PROTOCOLO BÁSICO RESPONSABLE TRATAMIENTO

La normativa europea en protección de datos RGPD 679/2016 y su desarrollo en España, la LOPGDD 03/2018 trae consigo bastantes cambios que afectan al tratamiento de datos personales.

OBLIGACIONES Y FUNCIONES

Comunicación a todo el personal de sus obligaciones y funciones en relación a todas las operaciones de tratamiento de datos personales en que participen o en las que puedan participar.

Comunicación a todo el personal de los protocolos y responsables de actuación en caso de que un interesado ejerza algunos de los derechos de acceso, rectificación, supresión, limitación de tratamiento, portabilidad, oposición al tratamiento de sus datos o a la toma de decisiones individuales automatizadas o cualquier otro que le sea reconocido por la legislación vigente.

Diseño del procedimiento de realización de copias de seguridad y recuperación de datos.

Realización de controles periódicos de verificación del cumplimiento.

DOCUMENTOS

Documentos de confidencialidad y consentimiento de cesión de datos firmados por los trabajadores. Además de otros documentos como el de videovigilancia en caso de ser necesario.

Deber de informar a clientes, asociados o usuarios. Siempre que se haga una toma de datos utilizaremos este documento de información y consentimiento, o bien uno adaptado a cada actividad.

Deber de información a candidatos. Utilizar cuando se nos entregue un CV en mano. El candidato deberá firmarnos el consentimiento para poder hacer entrega del CV. Una vez hecho esto graparemos esta hoja de deber de información al CV para demostrar que se cumplen las medidas que pide la ley.

Encargos de Tratamiento firmados por Responsable y Encargado. Esos encargos corresponden a empresas externas con quien compartimos datos, como por ejemplo el asesor.

Para cumplir con las garantías que pide la ley se deberá exigir a nuestros Encargado de Tratamiento que también estén al día con la normativa vigente en Protección de Datos.

EMAILS Y FACTURAS

Ambos con coletilla RGPD adaptada al negocio o actividad.

Recomendamos uso correos corporativos, ya que ofrecen mayor seguridad.

PÁGINA WEB

Si se cuenta con página web estas son las premisas básicas que se deberán tener en cuenta:

Que esté adaptada a la LSSICE (garantía de seguridad dentro de las webs).

Actualizar Aviso legal y Política de Cookies y Privacidad.

Casillas de consentimiento y aceptación si la página cuenta con un formulario de contacto.

Se recomienda contar con Certificado SSL. Garantiza el encriptado en las comunicaciones, por lo que será importante contar con él en negocios de venta online.

VIDEOVIGILANCIA

Imprescindible cartelería adaptada RGPD en zonas videovigiladas.

Colocar un cartel por entrada, y siempre en lugar visible.

Nunca enfocar cámaras hacia zonas de tránsito público.

Los trabajadores deberán firmar una hoja de consentimiento específica donde se informa de la finalidad de las grabaciones. (seguridad, control laboral...)

PROCEDIMIENTOS

Lugar de trabajo ordenado: Usar carpetas o cajones opacos para mantener privacidad. Sobre todo si recibimos clientes o usuarios.

Almacenaje de datos físicos bajo llave: Sólo tendrán acceso el/los responsables, así como los trabajadores con permiso, debiendo permanecer cerrado siempre que no sea necesario su uso.

Evitar dejar a la vista documentación que contenga datos personales.

Pantallas con bloqueo: Para evitar que otra persona pueda acceder a nuestros datos si nos ausentamos.

Ordenadores con contraseña: Preferible utilizar un perfil para cada usuario que permita control de acceso a datos.

Cambiar contraseña correo cada 3 meses: Usar contraseña segura (símbolos, números, mayúsculas y al menos 8 caracteres).

Envío de correos: Si se envía un mismo correo a más de una persona, hacerlo siempre con copia oculta (cco).

Difusión datos personales: No difundir datos personales a través de RRSS, medios electrónicos, etc sin consentimiento previo.

Destrucción de papel: Se utilizará una destructora de papel para aquella documentación con datos personales que ya se necesite. Determinar plazos de destrucción de documentos.

COMUNICACIÓN ALTAS Y CAMBIOS

Informar a **DATA PROTECT PLUS** siempre que tenga algún cambio, como altas de trabajadores o empresas nuevas con las que comparten datos personales.

BRECHAS SEGURIDAD

En caso de brecha de seguridad o pérdida de datos personales tanto automatizados como físicos se deberá informar a la AEPD (Agencia Española Protección de Datos) en un plazo máximo de 72h.

Por lo que se ruega al responsable o gerente se ponga en contacto cuanto antes con **DATA PROTECT PLUS** para poder gestionar la incidencia.

965038463 info@dataprotectplus.com