GrupoIWI®
protección de datos

Protocolo de privacidad y Protección de Datos

(V018.1)

www.grupoiwi.com

Estimado Cliente:

Tal y como le informamos en anteriores comunicaciones, le enviamos el Protocolo de Protección de Datos y Privacidad, actualizado según la normativa vigente en materia de protección de datos, en particular conforme al REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 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, conocido por sus siglas RGPD.

Esta nueva normativa trae consigo, entre otras novedades, un principio fundamental llamado "Accountability" o de "Responsabilidad Proactiva". A través de este principio de protección de datos, el responsable y encargado de tratamiento estarán obligados a demostrar que sus actividades de tratamiento de datos cumplen con los principios relativos al tratamiento de datos (art. 5.1 del RGPD).

Por ello le recomendamos, si dispone de ella, que conserve la documentación anterior relacionada con nuestros servicios, o con su anterior consultora legal, en particular el último Documento de Seguridad, así como los certificados o resolución de inscripción de los ficheros notificados al Registro General de la Agencia Española de Protección de Datos, e informes de auditoría, que fueron generados conforme a la normativa LOPD 15/1999 y R.D. 1720/2007, ya derogados.

Al objeto de que dicha consultoría sea completa, y evitar posibles sanciones, es necesario que nos comunique cualquier cambio que se haya producido en su empresa.

En cualquier caso, quedamos a su disposición para cualquier consulta o duda que nos quiera comunicar.

Sin otro particular, reciba un cordial saludo,

Departamento de Consultoría GrupoIWI

Protocolo de privacidad y Protección de Datos

VERSIÓN:

FECHA:

CREADO POR:

APROBADO POR:

NIVEL DECONFIDENCIALIDAD:

HISTORIAL DE CAMBIOS

FECHA	VERSIÓN	CREADA POR	DESCRIPCIÓN DE CAMBIO

INDICE

Tratamiento de los Datos

1 DATOS DEL RESPONSABLE DEL TRATAMIENTO, OBJETO Y ÁMBITO DE APLICACIÓN.

El presente PROTOCOLO DE PROTECCIÓN DE DATOS Y PRIVACIDAD propiedad de

ALAN GÓMEZ DAYOT

en adelante, la entidad, se ha redactado con el objetivo de recoger detalladamente las obligaciones derivadas del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 (RGPD).

CONTENIDO:

- Definición e identificación de las bases de legitimación para el tratamiento de los datos personales.
- Procedimiento para el ejercicio y contestación de los derechos de los interesados.
- Relación entre responsables y encargados del tratamiento, y su correspondientes obligaciones.
- Análisis de Riesgos en los tratamientos de datos personales.
- Registro de actividades de tratamiento de datos personales.
- Análisis de la necesidad de hacer evaluación de impacto.
- Mecanismos para la notificación de las violaciones de seguridad de los datos personales.
- Necesidad de contar con un Delegado de Protección de Datos (cuando sea preceptivo).
- Obligaciones derivadas de las posibles Transferencias Internacionales de Datos, si las hubiere.
- Medidas de seguridad técnicas y organizativas a implantar.

Todo ello de manera estructurada y de forma sistemática y progresiva para una correcta adecuación y seguimiento de las implicaciones en materia de protección de datos, y que deberá estar a disposición de los trabajadores/as de la entidad para su conocimiento y difusión.

2 PRINCIPIOS RELATIVOS AL TRATAMIENTO

La entidad tratará los datos personales, en todo caso, conforme a los principios establecidos por el RGPD.

2.1 LICITUD, LEALTAD Y TRANSPARENCIA.

Los datos son tratados de manera lícita, leal y transparente en relación con el interesado.

2.2 LIMITACIÓN DE LA FINALIDAD.

Los datos son recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

2.3 MINIMIZACIÓN DE LOS DATOS.

Los datos serán los adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que son tratados.

2.4 EXACTITUD.

Los datos serán exactos y, si fuera necesario, serán actualizados. La entidad ha adoptado todas las medidas razonables para suprimir o rectificar sin dilación los datos personales inexactos con respecto a los fines para los que son tratados.

2.5 LIMITACIÓN DEL PLAZO DE CONSERVACIÓN.

La entidad mantendrá los datos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de dichos datos.

2.6 INTEGRIDAD Y CONFIDENCIALIDAD.

Los datos son tratados por la entidad de tal manera que se garantiza una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas y organizativas apropiadas.

3 BASES DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS

La entidad solamente lleva a cabo el tratamiento de datos personales cuando cumple, al menos, una de las siguientes condiciones:

- Consentimiento.
- Relación contractual.
- Interés vital 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.

Por este motivo, la entidad identificará claramente la base legal sobre la que se desarrolla el tratamiento, siendo las principales:

- el consentimiento inequívoco de los afectados, prestado mediante una manifestación clara afirmativa.
- la existencia de una relación contractual entre la entidad y el interesado.

El consentimiento debe ser "inequívoco", definido como aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa. No se admiten formas de consentimiento tácito o por omisión, ya que se basan en la inacción.

El consentimiento será, además, "explícito", en las siguientes situaciones:

- Tratamiento de datos sensibles.
- Adopción de decisiones automatizadas.
- Transferencias internacionales.

Derechos del interesado en el Tratamiento de los Datos

B

4 DERECHOS DE LOS INTERESADOS EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

4.1 TRANSPARENCIA DE LA INFORMACIÓN, COMUNICACIÓN Y MODALIDADES DE EJERCICIO DE LOS DERECHOS DEL INTERESADO.

La entidad ha tomado las medidas oportunas para facilitar al interesado toda la información indicada en los arts. 13 y 14 RGPD, así como cualquier comunicación relativa al ejercicio de los derechos que le reconoce la normativa en protección de datos, de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

La información será facilitada al interesado por escrito o por medio electrónico (si la solicitud se realizó a través de este medio, la contestación se realizará del mismo modo si es posible, a menos que el interesado solicite que se haga de otro modo), incluso verbalmente si así lo solicita, siempre que se demuestre su identidad y, en su caso, de la persona que lo represente. En caso de duda razonable, se solicitará información adicional para confirmar la identidad del interesado y, en su caso, de su representante.

La entidad solamente rechazará la solicitud de ejercicio de derechos realizada en aquellos casos en que pueda demostrar que no está en condiciones de identificar al interesado.

La información derivada de la solicitud del interesado deberá serle facilitada en el plazo de un mes a partir de la recepción de la misma. Teniendo en cuenta la complejidad de lo solicitado y el número de solicitudes, dicho plazo podrá ampliarse otros dos meses. En caso de prórroga, la entidad informará al interesado en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la misma.

Si la entidad no da curso a la solicitud del interesado, deberá informarle en el plazo máximo de un mes desde la recepción de la misma de las razones de su negativa y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

La información facilitada al interesado así como toda comunicación y actuación a que dé lugar el ejercicio de los derechos que le reconoce el RGPD será gratuita.

La entidad podrá ante solicitudes manifiestamente infundadas o excesivas, especialmente por su carácter repetitivo, cobrar un canon razonable en función de los costes administrativos afrontados para dar curso a la solicitud del interesado, o negarse a actuar respecto a la solicitud.

4.2 DERECHO DE INFORMACIÓN.

El derecho a la información se manifiesta en el momento de la obtención de los datos personales al establecer el RGPD la información, ha de facilitarse al interesado en el momento de la obtención de dichos datos y en el caso de que no sea el propio interesado quien los facilite.

La entidad facilitará al interesado la siguiente información en el momento de la obtención de sus datos personales:

• La identidad y los datos de contacto de la entidad responsable del tratamiento y, en su caso, de su representante.

• Los datos de contacto del delegado de protección de datos, en su caso.

• Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.

• Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos de la entidad responsable del mismo o de un tercero, se facilitará información relativa a dichos intereses.

• Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.

• La intención de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión o referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

• El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.

• La existencia del derecho a solicitar el acceso a sus datos personales, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.

• Cuando el tratamiento esté basado en el consentimiento del interesado, la existencia de retirar dicho consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

• El derecho a presentar una reclamación ante una autoridad de control.

• Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitarlos.

• La existencia de decisiones automatizadas, incluida la elaboración de perfiles, e información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Cuando los datos personales no se hayan obtenido directamente del interesado, la entidad deberá también facilitarle información relativa a la fuente de la que proceden dichos datos y, en su caso, si proceden de fuentes de acceso público.

Esta información deberá ser comunicada:

• Dentro de un plazo razonable y a más tardar dentro de un mes, atendiendo a las circunstancias específicas en las que se traten los datos.

• En el momento de la primera comunicación con el interesado.

• O en el momento en que los datos personales sean comunicados por primera vez a un tercero si dicha comunicación estaba prevista.

La entidad facilitará dicha información a los interesados por escrito, incluidos los medios electrónicos cuando sea apropiado.

Como excepción a lo anterior, únicamente no será necesario para la entidad informar cuando el interesado ya disponga de la información, ni tampoco, en el caso de que los datos no procedan del interesado, cuando:

• La comunicación resulte imposible o suponga un esfuerzo desproporcionado

• El registro o la comunicación esté expresamente establecido por el Derecho de la Unión o de los Estados miembros.

• Cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto.

La entidad adaptará a las circunstancias de cada uno de los medios empleados para la recopilación o registro de los datos, el procedimiento para facilitar la información al interesado.

Entre dichos medios se encuentran:

- Cuestionarios o formularios en papel.
- Cuestionarios o formularios web.
- Entrevista telefónica o personal.
- Registro de aplicaciones móviles.
- Monitorización de actividades personales.

Con el objetivo de facilitar la información al interesado de manera concisa y comprensible, la entidad adoptará un modelo de información por capas o niveles atendiendo a las mencionadas circunstancias y medios de recogida de los datos personales.

El enfoque de información multinivel consiste en lo siguiente:

- Presentar una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos.

- Remitir a la información adicional en un segundo nivel, donde se presentarán detalladamente el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y, si se desea, archivo.

4.3 DERECHO DE ACCESO.

El interesado tendrá derecho a saber si la entidad está tratando o no datos personales que le conciernen y, de ser así, derecho de acceso a los mismos.

La entidad dentrá la obligación de facilitarle al interesado la siguiente información:

- los fines del tratamiento.

- las categorías de datos personales de que se trate.

- los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales. En estos últimos casos, se le informará de las garantías adecuadas relativas a la transferencia.

- de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar ese plazo.

- la existencia del derecho a solicitar de la entidad la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento.

- el derecho a presentar una reclamación ante una autoridad de control.

- cuando los datos no se hayan obtenido del interesado, cualquier información disponible sobre su origen.

- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, e información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

La entidad facilitará una copia de los datos personales objeto del tratamiento al interesado, con la facultad de poder cobrar un canon razonable por cualquier otra copia solicitada basado en los costes administrativos.

Dicha copia se facilitará por medio electrónico en un formato de uso común si la solicitud se presentó por estos medios, a menos que el interesado solicite que se le facilite de otro modo.

4.4 DERECHO DE RECTIFICACIÓN.

El interesado podrá solicitar a la entidad la rectificación de los datos personales inexactos que le conciernen, así como completar dichos datos teniendo en cuenta los fines del tratamiento.

La entidad comunicará cualquier rectificación de los datos personales a cada uno de los destinatarios a los que se hayan comunicado dichos datos, en su caso, salvo que sea imposible o exija un esfuerzo desproporcionado.

4.5 DERECHO DE SUPRESIÓN O "DERECHO AL OLVIDO".

La entidad suprimirá sin dilación indebida los datos personales del interesado que así lo solicite cuando se den alguna de las circunstancias siguientes:

- los datos personales ya no sean necesarios para los fines para los que fueron recogidos o tratados de otro modo;

- el interesado retire el consentimiento en el que se basa el tratamiento y este no se base en otro fundamento jurídico;

- el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento;

- los datos personales hayan sido tratados ilícitamente;

- los datos personales deban suprimirse en cumplimiemto de un obligación legal establecida en el Derecho de la Unión o de los Estados miembros aplicable a la entidad responsable del tratamiento;

- los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a niños.

La entidad suprimirá dichos datos cuando los haya hecho públicos adoptando medidas razonables, atendiendo a la tecnología disponible y el coste de su aplicación, con miras a informar a los responsables que estén tratando los datos personales de la solicitud de supresión del interesado de cualquier enlace a esos datos, o cualquier copia de los mismos.

No se procederá a la supresión de los datos cuando el tratamiento sea necesario:

- para ejercer el derecho a la libertad de expresión e información;

- para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros aplicable a la entidad responsable del tratamiento, o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos que le han sido conferidos;

- por razones de interés público en el ámbito de la salud pública;

- con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o para la formulación, el ejercicio o la defensa de reclamaciones.

La entidad comunicará cualquier supresión de datos personales a cada uno de los destinatarios a los que se hayan comunicado dichos datos, en su caso, salvo que sea imposible o exija un esfuerzo desproporcionado.

4.6 DERECHO A LA LIMITACIÓN DEL TRATAMIENTO.

El interesado podrá solicitar a la entidad la limitación del tratamiento de sus datos personales. Dichos datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, ejercicio o defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

- **La limitación se producirá cuando se cumpla alguna de las siguientes condiciones:**

- el interesado impugne la exactitud de los datos personales, durante el plazo necesario para que la entidad verifica la exactitud de los mismos;

- el tratamiento sea lícito y el interesado se oponga a la supresión de los datos personales, solicitando en su lugar la limitación de su uso;

- la entidad ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, ejercicio o defensa de reclamaciones;

• el interesado se oponga al tratamiento, mientras se verifica si los motivos legítimos de la entidad prevalecen sobre los del interesado.

La entidad comunicará cualquier limitación de los datos personales a cada uno de los destinatarios a los que se hayan comunicado dichos datos, en su caso, salvo que sea imposible o exija un esfuerzo desproporcionado y además informará al interesado antes del levantamiento de la limitación de los datos personales cuando ésta haya tenido lugar.

4.7 DERECHO A LA PORTABILIDAD DE LOS DATOS.

La entidad entregará al interesado que lo solicite los datos personales que le haya facilitado, en un formato estructurado, de uso común y lectura mecánica, teniendo derecho a transmitirlos a otro responsable del tratamiento cuando:

• el tratamiento está basado en el consentimiento del interesado o en un contrato en el que el interesado es parte. En este supuesto, el interesado podrá solicitar a la entidad que transmita directamente los datos personales al otro responsable si es técnicamente posible,

• el tratamiento se realice por medios automatizados.

No procederá la portabilidad cuando el tratamiento sea necesario para el cumpliimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a la entidad, ni cuando pueda afectar negativamente a los derechos y libertades de otros.

4.8 DERECHO DE OPOSICIÓN.

El interesado podrá oponerse en cualquier momento al tratamiento de sus datos personales cuando dicho tratamiento se base en:

• el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a la entidad;

• la satisfacción de intereses legítimos perseguidos por la entidad o un tercero.

La entidad procederá al cese del tratamiento de dichos datos salvo que pueda acreditar motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, ejercicio o defensa de reclamaciones.

Cuando el tratamiento tenga por por objeto la realización de actividades de marketing directo, el interesado podrá oponerse en todo momento a dicho tratamiento, incluida la elaboración de perfiles.

4.9 DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS.

El interesado podrá ejercitar ante la entidad su derecho a no ser objeto de decisiones basadas únicamente en tratamientos automatizados, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de forma similar, excepto:

- si la decisión es necesaria para la celebración o la ejecución de un contrato entre el interesado y la entidad,

- si la decisión está autorizada por el Derecho de la Unión o de los Estados miembros que sea aplicable a la entidad y que establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

- si la decisión se basa en el consentimiento explícito del interesado.

En aquellos casos en que no corresponda la negativa del interesado, la entidad adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo, el derecho a obtener la intervención humana en el tratamiento, a expresar su punto de vista y a impugnar la decisión adoptada.

La entidad no tomará decisiones basadas únicamente en el tratamiento automatizado de categorías especiales de datos personales, salvo consentimiento explícito del interesado o que el tratamiento sea necesario por razones de interés público, y siempre que se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los legítimos intereses del interesado.

Obligaciones del responsable del Tratamiento de los Datos

5 RELACIONES ENTRE EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio a la entidad que conlleva el tratamiento de datos personales por cuenta de éste.

Corresponde a la entidad decidir sobre la finalidad y los usos de la información, mientras que el encargado del tratamiento debe cumplir con las instrucciones dadas respecto al correcto tratamiento de los datos personales a los que pueda tener acceso como consecuencia de la prestación de este servicio.

El encargado podrá realizar todos los tratamientos, automatizados o no, que la entidad le haya encomendado formalmente, pudiendo adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado, pero en ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades. Eso sí, en todo caso deberá respetar las instrucciones dadas por la entidad.

5.1 ELECCIÓN DEL ENCARGADO DEL TRATAMIENTO.

La entidad actuará de forma diligente al elegir a un encargado del tratamiento, siendo, en todo caso, aquel que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas conforme a lo establecido por el RGPD, y que garantice la protección de los derechos de las personas afectadas.

La adhesión del encargado del tratamiento a un código de conducta o mecanismo de certificación aprobado conforme a las estipulaciones del RGPD podrá servir para acreditar que ofrece garantías suficientes.

5.2 REGULACIÓN DE LA RELACIÓN ENTRE RESPONSABLE Y ENCARGADO DEL TRATAMIENTO.

La relación entre la entidad y el encargado del tratamiento se regirá por un contrato u otro acto jurídico similar que constará por escrito, inclusive en formato electrónico. Dicho contrato o acuerdo, establecerá, al menos, el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

En particular, deberá contener necesariamente:

POSIBLES TRANSFERENCIAS INTERNACIONALES

Instrucciones documentadas de la entidad para el tratamiento de los datos, incluyendo lo relativo a posibles transferencias internacionales de datos personales a terceros países u organizaciones internacionales, salvo que el encargado esté obligado a realizar dichas transferencias en virtud de una exigencia legal previa.

La entidad identificará de forma clara y concreta qué tratamientos de datos va a realizar el encargado. El encargado informará a la entidad inmediatamente si, en su opinión, alguna instrucción infringe el RGPD o alguna otra norma en materia de protección de datos de la Unión o de los Estados miembros.

GARANTÍAS DE CONFIDENCIALIDAD

Forma en que el encargado del tratamiento garantizará que las personas autorizadas para tratar datos personales se han comprometido, de forma expresa, a respetar la confidencialidad o, en su caso, si están sujetas a una obligación de confidencialidad de naturaleza estatutaria. El cumplimiento de esta obligación debe quedar documentado y a disposición de la entidad.

MEDIDAS DE SEGURIDAD, TÉCNICAS Y ORGANIZATIVAS

Obligación del encargado de adoptar todas las medidas de seguridad necesarias, de conformidad con lo establecido en el RGPD.

La entidad y el encargado deberán evaluar los posibles riesgos derivados del tratamiento para garantizar la seguridad de la información tratada y los derechos de las personas afectadas, teniendo en cuenta los medios utilizados (tecnologías, recursos etc.) y otras circunstancias que puedan incidir en la seguridad, como por ejemplo que el encargado lleve a cabo otros tratamientos.

La entidad y el encargado del tratamiento establecerán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo existente, incluyendo, entre otros:

- la seudonimización y el cifrado de datos personales;
- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico;
- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

POSIBLES SUBENCARGADOS

Autorización de la entidad para que el encargado del tratamiento pueda recurrir a otro encargado (subencargado) para el desarrollo del servicio encomendado, cuando esto conlleve el tratamiento de los datos personas por parte de un tercero.

Esta autorización puede ser específica, identificando al subencargado de forma concreta, o general, autorizando solamente la subcontratación pero sin establecer un subencargado concreto.

En el supuesto que la autorización sea de carácter general, el encargado informará a la entidad de la incorporación o sustitución de un subencargado, dando así a la entidad la oportunidad de oponerse a dichos cambios.

En todo caso, el subencargado del tratamiento estará sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y en la misma forma (acuerdo por escrito o acto jurídico vinculante) que el encargado del tratamiento en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

En caso de incumplimiento por el subencargado, el encargado inicial seguirá siendo plenamente responsable ante la entidad en lo referente al cumplimiento de las obligaciones del subencargado.

COMPROMISO DEL ENCARGADO CON LOS DERECHOS DEL INTERESADO

Forma en la que el encargado del tratamiento, teniendo en cuenta la naturaleza del mismo y siempre que sea posible, asistirá a la entidad en el cumplimento de la obligación de responder a las solicitudes de ejercicio de sus derechos por parte de los interesados establecidos en el RGPD (acceso a datos personales, rectificación, supresión o “derecho al olvido”, limitación del tratamiento, portabilidad de los datos, oposición, a no ser objeto de decisiones individualizadas automatizadas incluida la elaboración de perfiles).

El acuerdo deberá establecer de forma clara si corresponde al encargado del tratamiento atender y dar respuesta a las solicitudes de estos derechos o bien establecer expresamente que su única obligación es comunicar a la entidad que se ha ejercido un derecho.

COMPROMISO DEL ENCARGADO CON LAS MEDIDAS DE SEGURIDAD

Forma en que el encargado ayudará a la entidad a garantizar el cumplimiento de las obligaciones relativas a la aplicación de las medidas de seguridad que correspondan, la notificación de violaciones de datos a las Autoridades de

Protección de Datos, la comunicación de violaciones de datos a los interesados, la realización de las evaluaciones de impacto relativa la protección de datos y, en su caso, la realización de consultas previas, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.

DESTINO DE LOS DATOS AL FINALIZAR EL SERVICIO

Destino de los datos al finalizar la prestación, es decir, se establecerá si, una vez finalizada la prestación del servicios, el encargado del tratamiento procederá a su supresión o a la devolución de los datos personales y de cualquier copia existente, ya sea a la entidad o a otro encargado designado por la misma, así como la forma y el plazo en que el encargado debe proceder. En todo caso, si la entidad está obligada a la conservación de los datos por alguna norma del Derecho de la Unión o de los Estados miembros, éstos le deberán ser devueltos por el encargado. No obstante, el encargado del tratamiento puede conservar una copia de los mismos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación del servicio.

PROTOCOLO DE CUMPLIMIENTO RGPD

Forma en que el encargado del tratamiento pondrá a disposición de la entidad toda la información necesaria para demostrar el cumplimiento de las obligaciones recogidas en el contrato o acuerdo de encargo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte de la entidad o de un auditor autorizado por ella.

El encargado del tratamiento podrá adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio contratado dentro del marco fijado por las instrucciones dadas por la entidad, pero en ningún caso podrá variar las finalidades y los usos de los datos ni podrá utilizar dichos datos para sus propias finalidades.

6 MEDIDAS DE RESPONSABILIDAD ACTIVA

La entidad aplica las medidas técnicas y organizativas apropiadas para garantizar que los tratamientos de datos personales llevados a cabo son conformes con el RGPD. Dichas medidas tendrán en todo momento en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de los interesados.

6.1 PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO.

La entidad aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos que entraña el mismo para los derechos y libertades de las personas físicas, con el objetivo de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias para cumplir con los requisitos del RGPD y proteger los derechos de los interesados.

De igual modo, aplicará las medidas técnicas y organizativas apropiadas para garantizar que solamente sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento. La entidad tomará las mismas precauciones en cuanto a la cantidad de datos recogidos, la extensión de su tratamiento, su plazo de conservación y a su accesibilidad.

Las medidas aplicadas para garantizar un nivel de seguridad adecuado al riesgo incluirán, en su caso, entre otros:

- la seudonimización y el cifrado de datos personales;

- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

- la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

6.2 REGISTRO DE ACTIVIDADES DE TRATAMIENTO.

La entidad se encuentra en proceso de recogida y analisis de los datos para el diseño de su registro de las actividades de tratamiento.

Dicho registro contendrá la siguiente información:

- Nombre y datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos, si existiese.

- Finalidad del tratamiento.

- Descripción de las categorías de interesados y de las categorías de datos personales.

- Categorías de destinatarios a quienes se han comunicado o comunicarán los datos personales.

- En su caso, las transferencias de datos personales a un tercer país o a una organización internacional y, en su caso, la documentación de las garantías adecuadas adoptadas para la protección de dichos datos.

- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad aplicadas

En los casos en que la entidad actúe como encargada del tratamiento, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contendrá:

- nombre y datos de contacto del encargado/s y de cada responsable por cuenta del cual actúa la entidad y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos, si existiese;

- categorías de tratamientos efectuados por cuenta de cada responsable;

- en su caso, las transferencias de datos personales a un tercer país u organización internacional y, en su caso, la documentación de las garantías adecuadas adoptadas para la protección de los datos personales;

6.3 ANÁLISIS DE RIESGO

La entidad llevará a cabo una valoración del riesgo con carácter previo a todo nuevo tratamiento con el fin de establecer las medidas de seguridad adecuadas para garantizar los derechos y libertades de los interesados afectados por dicho tratamiento.

Este análisis de riesgo variará en función del:

- Los tipos de tratamiento.
- La naturaleza de los datos.
- El número de interesados afectados.
- La cantidad y variedad de tratamientos llevados a cabo.

Para un adecuado diseño de las actividades de tratamiento de la entidad, se tendrán en cuenta las siguientes consideraciones:

Gestión de riesgos :

- **Identificar amenazas y riesgos,** entendiendo por amenaza cualquier riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento.

- **Evaluar los riesgos**, es decir, valorar el impacto de la exposición a la amenaza, junto con la probabilidad de que esta se materialice, determinándose el impacto en base a los posibles daños que se pueden producir si la amenaza se materializa.

- **Tratar los riesgos** con el objetivo de disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen.

Los principales riesgos para los derechos y libertades de las personas físicas se pueden diferenciar en 2 dimensiones:

- Riesgos asociados a la protección de la información, pudiendo categorizar las amenazas en 3 tipos:

  - Acceso ilegítimo a los datos, es decir, violación de la confidencialidad.

  - Modificación no autorizada de los datos, por tanto, se pone en riesgo la integridad de los mismos.

- Eliminación de los datos, afectando a su disponibilidad.

• Riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados.

Dada la variabilidad de los riesgos, la entidad dispone de una descripción detallada de los tratamientos que lleva a cabo, de su contexto y de los elementos más relevantes que intervienen en los mismos con el fin de revisar el análisis de riesgo ante cualquier variación en dichos tratamientos que pueda derivar en la aparición de nuevos riesgos.

6.4 EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

La entidad llevará a cabo una evaluación previa del impacto de las operaciones de tratamiento que vaya a iniciar, cuando sea probable que dicho tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas en base a su naturaleza, alcance, contexto o fines, con el objetivo de determinar, en su caso, la viabilidad o no del tratamiento, y las medidas de control más adecuadas para reducir el nivel de riesgo entrañado hasta un nivel considerado aceptable.

La obligación de realizar una evaluación de impacto corresponde a la entidad, con el asesoramiento del Delegado de Protección de Datos, si ha sido nombrado.

Se requerirá, especialmente, realizar una evaluación de impacto en caso de:

• Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

• Tratamiento a gran escala de categorías especiales de datos o de datos personales relativos a condenas e infracciones penales; o

• Observación sistemática a gran escala de una zona de acceso público.

La evaluación deberá contener como mínimo:

• Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento;

• Una evaluación de la necesidad la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

• Una evaluación de los riesgos para los derechos y libertades de los interesados;

• Las medidas previstas para afrontar los riesgos, incluidas las garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales.

Si de la evaluación de impacto llevada a cabo por la entidad, se determina que la operación de tratamiento presenta un riesgo residual, es decir, el riesgo una vez que se han aplicado las medidas de control para mitigar y/o reducir el impacto asociado a dicho riesgo, es alto o muy alto, realizará una consulta a la autoridad de control que deberá incluir:

• Las responsabilidades respectivas de la entidad, los corresponsables y los encargado del tratamiento implicados en el tratamiento, en su caso;

• Las medidas y garantías establecidas para proteger los derechos y libertades de los interesados;

• Los datos de contacto del Delegado de Protección de Datos, si ha sido nombrado;

• Cualquier otra información que solicite la autoridad de control.

En función de la resolución a la que llegue la autoridad de control, establecerá las condiciones y medidas que se deben aplicar para llevar a cabo el tratamiento o, en su caso, que no se podrá llevar a cabo.

6.5 NOTIFICACIÓN DE UNA VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES.

En caso de violación de la seguridad de los datos, la entidad la notificará a la autoridad de control competente a más tardar en 72 horas desde que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si dicha notificación no se produce en ese plazo de 72 horas, se indicarán los motivos de la dilación.

Contenido mínimo de la comunicación:

• Descripción de la naturaleza de la violación de la seguridad de los datos personales, indicando si es posible, las categorías y el número aproximado de interesados y registros de datos personales afectados;

• Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en que se pueda obtener más información;

• Descripción de las posibles consecuencias de la violación de la seguridad de los datos;

• Descripción de las medidas adoptadas o propuestas por la entidad para remediar dicha violación, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos provocados por la misma.

La entidad documentará cualquier violación de la seguridad de los datos personales, relatando los hechos relacionados con la misma, así como sus efectos y las medidas correctivas adoptadas, quedando dicha documentación a disposición de la autoridad de control competente.

• En el supuesto de que la violación de la seguridad de los datos pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, la entidad la comunicará a los interesados afectados. Dicha comunicación describirá de forma clara y sencilla la naturaleza de la violación de la seguridad producida y contendrá, como mínimo:

• Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en que se pueda obtener más información;

• Descripción de las posibles consecuencias de la violación de la seguridad de los datos;

• Descripción de las medidas adoptadas o propuestas por la entidad para remediar dicha violación, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos provocados por la misma.

La comunicación al interesado no será necesaria si se cumple algunas de las siguientes condiciones:

• La entidad ha aplicado medidas de protección técnicas y organizativas apropiadas

a los datos personales afectados por la violación de la seguridad de los datos personales, especialmente aquellas que hagan ininteligibles los datos personales para cualquier personas no autorizada a acceder a ellos;

• La entidad ha adoptado medidas ulteriores que garantizan que ya no existe la probabilidad de que se concretice un alto riesgo para los derechos y libertades del interesado;

• La comunicación supone un esfuerzo desproporcionado para la entidad, pudiendo optarse por una comunicación pública o similar para informar a los interesados.

Otras consideraciones acerca del Tratamiento de los Datos

D

7 TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

La entidad sólo transmitirá datos personales a aquellos países, territorios, sectores u organismos internacionales respecto de los que la Comisión Europea haya considerado que disponen de un nivel adecuado de protección o aporten garantías suficientes o se den algunas de las circunstancias previstas como excepciones, y siempre y cuando se observen los demás requisitos del RGPD.

Por tanto, el RGPD establece un régimen basado en:

• Transferencias basadas en una decisión de adecuación por parte de la Comisión.

• Transferencias basadas en la adopción de garantías adecuadas.

- Dichas garantías podrán ser aportadas, si necesidad de autorización expresa de una autoridad de control, por:

  • un instrumento jurídicamente vinculante y exigible entre las autoridades y organismos públicos;

  • normas corporativas vinculantes aprobadas por la autoridad de control competente;

  • cláusulas tipo de protección de datos adoptadas por la Comisión;

  • un código de conducta o mecanismo de certificación aprobado conforme al RGPD, junto con compromisos vinculantes y exigibles al responsable o al encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados.

- En caso de contar con autorización por parte de la autoridad de control competente, estas garantías podrán ser aportadas mediantes cláusulas contractuales la entidad y el encargado del tratamiento y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o mediantes disposiciones incorporadas en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

• **Excepciones para situaciones específicas:**

- Consentimiento explícito del interesado a la transferencia propuesta tras haber sido informado de los posibles riesgos para él de dicha transferencia al no existir una decisión de adecuación por parte de la Comisión y de garantías adecuadas;

- Necesidad de la transferencia para la ejecución de un contrato celebrado entre el interesado y la entidad o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

- Necesidad de la transferencia para la celebración o ejecución de un contrato, en interés del interesado, entra la entidad y otra personas física o jurídica;

- La transferencia sea necesaria por razones de interés público;

- Necesidad de la transferencia para la formulación, ejercicio o defensa de reclamaciones;

- Necesidad de la transferencia para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para prestar su consentimiento;

- Cuando la transferencia sea realizada desde un registro público cuyo objeto sea facilitar información al público y está abierto a consulta pública o de cualquier personas que acredite un interés legítimo, conforme a lo establecido por el Derecho de la Unión o de los Estados miembros.

8 REGIMEN SANCIONADOR EN MATERIA DE PROTECCIÓN DE DATOS

Las autoridades de control impondrán multas administrativas por las infracciones del RGPD, en función de las circunstancias de cada caso individual y debiendo tener en cuenta para la imposición de dicha multa y de su cuantía:

- la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de daños y perjuicios ocasionados;

- la adopción de medidas por parte de la entidad o del encargado del tratamiento para paliar los daños sufridos por los interesados;

- el grado de responsabilidad de la entidad o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas aplicadas;

- toda infracción anterior cometida por la entidad o el encargado del tratamiento;

- el grado de cooperación con la autoridad de control para remediar la infracción y mitigar las consecuencias negativas de la misma;

- las categorías de datos personales afectados;

- la forma en que la autoridad de control tuvo conocimiento de la infracción, especialmente si fue la entidad o el encargado del tratamiento quien la comunicó;

- si la entidad o el encargado del tratamiento han cumplido con las medidas correctivas previas impuestas por la autoridad de control, en su caso;

- la adhesión a códigos de conducta o a mecanismos de certificación;

- cualquier otro agravante o atenuante aplicable al caso.

Se sancionarán con **multas administrativas de 10.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior**, optándose por la de mayor cuantía, las infracciones de las disposiciones siguientes:

- las obligaciones del responsable y del encargado aplicables al consentimiento del menor en relación con los servicios de la sociedad de la información; tratamientos que no requieren identificación; la protección de datos desde el diseño; a los

corresponsables del tratamiento; a representantes de los responsables del tratamiento no establecidos en la UE; a los tratamientos bajo la autoridad del responsable y del encargado del tratamiento; al registro de las actividades del tratamiento; a la cooperación con la autoridad de control; a la seguridad del tratamiento; a la notificación de una violación de seguridad a la autoridad de control y comunicación de una violación de seguridad al interesado; a la evaluación de impacto relativa a la protección de datos; a las consultas previas; a la figura del delegado de protección de datos;

• las obligaciones del responsable y del encargado sobre la certificación y los organismos de certificación;

• las obligaciones de los organismos de certificación;

• las obligaciones de la autoridad de control sobre la supervisión de los códigos de conducta aprobados.

Se sancionarán con **multas administrativas de 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio anual global del ejercicio financiero anterior,** optándose por la de mayor cuantía, las infracciones de las disposiciones siguientes:

• los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento, la licitud del tratamiento y el tratamiento de categorías especiales de datos personales;

• los derechos de los interesados;

• las transferencias de datos personales a un destinatario en un tercer país o a una organización internacional;

• toda obligación en virtud del Derecho de los Estados miembros que se adopten en relación a situaciones específicas de tratamiento;

• el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control o el no facilitar su acceso a los locales del responsable y del encargado, incluidos sus equipos y medios de tratamiento de datos.

La imposición de las multas administrativas serán en cada caso individual efectivas, proporcionadas y disuasorias.

Además, las autoridades de control tienen la potestad de imponer las siguientes **acciones correctivas de forma adicional o como sustitución de la multa administrativa:**

• sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas pueda infringir el RGPD;

• sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido el RGPD;

• ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado;

• ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a lo dispuesto en el RGPD, cuando proceda, de una determinada manera y dentro de un plazo especificado;

• ordenar al responsable del tratamiento que comunique al interesado las violaciones de seguridad de los datos personales;

• imponer una limitación temporal o definitiva del tratamiento, incluso su prohibición;

• ordenar la rectificación o supresión de datos personales o la limitación de su tratamiento así como la notificación de dichas medidas a los destinatarios a quienes se hallan comunicados dichos datos;

• retirar una certificación u ordenar al organismo certificador que la retire, u ordenar que no la emita;

• ordenar la suspensión de los flujos de datos personales hacia un destinatario situado en un tercer país o hacia una organización internacional.

9 VIDEO-VIGILANCIA

La normativa en protección de datos define “dato personal” como toda información sobre una persona física identificada o identificable, considerándose como tal a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

En base a esta definición, los principios vigentes en la materia deben aplicarse a las imágenes de personas físicas identificadas o identificables, captadas y/o registradas por cámaras, videocámaras o cualquier otro medio técnico análogo, ya sea con fines de vigilancia u otros en los supuestos en que exista grabación, captación, transmisión, conservación, o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real o un tratamiento que resulte de los datos personales relacionados con aquéllas.

9.1 IMÁGENES EXCLUIDAS DE LA APLICACIÓN DEL RGPD.

Existen casos en los que no se aplican los principios de protección de datos:

- Al tratamiento de imágenes en el ámbito personal y doméstico, entendido como el que realiza una persona física en el marco de una actividad exclusivamente privada o familiar. Por ejemplo, fotos o grabaciones tomadas durante una celebración familiar o un viaje turístico.

- Al tratamiento de imágenes tratadas por los medios de comunicación en el ejercicio legítimo de los derechos que les confiere el art. 20 de la Constitución Española.

Sin perjuicio de las previsiones específicas de la Ley Orgánica 4/1997, de 4 de agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado en lugares públicos, a estos tratamientos se les aplica supletoriamente la normativa en protección de datos.

9.2 PRINCIPIOS BÁSICOS APLICABLES AL TRATAMIENTO DE IMÁGENES.

La videovigilancia puede propiciar una violación de los derechos a la intimidad, el honor y la propia imagen garantizados por el artículo 18 de nuestra Constitución además del

incumplimiento de las políticas de protección de datos de carácter personal. Por ello, el responsable tendrá que tener en cuenta los siguientes principios:

• La videovigilancia sólo debe utilizarse cuando no sea posible acudir a otros medios que causen menos impacto en la privacidad, debiendo valorarse si existe proporcionalidad entre la finalidad que se persigue y el uso de videocámaras.

• No se podrán obtener imágenes de espacios públicos, actividad que está reservada a las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus funciones, salvo imágenes parciales y limitadas que resulten imprescindibles para la vigilancia o sea imposible evitarlo por la ubicación de las cámaras. En cualquier caso, el uso de sistemas de videovigilancia deberá ser respetuoso con los derechos de las personas y el resto del Ordenamiento jurídico por lo que no podrán obtenerse imágenes en el interior de viviendas cercanas, baños, vestuarios o lugares análogos, ni de espacios ajenos al específicamente protegido por la instalación.

• El tratamiento de las imágenes será lícito, leal y transparente en relación con el interesado.

• Las imágenes serán recogidas con fines determinados, explícitos y legítimos, y no serán tratadas ulteriormente de manera incompatible con dichos fines.

• Las imágenes captadas serán las adecuadas, pertinentes y limitadas a lo necesario con los fines para los que son tratadas.

• Las imágenes se mantendrán durante no más tiempo del necesario para los fines del tratamiento, por lo que serán suprimidas en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservadas para acreditar la comisión de actos que atenten con la integridad de personas, bienes o instalaciones.

• Las imágenes serán tratadas de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

9.3 OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO.

DEBER DE INFORMACIÓN.

La información en la recogida de los datos es un elemento esencial del derecho a la protección de datos y por tanto su cumplimiento resulta ineludible. En todos los casos se deberá de informar de la existencia de un sistema de videovigilancia, tanto si permite la grabación o almacenamiento de las imágenes como si no. Dicha información se

facilitará mediante la colocación de carteles suficientemente visibles en los accesos a las zonas vigiladas, sean éstos exteriores o interiores, indicando, al menos, la existencia del tratamiento, quién es el responsable del mismo y la posibilidad de ejercitar los derechos que prevé la normativa de protección de datos. Si el lugar vigilado dispone de varios accesos habrá de colocarse en cada uno de ellos el cartel informativo para que la información sea visible con independencia de por donde se acceda.

SEGURIDAD.

El sistema de videovigilancia deberá cumplir con aquellas medidas de seguridad que resulten adecuadas para evitar la alteración, pérdida, tratamiento o accesos no autorizados. La utilización de cámaras orientables y/o con zoom, requerirá la instalación de máscaras de privacidad para evitar la captación de imágenes de espacios públicos y de propiedad de terceros. El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido, teniendo acceso a las imágenes sólo el personal autorizado, el cual habrá sido informado, previamente, por el responsable del fichero sobre sus obligaciones de seguridad y su deber de secreto. El acceso a las imágenes grabadas se restringirá con un código de usuario y una contraseña o cualquier otro medio que garantice la identificación y autenticación unívoca.

DERECHO DE ACCESO A LAS IMÁGENES CON INFORMACIÓN PERSONAL.

El ejercicio del derecho de acceso requerirá la presentación de una imagen actualizada del interesado para que el responsable del tratamiento verifique su presencia en el fichero. El acceso debe realizarse sin afectar a los derecho de terceros que también puedan aparecer en las imágenes, por lo que el responsable facilitará únicamente la información imprescindible para dar respuesta al derecho ejercitado.

9.4 ACCESO A LAS IMÁGENES POR PARTE DE TERCEROS.

La instalación de un sistema de videovigilancia puede dar lugar a dos supuestos:

- Instalación y/o mantenimiento técnico de los equipos y sistemas de videovigilancia por parte de una empresa externa sin acceso a las imágenes. En este caso la empresa instaladora no posee la condición de encargada de tratamiento correspondiendo al responsable, que la contrató, la adaptación de la instalación a los requisitos normativos.

- Instalación y/o mantenimiento de los equipos y sistemas de videovigilancia por parte de una empresa externa con utilización de los equipos o acceso a las imágenes. Únicamente en este segundo caso, dicha empresa será considerada encargada del tratamiento.

La existencia de un encargado del tratamiento obliga a la formalización en un contrato o acto jurídico de la relación existente entre encargado y responsable conforme a lo estipulado por el RGPD.

El responsable del tratamiento deberá elegir encargados que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme a la normativa en protección de datos. La misma previsión deberá tenerse presente en los casos de subcontratación por parte del encargado.

La petición de de imágenes por las Fuerzas y Cuerpos de Seguridad se realizará en el marco de actuaciones judiciales o policiales. El requerimiento al titular del fichero será el documento que ampare a este para ceder datos a las mismas o a los Juzgados y Tribunales que los requieran.

9.5 CANCELACIÓN DE OFICIO DE LAS IMÁGENES.

La Instrucción 1/2006 establece en su artículo 6 un plazo de cancelación máximo de un mes desde su captación. En ella se ha seguido el mismo criterio que el fijado en el artículo 8 de la Ley Orgánica 4/1997, de 4 de agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado en lugares públicos.

Por tanto, una vez transcurrido dicho plazo, las imágenes deberán ser canceladas, lo que implica el bloqueo de las mismas, siendo conservadas únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo, deberá procederse a la supresión.

En aquellos casos en los que el responsable constate la grabación de un delito o infracción administrativa que deba ser puesto en conocimiento de una autoridad, y la denuncie, deberá conservar las imágenes a disposición de la citada autoridad.

9.6 SUPUESTOS ESPECÍFICOS.

CÁMARAS CONECTADAS A INTERNET.

Los sistemas de videocámaras IP y Webcams capaces de transmitir las imágenes a través de Internet, comportan una serie de riesgos adicionales si no se configuran adecuadamente, por lo que deberá prestarse especial atención a la configuración del software y verificar que están activadas las funciones de identificación y autenticación evitando así accesos no autorizados a los datos.

Se restringirá el acceso con un código de usuario y una contraseña o cualquier otro medio que garantice la identificación unívoca, que sólo serán conocidos por las personas autorizadas a acceder a las imágenes.

CÁMARAS EN COMUNIDADES DE PROPIETARIOS

La instalación de cámaras en zonas comunes requiere el acuerdo de la Junta de Propietarios y su reflejo en las actas de dicha Junta. Para su aprobación será necesario el voto favorable de las partes del total de los propietarios que, a su vez, representen las partes de las cuotas de participación.

Es aconsejable que en el acuerdo queden reflejadas las características del sistema de videovigilancia, como el número de cámaras o el espacio captado por las mismas.

Las cámaras sólo podrán captar imágenes de las zonas comunes de la Comunidad de Propietarios, por lo que no se podrán captar imágenes de la vía pública a excepción de una franja mínima de los accesos al inmueble. Tampoco se podrán captar imágenes de terrenos y viviendas colindantes o de cualquier otro espacio ajeno a la Comunidad.

El acceso a las imágenes estará restringido a las personas designadas por la Comunidad de Propietarios y en ningún caso estarán accesible mediante canales de televisión comunitarios.

El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido. A las imágenes grabadas accederán tan sólo el personal autorizado, que deberá introducir un código de usuario y una contraseña.

La instalación de cámaras en una plaza de garaje que forme parte del espacio comunitario requerirá autorización previa por parte de la Junta de Propietarios que deberá constar en el Acta correspondiente. Las imágenes captadas por las cámaras se limitarán exclusivamente a la plaza de aparcamiento de las que sea titular el responsable de dichas cámaras y a una franja mínimas de las zonas comunes que no sea posible evitar para la vigilancia de dicha plaza. Las cámaras no captarán imágenes de plazas de aparcamiento ajenas ni de la vía pública, terrenos o viviendas colindantes o de cualquier otro espacio ajeno al responsable del sistema.

CÁMARAS PARA EL CONTROL EMPRESARIAL

El art. 20 del Estatuto de los Trabajadores permite al empresario adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por parte del trabajador de sus obligaciones y deberes laborales, guardando en todo caso la debida consideración a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores con discapacidad.

Los sistemas de videovigilancia para control empresarial tendrán que tener en cuenta la proporcionalidad entre la finalidad perseguida y el modo en que se traten las imágenes y sólo se usarán cuando no exista otra medida más idónea.

Las cámaras solamente captarán imágenes en los espacios indispensables para satisfacer las finalidad de control laboral, respetando en todo caso los derechos a la intimidad, a la propia imagen y a la protección de datos de los trabajadores, no pudiéndose utilizar este tipo de medios en vestuarios, baños, taquillas o zonas de descanso. Tampoco se podrán registrar conversaciones privadas.

En cuanto al deber de información, además de la colocación de carteles en las zonas de videovigiladas, habrá de informarse personalmente a los trabajadores y a la representación sindical, por cualquier medio que garantice la recepción de la información (nunca a través de sus móviles privados o en su dirección particular).

10 GLOSARIO

Las siguientes definiciones le ayudarán a comprender algunos términos utilizados en el presente documento. A efectos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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, se entenderá por:

Datos personales: toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social en dicha persona.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimiento automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Responsable del tratamiento o responsable: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Encargado del tratamiento o encargado: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Destinatario: la persona física o jurídica, autoridad pública, servicio u organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

Tercero: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Violación de la seguridad de los datos personales: toda violación de la 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.

Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicos o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Establecimiento principal:

A. en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal.

B. en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al Reglamento.

Representante: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al art. 27 RGPD, represente al responsable o al encargo en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento..

Empresa: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.

Grupo empresarial: grupo constituido por una empresa que ejercer el control y sus empresas controladas.

Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial, o una unión de empresas dedicadas a una actividad económica conjunta.

Autoridad de control: la autoridad pública independiente establecida por un Estado miembro.

Autoridad de control interesada: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a) el responsable o el encargado del tratamiento esté establecido en el territorio del Estado miembro de esa autoridad de control;

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control.

Tratamiento transfronterizo:

a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

Objeción pertinente y motivada: la objeción a una propuesta de decisión sobre la existencia o no de infracción del Reglamento, o sobre la conformidad con el Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión.

Servicio de la sociedad de la información: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

Organización internacional: una organización internacional y sus entes subordinados en Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

958 41 57 36
info@grupoiwi.com