REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

2022

Este documento contiene las medidas técnicas y organizativas de seguridad y de gestión de la información, que debe implementar.

CONTENIDOS

I.- INTRODUCCIÓN

El REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, en adelante **RGPD**, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Ambas están destinadas a proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

La Ley Orgánica 3/2018 pretende lograr la adaptación del ordenamiento jurídico español al Reglamento UE 2016/679 y, garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Ambos textos legales consideran lo siguiente:

- La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental.
- Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal, deben respetar sus libertades y derechos fundamentales.

Y garantiza:

- Un nivel uniforme y elevado de protección de las personas físicas y elimina los obstáculos a la circulación de datos personales dentro de España y de la Unión Europea.
- Un nivel coherente de protección de las personas físicas en toda el territorio UE y evitar divergencias que dificulten la libre circulación de datos personales.

II.- OBJETO DEL REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

El artículo 24 del RGPD establece la responsabilidad del Responsable del Tratamiento: “El Responsable del Tratamiento aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD.”

Para ello, el Responsable del Tratamiento deberá tener un registro de actividades del tratamiento que contenga la información establecida en el artículo 30.1 del RGPD.

Así mismo, el artículo 28.1 de la Ley 3/2018, de 5 de diciembre, Ley Orgánica de Protección de Datos de Carácter Personal y de las garantías digitales, establece que “Los Responsables y Encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantaizar y acreditar que el tratamiento es conforme con el citado Reglamento, con la presente Ley Orgánica, sus normas de desarrollo y la legislación sectorial aplicable.”

Por tanto, es la finalidad del presente documento y sus anexos, en cumplimiento de lo dispuesto con la normativa vigente, recoger las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos de los afectados cuyos datos de carácter personal sean objeto de tratamiento.

III.- ÁMBITO DE APLICACIÓN DEL REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

El ámbito de aplicación del RGPD y la Ley Orgánica 3/2018, es el relativo al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero y garantizar los derechos digitales de las personas.

La protección otorgada por las citadas normativas deben aplicarse a las personas físicas, independientemente de su nacionalidad, lugar de residencia, en relación con el tratamiento de sus datos personales.

La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como su tratamiento manual, cuando los datos figuren en un fichero o estén destinados a ser incluidos en él, y garantizar los derechos digitales de las personas.

Fuera del ámbito de aplicación de estos textos legales se encuentran el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas,incluido el nombre y la forma jurídica y sus datos de contacto.

El ámbito de aplicación de éste Registro de Actividades del Tratamiento comprende a los ficheros que contienen datos de carácter personal que se hallen bajo la responsabilidad del Responsable del Tratamiento, incluyendo los sistemas de información, soportes, infraestructuras y equipos y empleados para el tratamiento de datos de carácter personal,que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, las personas que intervienen en el tratamiento y los establecimientos (locales/dependencias) en los que se ubican.

IV.- IDENTIFICACION DEL RESPONSABLE DEL TRATAMIENTO

RESPONSABLE:	**Cámara Of. de Comercio, Industria y Navegación de Cádiz**
CIF:	**Q1173001G**
DOMICILIO:	**C/ Antonio López 4, Cádiz, 11004 (Cadiz)**
TELÉFONO:	**956 010 000**
CORREO ELECTRÓNICO:	**info@camaracadiz.com**
ACTIVIDADES:	**Mejorar la capacidad competitiva del tejido empresarial, mediante el impulso de servicios especializados de calidad y alto valor añadido, y la promoción y defensa de los intereses generales del comercio, la industria, los servicios y la navegación.**

FUNCIONES y OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

El Responsable del Tratamiento es el encargado jurídicamente dela seguridad de la información y por tanto de la aplicación de medidas técnicas y oganizativas. Para ello, debe realizar las acciones correspondientes para que el Personal afectado por este Documento conozca las normas que aplican al desarrollo de sus funciones, para lo cual debe:

1. Implantar las medidas de seguridad establecidas en este Documento. El Responsable del Tratamiento deberá garantizar la difusión de este Documento entre todo el Personal de la Organización y todo aquel implicado.

2. Mantener el Registro de Actividad de Tratamiento actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

3. Adecuar en todo momento el contenido del mismo, a las disposiciones vigentes en materia de seguridad de la información.

4. Comprobar que los sistemas informáticos de acceso a los ficheros de información tengan acceso restringido, por ejemplo mediante un código de usuario y contraseña.

5. Cuidar que todos los usuarios autorizados para acceder a los ficheros, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

6. Garantizar que el archivo de los documentos en soportes no automatizados (papel) se realice mediante criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de los interesados.

7. Autorizar expresamente la salida de soportes que contengan datos de carácter personal fuera de las dependencias del Responsable del Tratamiento.

8. Proteger el acceso a la información/documentación ubicada en soportes no automatizados (archivadores, armarios, etc..) con puertas con llave, si la sensibilidad de la información lo requiere.

9. El Responsable del Tratamiento se encargará de verificar la definición y correcta aplicación de las copias de seguridad y recuperación de los datos.

10. El Responsable del Tratamiento designará a uno o a varios Delegados de Protección de Datos, cuando así lo requiera la normativa vigente, en virtud de la dimensión, sistemática del tratamiento, sensibilidad de la información, y actividades desarrolladas por el Responsable del Tratamiento.

V.- DESCRIPCIÓN DE LAS ACTIVIDADES DE TRATAMIENTO Y DE LOS DATOS TRATADOS

TRATAMIENTO DE DATOS DE:	**PROVEEDORES**
LEGITIMACIÓN de los Tratamientos:	• Relación Contractual
FINALIDADES de los Tratamientos:	• Facturación de los servicios prestados. Gestión económica , contable, fiscal y administrativa.
SOPORTE de los Datos:	**SOPORTES PAPEL Y AUTOMATIZADO**
Categorías de los Datos:	**NOMBRE/A, DNI, TELÉFONO, DATOSECON, EMAIL**
Categorías de los INTERESADOS:	**PROVEEDORES**
Categorías de los DESTINATARIOS:	**BANCOS, ENT. FINANCIERAS, GESTORÍA, AA.PP**
Plazos de CONSERVACIÓN:	**PLAZOS SEGÚN LEGISLACIÓN**
Categorías DATOS SENSIBLES:	**NO**
Envío Comunicaciones Comerciales:	**NO**
Tiene Registro de Ejercicio de Derechos:	**SI**

TRATAMIENTO DE DATOS DE:	**CLIENTES**
LEGITIMACIÓN de los Tratamientos:	• Consentimiento expreso • Relación Contractual • Por obligación legal
FINALIDADES de los Tratamientos:	• Envío de comunicaciones de tipo informativo sobre los servicios prestados y/o productos adquiridos. • Facturación de los servicios prestados. Gestión económica , contable, fiscal y administrativa. • Gestión de la relación con los Usuarios/Clientes.
SOPORTE de los Datos:	**SOPORTES PAPEL Y AUTOMATIZADO**
Categorías de los Datos:	**OTROS, CURRICULUM, DATOSECON, EMAIL, TELÉFONO, DNI, NOMBRE/A**
Categorías de los INTERESADOS:	**CLIENTES**
Categorías de los DESTINATARIOS:	**AA.PP**
Plazos de CONSERVACIÓN:	**PLAZOS SEGÚN LEGISLACIÓN**
Categorías DATOS SENSIBLES:	**NO**
Envío Comunicaciones Comerciales:	**NO**
Tiene Registro de Ejercicio de Derechos:	**SI**

TRATAMIENTO DE DATOS DE:	**TRABAJADORES**
LEGITIMACIÓN de los Tratamientos:	• Relación Contractual • Por obligación legal
FINALIDADES de los Tratamientos:	• Gestión de contactos para el desarrollo de procesos de selección de personal. • Gestión de la relación laboral con los Trabajadores. • Gestión de nóminas, confección de seguros sociales, recursos humanos.
SOPORTE de los Datos:	**SOPORTES PAPEL Y AUTOMATIZADO**
Categorías de los Datos:	**NOMBRE/A, DNI, TELÉFONO, EMAIL, DATOSECON**
Categorías de los INTERESADOS:	**TRABAJADORES**
Categorías de los DESTINATARIOS:	**AA.PP, BANCOS**
Plazos de CONSERVACIÓN:	**PLAZOS SEGÚN LEGISLACIÓN**
Categorías DATOS SENSIBLES:	**NO**
Envío Comunicaciones Comerciales:	**NO**
Tiene Registro de Ejercicio de Derechos:	**SI**

TRATAMIENTO DE DATOS DE:	**VIDEOVIGILANCIA**
LEGITIMACIÓN de los Tratamientos:	• Interés Legítimo del Resp.
FINALIDADES de los Tratamientos:	• Seguridad de las personas, bienes e instalaciones.
SOPORTE de los Datos:	**SOPORTE AUTOMATIZADO**
Categorías de los Datos:	**IMAGEN**
Categorías de los INTERESADOS:	**CLIENTES, TRABAJADORES**
Categorías de los DESTINATARIOS:	**FCSE**
Plazos de CONSERVACIÓN:	**30 DÍAS DESDE SU CAPTACIÓN**
Categorías DATOS SENSIBLES:	**NO**
Envío Comunicaciones Comerciales:	**NO**
Tiene Registro de Ejercicio de Derechos:	**SI**

VI.- MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LOS NIVELES DE SEGURIDAD

6.1.- MEDIDAS Y NORMAS RELATIVAS A LA IDENTIFICACIÓN DEL PERSONAL AUTORIZADO A ACCEDER A LOS DATOS PERSONALES

CONTROL DE ACCESO A FICHEROS AUTOMATIZADOS

- Los sistemas informáticos que contienen los ficheros cuyos datos de carácter personal son objeto de tratamiento, deberán tener su acceso restringido mediante un código de usuario y una contraseña. La contraseña no ha de ser perpetua y ha de forzarse el cambio cada cierto tiempo (por ejemplo trimestralmente).
- Debe existir una relación actualizada de los Usuarios con acceso, que sólo será conocida por el propio Administrador de Sistemas o en su defecto por la persona responsable.
- Cuando el mismo equipo informático o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesionales y personal en el equipo informático o dispositivo.
- También resulta recomendable disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- Exclusivamente el Administrador de Sistemas, o persona responsable en su defecto, debe estar autorizado para conceder, alterar o anular el acceso autorizado de terceros usuarios sobre los datos y los recursos,conforme a los criterios establecidos por el Responsable del Tratamiento.
- Los equipos informáticos deberán contar con herramientas del tipo antimalware / antivirus y cortafuegos (firewall).
- Los sistemas operativos de los equipos informáticos deberán estar actualizados.
- Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información limitando el número máximo de intentos fallidos. Cuando sea técnicamente posible, se guardará en un fichero auxiliar a modo de registro la fecha, hora, código y claves erróneas que se han introducido, así como otros datos que ayuden a descubrir la autoría de esos intentos de acceso no autorizados en los ficheros. Este tipo de medidas de seguridad tiene especial importancia cuando se traten datos personales de carácter sensibles.

PROCEDIMIENTO DE ASIGNACIÓN DE CONTRASEÑA

- Las contraseñas se asignarán y cambiarán mediante un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del Administrador de Sistemas (si existe ésta figura).
- La periodicidad del cambio de contraseñas debe ser inferior a un año.
- Las contraseñas deberán ser suficientemente complejas y seguras, evitando el uso propio identificador como contraseña o palabras sencillas, el nombre propio, fecha de nacimiento, etc. Para ello se seguirán las siguientes pautas en la elección de las contraseñas:

1. Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
2. No deberán coincidir con el código de usuario.
3. No deberán estar basadas en cadenas de caracteres que sean fácilmente asociables al usuario (nombre, apellidos, ciudad y fecha de nacimiento, DNI, nombre de familiares, matrícula del coche, etc.).

- Las contraseñas deberán ser estrictamente confidenciales y personales. Cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al Administrador de Sistemas (si existe ésta figura) y subsanada en el menor plazo de tiempo posible. Deberá registrarse como incidencia y proceder inmediatamente a su cambio.

- El archivo donde se almacenen las contraseñas deberán estar protegido y bajo la responsabilidad del Administrador de Sistemas (si existe ésta figura).

CONTROL DE ACCESO FÍSICO A CENTRO/S Y PUESTO/S DE TRABAJO

- Las dependencias donde se ubiquen los ordenadores o archivos que contienen los ficheros con información personal deben ser objeto de especial protección, de modo que se garantice la disponibilidad y confidencialidad de los datos protegidos.
- Las dependencias deberán contar con los medios de seguridad que eviten los riesgos de indisponibilidad de los ficheros que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas. La descripción de esos medios se encuentra en:
    - ANEXO I. DESCRIPCIÓN DE LOS PUESTOS DE TRABAJO
    - ANEXO II. DESCRIPCIÓN DE CENTRO/S DE TRABAJO Y EQUIPAMIENTOS
- Solo el personal autorizado, podrá tener acceso a las dependencias donde se encuentren ubicados los sistemas de información condatos de carácter personal.

CONTROL DE ACCESO A FICHEROS NO AUTOMATIZADOS (EN SOPORTE PAPEL)

- El Responsable del Tratamiento deberá establecerse un control de los accesos autorizados, pudiendo exclusivamente los usuarios autorizados acceder a los ficheros no automatizados.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- La entidad responsable de la limpieza del centro de trabajo, así como cualquier otra entidad prestataria de servicios con acceso limitado o no, frecuente o esporádico a la informati cóntratada por el Responsable del Tratramiento garantizará la observancia de las medidas de seguridad necesarias para que no se produzca, voluntaria o involuntariamente, incidencia alguna en tales dependencias, siendo aquella responsable de las que pudieran producirse.
- Iguales garantías se deberán adoptar en el desarrollo de las obras y tareas de mantenimiento y reparación de los elementos ubicados dentro de las dependencias del Responsable del Tratamiento.
- El acceso de usuarios no incluidas en el Anexo de Personal Autorizado,deberá estar adecuadamente registrado.

6.2.- GESTIÓN Y ALMACENAMIENTO DE SOPORTES Y DOCUMENTOS

FICHEROS AUTOMATIZADOS

Un soporte de ficheros automatizados es un objeto físico o virtual susceptible de ser tratado en un sistema de información y en el cual se pueden grabar o recuperar datos.

- Los soportes automatizados que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado.
- La información contenida en los soportes automatizados deberá estar cifrada.
- Los soportes deben almacenarse en un lugar con acceso restringido, para que su utilización quede restringida a las personas con acceso autorizado a los ficheros, según la relación del ANEXO III: PERSONAL AUTORIZADO.
- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.
- La salida de soportes informáticos que contengan datos de carácter personal, fuera de las dependencias en las que esté ubicado el fichero, únicamente podrá ser autorizada por el Responsable del Tratamiento.
- Se confeccionará un inventario de soportes que contendrá la siguiente información: tipo de soporte, fecha de creación, información que contiene y lugar donde se encuentra almacenado. El inventario se mantendrá

constantemente actualizado.

- Cuando los soportes informáticos vayan a salir fuera de las dependencias en las que se encuentren ubicados los ficheros, como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.
- Deberá establecerse un sistema de registro de entrada de soportes que permita conocer el tipo de documentos, la fecha, hora, el emisor, el número de soportes y la personal responsable de la recepción que deberá estar debidamente autorizada.
- La distribución de los soportes se realizará del siguiente modo:
    - Los soportes serán almacenados con un sistema de etiquetado confidencial.
    - La distribución de los soportes se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte, evitándose el uso de los dispositivos que no permitan cifrado o la adopción de medidas alternativas.

FICHEROS NO AUTOMATIZADOS

- El Responsable del Tratamiento contará con dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.
- El archivo de los documentos se realizará garantizando que los documentos van a estar perfectamente conservados, y sea fácil localizar y consultar su información. Todo ello para posibilitar el ejercicio de los derechos de las personas cuyos datos sean objeto de tratamiento.
- Cuando los documentos con datos personales no se encuentren archivados en las carpetas u otros dispositivos de almacenamiento indicados anteriormente, por estar en proceso de tramitación, las personas que se encuentren al cargo de los mismos deberán custodiarlos e impedir en todo momento que pueden ser una documentación a la que tenga acceso personal no autorizado.
- Se utilizarán armarios cerrados con llave en los que los datos estarán dispuestos, con un criterio lógico en los archivadores, siendo responsabilidad del Responsable del Tratamiento el impedir el acceso a la información por personas no autorizadas.
- Deberá establecerse un sistema de registro de entrada y salida de documentos que permita conocer el tipo de información contenida, la fecha, hora, el emisor, el número de documentos y la personal responsable de la entrada y salida.
- La entrada o salida de documentos debe estar autorizada por el Responsable del Tratamiento.

6.3.- ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones, tales como Internet, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Los datos personales que se transmitan a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizarán previamente cifrando los datos por los distintos mecanismos de cifrado que se utilicen y garanticen que la información no va a ser inteligible ni manipulada por terceros.

6.4.- RÉGIMEN DE TRABAJO FUERA DE LAS DEPENDENCIAS FÍSICAS

FICHEROS AUTOMATIZADOS

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del tratamiento y, en todo caso, deberá garantizarse las medidas de seguridad.

En la autorización para el tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá aparecer lo siguiente:

- Finalidad para la cual se solicita la autorización.

- Tipo de tratamiento (automatizado, no automatizado, mixto)
- Tipo de dispositivo portátil (en su caso)
- Tipo de documentación objeto de tratamiento
- Ficheros de dónde proceden los datos
- Periodo de validez de la autorización
- Medidas de seguridad implementadas para proteger la información
- Persona autorizada para trabajar fuera de los locales
- Cargo/departamento
- Observaciones
- Firma de la persona que autoriza

El tratamiento fuera de los locales de trabajo deberá cifrarse los datos que contengan los dispositivos portátiles cuando éstos se encuentran fuera de las instalaciones que están bajo control del responsable del tratamiento.

Se deberá evitar el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado.

FICHEROS NO AUTOMATIZADOS

Siempre que se proceda al traslado físico de la documentación contenida en un fichero se trasladará con la debida diligencia y cuidado, para impedir su pérdida en el desplazamiento.

En los ficheros no automatizados se adoptarán medidas que impidan el acceso o manipulación, tales como la utilización de un maletín con cierre de seguridad para trasladar los documentos.

6.5.- PROCEDIMIENTO PARA LA REALIZACIÓN DE COPIAS DE REPRODUCCIÓN

- Deberán realizarse copias de seguridad periódicamente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
- Los procedimientos establecidos para la realización de copias de seguridad y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
- El Responsable del Tratamiento se encargará de verificar al menos cada seis meses, la definición y correcta aplicación de los procedimientos de realización de copias de seguridad y de recuperación de los datos.
- Será necesaria la autorización por escrito del Responsable del Tratamiento para la ejecución de los procedimientos de recuperación de los datos.
- Deberá conservarse una copia de seguridad y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos.
- Las copias desechadas deberán ser destruidas, imposibilitando el posterior acceso a la información contenida en los documentos.

VII.- PROCEDIMIENTO DE REVISIÓN DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Según establece el articulo 30 del RGPD “El Responsable o Encargado del Tratamiento y, en su caso, el Representante del Responsable o del Encargado pondrá el registro a disposición de la autoridad de control que lo solicite”

Teniendo en cuenta el artículo 31.1 de la Ley Orgánica 3/2018 establece que "Los responsables y encargados del tratamiento o, en su caso, su representante deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del RGPD"

Por tanto es fundamental que éste documento esté permanentemente actualizado, y en un formato claro y legible que facilite su compresión por parte de terceros. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal deberá conllevar la revisión de la documentación total o parcial.

Las medidas de seguridad serán revisadas de forma periódica, pudiéndose realizar por mecanismos automáticos(software o programas informáticos) o de manera manual.

VIII.- IDENTIFICACIÓN DEL ENCARGADO DEL TRATAMIENTO

En el Considerando 81 del RGPD establece que "*.. respecto del tratamiento que lleve a cabo el Encargado por cuenta del Responsable, éste, al encomendar actividades de tratamiento a un Encargado, debe recurrir únicamente a Encargados que ofrezcan suficientes garantías, en particular, en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento.*

El tratamiento por un Encargado debe regirse por un contrato, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los interesados."

Así mismo el artículo 28.1 del RGPD establece que "*..cuando se vaya a realizar un tratamiento por cuenta de un Responsable del tratamiento, éste elegirá únicamente a un Encargado de Tratamiento que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con el Reglamento.*"

Por tanto, en cumplimiento del articulo 28.3 del RGPD se deberá formalizarse un contrato de acceso (tratamiento) a datos, de manera que acredite fe hacientemente su celebración y contenido.

X.- PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Todos los usuarios debe conocer sus funciones y obligaciones en lo concerniente al RGPD y a la Ley Orgánica de Protección de Datos de carácter Personal y garantía de los derechos digitales.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con siguiente procedimiento:

1. Se facilitará una copia del ANEXO de FUNCIONES Y OBLIGACIONES DEL PERSONAL a cada usuario con acceso a los ficheros, o, en su defecto, se tendrá siempre a su disposición para cualquier consulta.

2. Se firmará por cada usuario el DOCUMENTO DE CONFIDENCIALIDAD, incorporando estos documentos al mismo.

3. Según establece el artículo 87 (Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral) de la Ley Orgánica 3/2018 establece que "Los trabajadores tendrán derecho a la protección de su intimidad en el uso de los dipositivos digitales puestos a su disposición por su empleador". En el punto 2 "El empleador podrá acceder a los conteniedos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.En el punto 3 "Los empleadores deberán establecer los criterios de utilización de los criterios digitales respetando en todo caso los estandares mínios d eprotección de su intimidad de acuerdo con los usos sociles y derechos reconocidos contitucionalo y legalmente. Los trabajadores deberán ser informados de dichos criterios. En el artículo 88 se establece que se deberá elaborarse una política dirigida a los trabajadores en las que se definirán las modalidades de ejercicio del derecho a la desconexión digital del trabajo..

- Por último, el artículo 90 establce que "los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores. Los empleadores deberán informar de forma expresa, clara e inequívoca jacerca de la existencia y carcaterísticas de estos dispositivos. .

XI.- PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LA VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

Se considera una violación de la seguridad de los datos personales aquel incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

NOTIFICACIONES

En caso de violación de la seguridad de la información de carácter personal, el Responsable del Tratamiento deberá notificar a la Autoridad de Control competente sin dilación y,de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella; a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos del interesado. Si la notificación a la Autoridad de Control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

La notificación contemplada deberá contener como mínimo:

- Describirla naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximados de registros de datos personales afectados.
- Comunicar el nombre y los datos de contacto del Delegado de protección de datos u otro contacto en el que pueda obtenerse más información.
- Describirlas posibles consecuencias de la violación de la seguridad delos datos personales.
- Describirlas medidas adoptadas o propuestas por el Responsable del Tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- El Responsable del Tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la Autoridad de Control verificar el cumplimiento de lo exigido por la normativa reguladora.

ANEXOS

DEL REGISTRO DE ACTIVIDADES DEL TRATAMIENTO DE DATOS PERSONALES