REGISTRO DE TRATAMIENTOS EN PROTECCIÓN DE DATOS.

Introducción

Con la entrada en vigor del RGPD se establecen una serie de cambios, en relación a lo establecido por la Ley Orgánica de Protección de Datos, cambios a los que debemos adaptarnos, para dar cumplimiento a lo que el nuevo Reglamento exige. Dicho reglamento incorpora nuevas obligaciones y modifica algunas de las anteriores. Una de las principales novedades es el principio de responsabilidad proactiva (accountability). Dicha responsabilidad consiste en la necesidad de que el responsable de los datos y su tratamiento aplique medidas de seguridad técnicas y organizativas para que garantice el cumplimiento normativo y los derechos de los afectados.

Las organizaciones deben analizar los datos que tratan y con que finalidad los usan. Con dicho análisis deben implementar medidas de seguridad acorde a dichos tratamientos.

¿A QUIÉN AFECTA ?

A toda organización, empresa o autónomo que tenga, utilice o trate datos de carácter personal, ya sea en soporte informático o en suporte no automatizado (papel).

¿QUE ES LA PROTECCIÓN DE DATOS?:

La Protección de Datos es un Derecho Fundamental, que se desarrolla a partir del artículo 18.4 de la Constitución Española.

Este derecho hace referencia al poder de disposición y control sobre nuestros datos personales y la facultad para consentir que sean tratados por terceros.

¿QUÉ ES UN DATO PERSONAL?

Se define dato personal, como cualquier información que identifique, o haga identificable a una persona.

También existen los denominados datos especialmente protegidos, referidos a su ideología, religión, origen racial, vida sexual,comisión de infracciones penales y administrativas. Debemos incluir también la protección de datos de los menores de 14 años.

¿QUE DATOS PODEMOS SOLICITAR?

Sólo los datos necesarios y pertinentes para la finalidad que se les vaya a dar. Se exige también que los datos estén actualizados y que cuando dejen de ser necesarios para la finalidad para la que fueron recabados, se proceda a su cancelación. Debemos seguir en la empresa una política de transparencia, lealtad y licitud de los datos.

¿QUIEN ES EL RESPONSABLE DE ESOS DATOS?

El responsable de un fichero de datos,es la persona física o jurídica, pública o privada, entidad u órgano administrativo, que decide sobre el contenido, el uso y la finalidad del tratamiento de datos personales.

¿ QUIÉN ES EL ENCARGADO DE ESTOS DATOS?

El encargado del tratamiento es la persona física o jurídica, pública o privada, u órgano administrativo, que trate datos personales **por cuenta del responsable del tratamiento** o del responsable del fichero, y ello como consecuencia de la existencia de una relación jurídica, que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio (por ejemplo: el gestor administrativo que confecciona nóminas y gestiona el fichero de personal).

Con los encargados de los tratamientos de su empresa deberá firmar un contrato de tratamiento donde se definan de forma concreta los usos (**adjuntamos un modelo que puede utilizar con sus encargados en los anexos del presente documento. ANEXO III).** Debe tener un modelo firmado con cada empresa a la que cede datos para que le presten un servicio.

¿QUE ES LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS?

La Agencia Española de Protección de Datos, (AEPD) protege los derechos de los ciudadanos. Es el ente de derecho público que vela por el cumplimiento de la normativa sobre protección de datos personales en todos los ámbitos, público y privado, por lo que actúa con plena independencia de las Administraciones Públicas.

PASOS A SEGUIR

PRIMER PASO :Como obligado al cumplimiento del contenido del Reglamento, es necesario elaborar un REGISTRO DE ACTIVIDADES DE TRATAMIENTO (registro de los datos personales que utilizamos).

SEGUNDO PASO: Realizado el registro de tratamientos, se realizará un análisis personalizado de los posibles riesgos.

TERCER PASO: Analizados los riesgos, se propondrán medidas de seguridad adecuadas a los mismos y dirigidas a evitar las posibles consecuencias sancionatorias. (verificación de los documentos utilizados, clausulado de los contratos, contenido de páginas web).

CUARTO PASO: mecanismos y procedimientos para notificar posibles quiebras de seguridad .

QUINTO PASO: Si fuera necesario, designar un Delegado de Protección de Datos, que actuará como intermediario, ante la Agencia, y que asumirá las funciones derivadas del cumplimiento del contenido del Reglamento.

Registro de actividades de tratamiento

Cada empresa u organización deberá llevar un Registro de Actividades de Tratamiento de acuerdo a lo que el Artículo 30 del RGPD detalla. El artículo 30.1 dicta su contenido para el responsable de tratamiento, y el 30.2 detalla el contenido del Registro de Actividades que el encargado de tratamiento debe llevar.
Un tratamiento es el conjunto de operaciones dirigidas a conseguir una determinada finalidad que se legitiman en una misma base jurídica. Cada tratamiento incluirá una serie de operaciones como, recogida de datos, registro, organización de datos, estructuración, consulta o uso de los datos.
El artículo 30 del RGPD indica *" El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite".*
Es por tanto necesario que el registro de actividades esté permanentemente actualizado y en un formato claro y legible para que se comprenda por terceros. Es un documento vivo y requiere revisión continua, cada vez que se produzca un cambio relevante.

Corresponde a cada empresa, de acuerdo al **principio de responsabilidad proactiva** que rige el RGPD, decidir el nivel de segregación o agregación con el que desea registrar los tratamientos de datos de carácter personal que requiere su actividad. Deberá valorar hasta qué punto la segregación de sus tratamientos en elementos diferentes se corresponde con finalidades, bases jurídicas y categorías de afectados distintos. La gran mayoría de empresas tienen un tratamiento principal (el propio de la actividad de la empresa) y una serie de tratamientos vinculados al mismo.

El objetivo de este registro es que los individuos cuyos datos son objeto de tratamiento puedan tener control sobre efectivo sobre los mismos.
Para realizar el registro de actividades es conveniente conocer tanto el uso que se le da a los datos manejados por la empresa como a la base legal o legitimación para obtener dichos datos.
El RGPD impone a cada responsable de tratamiento, al menos, dos obligaciones que pueden suponer tratamientos sobre datos de carácter personal y, por lo tanto, actividades que necesariamente debo incluir en mi Registro de Actividades de Tratamiento:

- **Atención a los derechos de las personas:** lo que antes iba implícito en la gestión de cada fichero ahora cabría definirlo como una actividad de tratamiento específica, puesto que recogeremos los datos personales necesarios, según los principios que el artículo 5 del RGPD establece y explica, para poder atender los derechos de las personas que se dirijan a la organización.

- **Notificación de una quiebra de seguridad de los datos personales a la autoridad de control y a los interesados:** será ésta una actividad que refleje los datos de carácter personal que debo incluir para dar cumplimiento a lo establecido en los artículos 33 y 34 del RGPD.

En cualquier caso, y en ejecución del principio de responsabilidad proactiva, corresponde a la organización decidir de dónde parte a la hora de registrar sus actividades de tratamiento y cómo realizar la gestión de la misma.

La definición de las actividades de tratamiento es un paso necesario para conocer la finalidad de los datos que recabamos en la organización. La gestión en protección de datos debe resultar útil, ágil y efectiva, el objetivo final es que los individuos cuyos datos son objeto de tratamiento puedan tener, en su caso, un conocimiento claro de los tratamientos que la organización realiza sobre ellos.
El RGPD establece en su artículo 5 los siguientes principios relativos al tratamiento de datos personales que es necesario considerar:

- **Licitud, lealtad y transparencia:** Los datos deben ser tratados de manera lícita, leal y transparente en relación con el interesado.
- **Limitación de la finalidad:** Se deben recoger con fines determinados, explicitos y legítimos.
- **Minimización de los datos:** Deben ser adecuados, pertinentes y limitados a lo necesario.
- **Exactitud:** Deben ser exactos y actualizados. Si son inexactos o no están actualizados deben suprimirse o rectificarse.
- **Limitación en el plazo de conservación:** No se deben guardar más tiempo del necesario.
- **Integridad y confidencialidad:** Deben ser tratados de tal manera que se garantice una seguridad adecuada.

El artículo 5 establece también que el responsable del tratamiento deberá garantizar el cumplimiento de los principios relativos al uso de los datos, así como, la figura responsable de demostrarlo. Por tanto es vital definir adecuadamente las actividades de tratamiento y documentar los análisis realizados.
Una vez realizado el registro de tratamientos se debe analizar si entraña un riesgo alto con el objetivo de determinar si se precisa una evaluación de impacto relativa a la protección de datos.

Las evaluaciones de impacto (EIPD) no se requieren en todos los casos, en cada actividad de tratamiento se debe valorar la necesidad de realizarla, es fundamental por tanto, un análisis previo para conocer el nivel de riesgo del tratamiento.

Para el registro de actividades de tratamiento vamos a proceder a describir las actividades para la figura del responsable del tratamiento y del encargado del tratamiento.

El **ciclo de vida de los datos** se puede dividir en las siguientes etapas:

Captura de datos: Proceso de obtención de datos para su almacenamiento y posterior procesado. Dentro de esta categoría se pueden encontrar diversas técnicas: formularios web, formularios en papel, toma de muestras y realización de encuestas, grabaciones de audio y vídeo, redes sociales, captación mediante sensores, etc.

Clasificación/Almacenamiento: Establecer categorías y asignarlas a los datos para su clasificación y almacenamiento en los sistemas o archivos.

Uso/Tratamiento: Operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos de los datos automatizados o manuales.

Cesión o transferencia de los datos a un tercero para su tratamiento: Traspaso o comunicación de datos realizada a un tercero, definido como aquella persona física o jurídica, pública o privada u órgano administrativo. Este concepto es muy amplio, puesto que recoge tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma de acceso a los datos..

Destrucción: Eliminar los datos que puedan estar contenidos en los sistemas o archivos, de manera que no puedan ser recuperados de los soportes de almacenamiento.

Tratamiento principal de la empresa: Usuarios

Responsable del tratamiento:	Concaes
Delegado de protección de datos:	
Actividad del tratamiento: (registro, cesión, grabación...etc)	Registro, grabación y procesado
Finalidad de este tratamiento: (Para que usamos estos datos)	Mantener, gestionar y ejecutar la prestación de los servicios sociales correspondientes a los usuarios.
Categoría de los datos solicitados: (generales, nombre, dni, bancarios...etc)	Identificativos, de contacto, económicos, de salud, académicos y profesionales.
Destinatarios de los datos: (Bancos, gestorías, Seguridad Social...etc)	Agencia Estatal de Administración Tributaria e Instituto Nacional de la Seguridad Social. Bancos y otras Autoridades públicas, entidades financieras, gestoría y otros posibles prestadores de servicios necesarios para la ejecución del contrato. Autoridades públicas y entidades sociales relacionadas con el servicio prestado.
Cesiones:	
Transferencias internacionales: (¿se ceden fuera de la UE?)	No previstas
Plazo previsto para suprimir (borrar o destruir) los datos:	Los previstos por la legislación fiscal y otras normativas aplicables a la relación contractual respecto a la prescripción de responsabilidades y las obligaciones de conservación tras la extinción de la necesidad que motivó su captación.
Medidas de seguridad implantadas en este tratamiento (describir)	Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado según lo previsto en el artículo 32 del RGPD
Nivel de riesgo en el tratamiento:	Limitado en impacto y probabilidad.
¿Precisa de evaluación de impacto a la privacidad?	NO
Legitimación del tratamiento: Base legal para tratar los datos *	Ejecución de un contrato en el que el interesado es parte, realización de una misión realizada en interés público o cumplimiento de una obligación legal aplicable al responsable.
Observaciones:	.

*El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:
- Consentimiento. - Relación contractual. - Intereses vitales del interesado o de otras personas. - Obligación legal para el responsable. - Interés público o ejercicio de poderes públicos.

Tratamiento : Recursos Humanos (C.V. posibles contrataciones)

Tratamiento vinculado:	Usuarios
Finalidad de este tratamiento: (Para que usamos estos datos)	Gestión de la relación con los candidatos a un empleo
Categoría de los datos solicitados: (generales, nombre, dni, bancarios...etc)	Identificativos, de contacto, profesionales, académicos y formativos, personalest
Destinatarios de los datos: (Bancos, gestoras, Seguridad Social...etc)	No se prevén cesiones de datos a ningún destinatario
Transferencias internacionales: (¿se ceden fuera de la UE?)	No previstas
Plazo previsto para suprimir (borrar o destruir) los datos:	2 años
Medidas de seguridad implantadas en este tratamiento (describir)	Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado según lo previsto en el artículo 32 del RGPD
Nivel de riesgo en el tratamiento:	Despreciable en impacto y probabilidad
¿Precisa de evaluación de impacto a la privacidad?	No
Legitimación del tratamiento: Base legal para tratar los datos *	Consentimiento del interesado
Observaciones:	

*El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

- Consentimiento. - Relación contractual. - Intereses vitales del interesado o de otras personas. - Obligación legal para el responsable. - Interés público o ejercicio de poderes públicos. - Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

Tratamiento : Redes Sociales

Tratamiento vinculado:	Usuarios
Finalidad de este tratamiento: (Para que usamos estos datos)	Publicidad y contacto
Categoría de los datos solicitados: (generales, nombre, dni, bancarios...etc)	Imagen e identificativos
Destinatarios de los datos: (Bancos, gestoras, Seguridad Social...etc)	
Transferencias internacionales: (¿se ceden fuera de la UE?)	No previstas
Plazo previsto para suprimir (borrar o destruir) los datos:	Hasta ejercer supresión
Medidas de seguridad implantadas en este tratamiento (describir)	Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado según lo previsto en el artículo 32 del RGPD
Nivel de riesgo en el tratamiento:	Despreciable en impacto y probabilidad
¿Precisa de evaluación de impacto a la privacidad?	NO
Legitimación del tratamiento: Base legal para tratar los datos *	Interés legítimo. Consentimiento expreso demostrable para imagen
Observaciones:	.

*El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

- Consentimiento. - Relación contractual. - Intereses vitales del interesado o de otras personas. - Obligación legal para el responsable. - Interés público o ejercicio de poderes públicos. - Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

Tratamiento : Formulario Web

Tratamiento vinculado:	Usuarios
Finalidad de este tratamiento: (Para que usamos estos datos)	Petición de información y medidas precontractuales
Categoría de los datos solicitados: (generales, nombre, dni, bancarios...etc)	Identificativos, email y teléfono
Destinatarios de los datos: (Bancos, gestoras, Seguridad Social...etc)	La propia empresa. Gestora del dominio web, Google (cookies)
Transferencias internacionales: (¿se ceden fuera de la UE?)	No previstas
Plazo previsto para suprimir (borrar o destruir) los datos:	1 año máximo
Medidas de seguridad implantadas en este tratamiento (describir)	Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado según lo previsto en el artículo 32 del RGPD
Nivel de riesgo en el tratamiento:	Despreciable en impacto y probabilidad
¿Precisa de evaluación de impacto a la privacidad?	NO
Legitimación del tratamiento: Base legal para tratar los datos *	Consentimiento expreso
Observaciones:	.

*El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

- Consentimiento. - Relación contractual. - Intereses vitales del interesado o de otras personas. - Obligación legal para el responsable. - Interés público o ejercicio de poderes públicos. - Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

Tratamiento : Recursos Humanos (registro de jornada laboral)

Tratamiento vinculado:	Usuarios
Finalidad de este tratamiento: (Para que usamos estos datos)	Registro de jornada laboral (papel / GPS / huella dactilar)
Categoría de los datos solicitados: (generales, nombre, dni, bancarios...etc)	Identificativos, DNI, NAF y firma/ Ubicación / Huella
Destinatarios de los datos: (Bancos, gestoras, Seguridad Social...etc)	Autoridad Competente
Transferencias internacionales: (¿se ceden fuera de la UE?)	No previstas
Plazo previsto para suprimir (borrar o destruir) los datos:	4 años mínimo
Medidas de seguridad implantadas en este tratamiento (describir)	Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado según lo previsto en el artículo 32 del RGPD
Nivel de riesgo en el tratamiento:	Despreciable en impacto y probabilidad
¿Precisa de evaluación de impacto a la privacidad?	NO
Legitimación del tratamiento: Base legal para tratar los datos *	Cumplimiento Normativo
Observaciones:	.

*El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

- Consentimiento. - Relación contractual. - Intereses vitales del interesado o de otras personas. - Obligación legal para el responsable. - Interés público o ejercicio de poderes públicos. - Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

Tratamiento : Página Web (Cookies)

Tratamiento vinculado:	Usuarios
Finalidad de este tratamiento: (Para que usamos estos datos)	Técnicas de preferencia, perfilado de terceros, etc
Categoría de los datos solicitados: (generales, nombre, dni, bancarios...etc)	IP, conductas, preferencias e intereses
Destinatarios de los datos: (Bancos, gestoras, Seguridad Social...etc)	Gestora del dominio web, Google (cookies)
Transferencias internacionales: (¿se ceden fuera de la UE?)	No previstas
Plazo previsto para suprimir (borrar o destruir) los datos:	Varía en función de la finalidad
Medidas de seguridad implantadas en este tratamiento (describir)	Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado según lo previsto en el artículo 32 del RGPD
Nivel de riesgo en el tratamiento:	Despreciable en impacto y probabilidad
¿Precisa de evaluación de impacto a la privacidad?	NO
Legitimación del tratamiento: Base legal para tratar los datos *	Consentimiento expreso
Observaciones:	.

*El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

- Consentimiento. - Relación contractual. - Intereses vitales del interesado o de otras personas. - Obligación legal para el responsable. - Interés público o ejercicio de poderes públicos. - Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

Tratamiento : Recursos Humanos

Tratamiento vinculado:	Usuarios
Finalidad de este tratamiento: (Para que usamos estos datos)	Contratación / nóminas / PRL
Categoría de los datos solicitados: (generales, nombre, dni, bancarios...etc)	Identificativos, DNI, NAF, profesionales, académicos, de contacto y bancarios
Destinatarios de los datos: (Bancos, gestoras, Seguridad Social...etc)	Hacienda y Seguridad Social
Transferencias internacionales: (¿se ceden fuera de la UE?)	No previstas
Plazo previsto para suprimir (borrar o destruir) los datos:	Borrado o destruccion a los 5 años
Medidas de seguridad implantadas en este tratamiento (describir)	Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado según lo previsto en el artículo 32 del RGPD
Nivel de riesgo en el tratamiento:	Despreciable en impacto y probabilidad
¿Precisa de evaluación de impacto a la privacidad?	NO
Legitimación del tratamiento: Base legal para tratar los datos *	Ejecución de un contrato
Observaciones:	.

*El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. También recoge las mismas bases jurídicas que contenía la Directiva y que reproduce la LOPD:

- Consentimiento. - Relación contractual. - Intereses vitales del interesado o de otras personas. - Obligación legal para el responsable. - Interés público o ejercicio de poderes públicos. - Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.