR POSIBLES SANCIONES

La plena aplicación del Reglamento General de Protección de Datos supuso un incremento de la cuantía de las sanciones, pudiendo llegar hasta los 20 millones de euros o el 4% del volumen de negocio anual global del ejercicio financiero anterior. Estas cifras pueden representar un impacto brutal en la economía de cualquier compañía e, incluso, llevarla a desaparecer.

Todas las medidas mencionadas anteriormente llevarían a evitar cualquier tipo de brecha de seguridad y violación de la privacidad y la protección de datos personales. Sin embargo, en caso de que se acabara produciendo, los empleados también deben conocer los procedimientos a llevar a cabo: las brechas de seguridad deben notificarse a la Autoridad de Control dentro en las 72 horas posteriores de conocerse el incidente.

CONVERSIA

info@conversia.es | T. 902 877 192 | www.conversia.es