

CONTRATO DE ACCESO A DATOS DE CARÁCTER PERSONAL

En XXXX, a XX de XXXX de XXXX

REUNIDOS

DE UNA PARTE: D./Dña. XXXX, mayor de edad, con domicilio en XXXX de XXXX, titular del D.N.I. número XXXX.

Y DE LA OTRA: D./Dña. XXXX, mayor de edad, con domicilio en XXXX de XXXX, titular del D.N.I. número XXXX.

INTERVIENEN

El primero en nombre y representación de XXXX [empresa del grupo EDPR], (en lo sucesivo CLIENTE o RESPONSABLE DEL TRATAMIENTO), con C.I.F. XXXX y domicilio en XXXX, según resulta de la escritura de poder otorgada con fecha XX de XXXX de XXXX, ante el Notario de XXXX [ciudad], D./Dña. XXXX, bajo el número XXXX de su protocolo.

El segundo en nombre y representación de XXXX [proveedor], (en lo sucesivo, EMPRESA CONTRATISTA o ENCARGADO DEL TRATAMIENTO), con C.I.F. XXXX y domicilio en XXXX, según resulta de la escritura de poder otorgada con fecha XX de XXXX de XXXX, ante el Notario de XXXX D./Dña. XXXX, bajo el número XXXX de su protocolo.

En lo sucesivo, individualmente cada “**Parte**”, y conjuntamente las “**Partes**”.

Ambas partes reconociéndose capacidad jurídica y de obrar suficiente para el otorgamiento del presente Contrato (en adelante, el “**Contrato**”),

MANIFIESTAN

- I.- Que con fecha de hoy el CLIENTE ha contratado con la EMPRESA CONTRATISTA la prestación de los servicios de XXXX (en adelante, los “Servicios”)
- II.- Que la prestación de los indicados Servicios conlleva un acceso, por parte de la EMPRESA CONTRATISTA, a datos de carácter personal respecto de los que el CLIENTE **es Responsable y Encargado / Responsable / Encargado**. *Nota: antes de imprimir en el caso de que así lo sea habrá que hacer esta mención*
- III.- Que, para regular dicho acceso, ambas Partes acuerdan el otorgamiento del presente Contrato, que se regirá por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (en adelante, RGPD), su normativa de desarrollo y, en especial, por las siguientes

ESTIPULACIONES

PRIMERA.- DEFINICIONES

En el presente contrato, las siguientes expresiones se entenderán, obligarán, contendrán e incluirán todo lo definido en adelante, de acuerdo con el artículo 4 del RGPD.

DATOS DE CARÁCTER PERSONAL: toda información sobre una persona física identificada o identificable.

TRATAMIENTO DE DATOS: Operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos 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.

FICHERO DE DATOS: Conjunto estructurado de datos personales, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

RESPONSABLE DEL TRATAMIENTO: Persona jurídica de naturaleza privada que determine los fines y medios del tratamiento. A efectos del presente contrato, el CLIENTE tendrá la consideración de RESPONSABLE DEL TRATAMIENTO.

ENCARGADO DEL TRATAMIENTO: La persona física o jurídica que trate datos personales por cuenta del RESPONSABLE DEL TRATAMIENTO. A efectos del presente contrato, la EMPRESA CONTRATISTA y aquellas empresas que éste precise subcontratar para el desarrollo de la prestación de los servicios contratados, tendrán la consideración de ENCARGADO DEL TRATAMIENTO.

SEGUNDA.- OBJETO DEL CONTRATO

2.1 El presente Contrato tiene por objeto definir las condiciones conforme a las cuales el Encargado del Tratamiento llevará a cabo el tratamiento de datos personales necesario para la correcta prestación de los Servicios proporcionados al CLIENTE.

2.2 La prestación de los Servicios contratados implica la realización por LA EMPRESA CONTRATISTA de los siguientes tratamientos: 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 de datos personales
Nota: deben suprimirse los que no procedan o añadirse los que correspondan.

2.3 En el caso de que la prestación de Servicios implique la recogida de datos personales, el Encargado del Tratamiento cumplirá el deber de información conforme a las instrucciones que le sean facilitadas por el CLIENTE.

TERCERA .- DURACIÓN

El presente Contrato estará vigente durante todo el tiempo de prestación de los Servicios contratados a que se refiere el Manifiesto I. No obstante lo anterior, ambas Partes acuerdan que las estipulaciones del presente Contrato, con intención expresa o implícita de que continúen en vigor tras el momento de resolución o vencimiento del mismo, se mantendrán en vigor y continuarán vinculando a ambas Partes según lo estipulado.

CUARTA.- FINALIDAD

Los datos personales serán tratados, únicamente, para llevar a cabo la prestación de los Servicios contratados. Si la EMPRESA CONTRATISTA considerase necesario llevar a cabo un tratamiento de los datos con una finalidad distinta, deberá proceder a solicitar previamente la autorización por escrito del CLIENTE. A falta de dicha autorización, la EMPRESA CONTRATISTA no podrá efectuar dicho tratamiento y, en caso de realizarlo incumpliendo las instrucciones del CLIENTE, será considerado como Responsable del Tratamiento.

QUINTA.- DATOS OBJETO DE TRATAMIENTO Y CATEGORÍAS DE INTERESADOS, CRITICIDAD

5.1 Los tipos de datos personales que la EMPRESA CONTRATISTA tratará en virtud de este Contrato son los siguientes (**deben suprimirse los que no procedan o añadirse los que correspondan**):

- Datos identificativos (nombre y apellidos, NIF/DNI, nº Seguridad Social/Mutualidad, dirección, teléfono, firma, huella, imagen/voz, marcas físicas, firma electrónica, otros datos biométricos).
- Datos de características personales (estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas).

- Datos de circunstancias sociales características de alojamiento/vivienda, propiedades o posesiones, aficiones y estilo de vida, pertenencia a clubes o asociaciones, licencias, permisos o autorizaciones).
- Datos académicos y profesionales (formación/titulaciones, historial de estudiante, experiencia profesional, pertenencia a colegios o asociaciones profesionales).
- Datos de detalles de empleo (profesión, puesto de trabajo, datos no económicos de nómina, historial del trabajador).
- Datos de información comercial (actividades o negocios, licencias comerciales, suscripciones a publicaciones o medios de comunicación, creaciones literarias, artísticas, científicas o técnicas).
- Datos económicos, financieros y de seguros (ingresos y rentas, inversiones y bienes patrimoniales, créditos, préstamos y avales, datos bancarios, planes de pensiones y jubilación, datos económicos de nómina, datos de deducciones impositivas e impuestos, seguros, hipotecas, subsidios y beneficios, historial de créditos, tarjeta de crédito).
- Datos de transacciones de bienes y servicios (bienes y servicios suministrados por el interesado, bienes y servicios recibidos por el interesado, transacciones financieras, compensaciones e indemnizaciones).
- Datos de comportamiento (curvas de carga de los consumos, datos de geolocalización o datos de evaluaciones del desempeño).
- Datos de salud o minusvalías.
- Datos de afiliación sindical, religión, creencias o datos relativos a vida sexual.
- Datos biométricos.
- Datos relativos a infracciones penales.

5.2 Las categorías de interesados cuyos datos serán tratados por la EMPRESA CONTRATISTA en virtud de este Contrato son las siguientes **Nota: deben suprimirse los que no procedan o añadirse otros:**

- Clientes.
- Potenciales Clientes.
- Titulares de puntos de suministro
- Proveedores.
- Personas de contacto.
- Empleados.
- Becarios
- Personal de contrata
- Personal de ETT
- Candidatos en procesos de selección de personal.
- Personas cuyas imágenes sean captadas por sistemas de videovigilancia.

- Visitas.

- Otros

5.3. Criticidad del encargado del tratamiento

A fin de determinar las medidas de seguridad exigibles de las recogidas en el Anexo I, así como los mecanismos de supervisión recogidos en el Anexo II a efectos del presente contrato, la EMPRESA CONTRATISTA, es considerada de criticidad **BÁSICA / MEDIA / ALTA** (Nota: deben suprimirse los que no procedan una vez realizado el cuestionario que facilitará EDPR) y utiliza **SISTEMAS PROPIOS DEL ENCARGADO / SISTEMAS DE EDPR** (Nota: deben suprimirse los que no procedan)

SEXTA.-OBLIGACIONES DEL CLIENTE - RESPONSABLE DEL TRATAMIENTO

Para la ejecución del Servicio, el CLIENTE se compromete a poner a disposición de la EMPRESA CONTRATISTA los datos personales y/o la información necesaria para el adecuado tratamiento de los mismos para la correcta prestación de los Servicios.

SÉPTIMA- OBLIGACIONES DE LA EMPRESA CONTRATISTA - ENCARGADO DEL TRATAMIENTO

7.1 La EMPRESA CONTRATISTA se compromete a cumplir las siguientes obligaciones:

- a. Tratar los datos personales, únicamente, para llevar a cabo la prestación de los Servicios contratados, ajustándose a las instrucciones que, en cada momento, le indique, por escrito, el CLIENTE. No obstante, si existiera una normativa que obligase a tratamientos complementarios, la EMPRESA CONTRATISTA informará al CLIENTE de esa exigencia legal, salvo que tal normativa lo prohíba por razones importantes de interés público.
- b. Mantener el deber de secreto respecto a los datos de carácter personal a los que tenga acceso, incluso después de finalizada la relación contractual, así como a garantizar que las personas a su cargo se hayan comprometido por escrito a mantener la confidencialidad de los datos personales tratados.
- c. Garantizar, teniendo en cuenta - el estado de la técnica, - los costes de aplicación, y - la naturaleza, el alcance, el contexto y los fines del tratamiento, - así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, la aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, 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.

Al evaluar la adecuación del nivel de seguridad tendrá particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

En cualquier caso, teniendo en cuenta la tipología de tratamientos a realizar, se dará cumplimiento, como mínimo, a las medidas de seguridad identificadas en el Anexo I del presente Contrato.

d. Guardar bajo su control y custodia los datos personales a los que acceda con motivo de la prestación del Servicio y a no divulgarlos, transferirlos, o de cualquier otra forma comunicarlos, ni siquiera para su conservación a otras personas ajenas al mismo y a la prestación del Servicio objeto del presente Contrato.

No obstante, el CLIENTE podrá autorizar de manera expresa y por escrito a la EMPRESA CONTRATISTA para que recurra a otro Encargado del Tratamiento (en adelante, el "Subcontratista"), cuyos datos identificativos (nombre social completo y NIF) y servicios subcontratados deberán ser comunicados al CLIENTE, antes de la prestación del servicio, con una antelación mínima de un (1) mes. La EMPRESA CONTRATISTA informará del mismo modo al CLIENTE de cualquier cambio previsto en la incorporación o sustitución de los Subcontratistas, dando así al responsable la oportunidad de oponerse a dichos cambios.

En caso de hacer uso de la facultad reconocida en el párrafo anterior la EMPRESA CONTRATISTA queda obligada a trasladar y comunicar al Subcontratista el conjunto de las obligaciones que para el Encargado del Tratamiento se derivan del presente Contrato y, en particular, la prestación de garantías suficientes de que aplicará medidas técnicas y organizativas apropiadas, de manera que el tratamiento se realice conforme con la normativa aplicable.

En cualquier caso, queda autorizado el acceso a los datos que realicen las personas físicas que presten sus servicios a la EMPRESA CONTRATISTA actuando dentro del marco organizativo de ésta en virtud de una relación mercantil y no laboral. Asimismo, queda autorizado el acceso a los datos a las empresas y profesionales que la EMPRESA CONTRATISTA tenga contratados en su ámbito organizativo interno para que le presten servicios generales o de mantenimiento (servicios informáticos, asesoramiento, auditorías, etc.), siempre que dichas tareas no hayan sido concertadas por la EMPRESA CONTRATISTA con la finalidad de subcontratar con un tercero todo o parte de los Servicios que presta al CLIENTE.

e. Suprimir o devolver al CLIENTE, a su elección, todos los datos personales a los que haya tenido acceso para prestar el Servicio. Asimismo, la EMPRESA CONTRATISTA se obliga a suprimir las copias existentes, a menos que exista una norma jurídica que exija la conservación de los datos personales. No obstante, la EMPRESA CONTRATISTA podrá conservar los datos, debidamente bloqueados, en tanto pudieran derivarse responsabilidades de su relación con el CLIENTE.

f. Notificar, sin dilación indebida y en el plazo máximo de veinticuatro (24) horas, al CLIENTE las violaciones de la seguridad de los datos personales de las que tenga conocimiento, dándole apoyo en la notificación a la Agencia Española de Protección de Datos u otra Autoridad de Control competente, y en su caso, a los interesados de las violaciones de seguridad que se produzcan, así como a darle apoyo, cuando sea necesario, en la realización de evaluaciones de impacto de privacidad y en la consulta previa a la Agencia Española de Protección de Datos, cuando proceda, así como asistir al CLIENTE para que éste pueda cumplir con la obligación de dar respuesta a las solicitudes de ejercicio de derechos.

Estas notificaciones deberán comprender, como mínimo, la siguiente información:

- Descripción de la naturaleza de la violación de seguridad: categorías y número aproximado de los titulares afectados, así como de los registros afectados
- Identificación de las personas encargadas de protección de datos
- Descripción de las consecuencias
- Descripción de las medidas adoptadas o propuestas por la EMPRESA CONTRATISTA para reparar la violación de seguridad

Esta información podrá ser facilitada de forma simultánea o a medida que se vaya teniendo conocimiento de la misma.

g. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del CLIENTE.

h. Cooperar con la Agencia Española de Protección de Datos u otra Autoridad de Control, a solicitud de ésta, en el cumplimiento de sus atribuciones.

i. Poner a disposición del CLIENTE toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en este Contrato y para permitir y contribuir a la realización de auditorías, incluidas las inspecciones, por parte del CLIENTE o un tercero autorizado por él. La falta de acreditación de que la EMPRESA CONTRATISTA esté cumpliendo correctamente las obligaciones asumidas en este Contrato, será causa de resolución del mismo.

OCTAVA.- RESPONSABILIDADES Y GARANTÍAS

8.1 Si la EMPRESA CONTRATISTA o cualquiera de sus Subcontratistas infringe el presente Contrato o alguna normativa al determinar los fines y medios del tratamiento, será considerado responsable de dicho tratamiento, asumiendo todas las responsabilidades directas e indirectas que pudieran derivarse para EDPR motivado por dicho incumplimiento por parte del encargado del tratamiento.

8.2 Así mismo, ambas Partes convienen que el incumplimiento de estas obligaciones tiene la condición de causa de resolución del Contrato, por lo que su incumplimiento por la EMPRESA CONTRATISTA, las personas a su cargo o las que intervengan en la prestación de los servicios en nombre o a instancia del mismo, facultará al CLIENTE para resolver el mismo y dará lugar a la correspondiente indemnización de daños y perjuicios por incumplimiento de las obligaciones contractuales.

8.3 Por último, y adicionalmente a lo anteriormente expuesto, en caso de incumplimiento o cumplimiento defectuoso de estas obligaciones por parte de la EMPRESA CONTRATISTA, y sin perjuicio de la posibilidad de resolver el presente Contrato por el CLIENTE y la indemnización por los daños y perjuicios que se le hubiesen causado, la EMPRESA CONTRATISTA vendrá obligada a abonar al CLIENTE, en concepto de cláusula penal, la cantidad correspondiente al 2% del importe del contrato de servicios al que está vinculado el presente contrato de tratamiento de datos.

NOVENA.- DATOS DE LOS INTERVINIENTES

Los datos personales incluidos en este Contrato y aquellos otros intercambiados entre las Partes para posibilitar la prestación de los Servicios serán tratados por la otra Parte con la finalidad de permitir el desarrollo, cumplimiento y control de la relación de prestación de Servicios concertada, siendo la base del tratamiento el cumplimiento de la relación contractual conservándose los datos durante todo el tiempo en que esta subsista y aún después, hasta que prescriban las eventuales responsabilidades derivadas de ella. Las partes se comprometen a trasladar a los titulares de los datos facilitados esta información, así como a indicarles que podrán dirigirse por escrito a los respectivos domicilios señalados en el encabezamiento del presente Contrato para ejercitar sus derechos de acceso, rectificación, oposición, supresión, limitación y portabilidad.

DÉCIMA.- EJERCICIO DE DERECHOS POR PARTE DE LOS INTERESADOS

La EMPRESA CONTRATISTA trasladará al CLIENTE, cualquier solicitud de ejercicio de derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad que hubiese recibido por parte de los interesados cuyos datos sean objeto de tratamiento en el marco de la prestación del servicio, a fin de que sea resuelta por el CLIENTE.

Dicho traslado deberá ser inmediato, de forma que permita al CLIENTE respetar los plazos legalmente establecidos de atención al ejercicio de sus derechos por parte de los interesados, asumiendo la EMPRESA CONTRATISTA la responsabilidad que se pueda derivar del incumplimiento de dichos plazos por causa imputable a la falta o tardanza en su comunicación al CLIENTE.

UNDÉCIMA.- CONTRAPRESTACIÓN

La contraprestación por los servicios prestados se integra en los pactos y condiciones suscritos por las partes en el correspondiente contrato de arrendamiento de servicios.



DUODÉCIMA.- ACUERDO COMPLETO

Este Contrato contiene todas las condiciones convenidas por las partes con relación al objeto del mismo y se considerarán como inexistentes cualesquiera declaraciones, compromisos o promesas, verbales, escritas o implícitas, resultantes de las negociaciones entre las Partes anteriores a este contrato con relación al objeto del mismo.

El hecho de que cualquiera de las partes no exija en un momento determinado el respeto de alguna de las condiciones establecidas en este contrato, no puede ser interpretado por la otra como la renuncia a exigir ulteriormente su cumplimiento.

DECIMOTERCERA.- MODIFICACIONES AL CONTRATO

Las modificaciones a este contrato deberán realizarse de mutuo acuerdo entre la EMPRESA CONTRATISTA y el CLIENTE. A tal efecto, la parte que proponga la modificación solicitará la conformidad escrita de la otra parte con al menos quince (15) días de antelación a la fecha efectiva de modificación, debiendo esta última dar su contestación por escrito, dentro de los QUINCE (15) DIAS siguientes a la recepción de la solicitud. La falta de contestación a la solicitud de modificación o la contestación fuera del plazo previsto para hacerlo, se entenderá como una no-aceptación a la misma.

DECIMOCUARTA.- EFECTOS DE LA TERMINACIÓN

Una vez concluida la prestación de servicios, la EMPRESA CONTRATISTA y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, deberán destruir o devolver los datos de carácter personal al CLIENTE, de acuerdo con sus instrucciones, así como cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá a la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberán ser necesariamente devueltos al CLIENTE.

Los datos únicamente podrán ser conservados por la EMPRESA CONTRATISTA durante el periodo en que pudiera derivarse alguna responsabilidad de la relación establecida con el CLIENTE mediante el presente contrato. En ese caso los datos serán conservados por la EMPRESA CONTRATISTA debidamente bloqueados, para lo que informará al CLIENTE del sistema de bloqueo empleado.

En los supuestos de resolución, denuncia o rescisión, con independencia de los motivos en los que tenga origen, la EMPRESA CONTRATISTA dejará de prestar los servicios objeto del presente contrato con carácter inmediato a la extinción del presente contrato, manteniéndose las obligaciones de confidencialidad establecidas en este contrato con carácter indefinido y en vigor, incluso con posterioridad a la finalización por cualquier causa de la relación mercantil entre las partes.

DECIMOQUINTA.- NOTIFICACIONES

Todas las notificaciones y comunicaciones que deban hacerse bajo el presente contrato tales como avisos, consentimientos, autorizaciones, aprobaciones y nuevas instrucciones del CLIENTE, se harán por escrito, siendo inicialmente válido el envío mediante fax, telegrama, e-mail, correo certificado o mensajero, a las direcciones establecidas seguidamente.

EMPRESA CONTRATISTA / ENCARGADO DEL TRATAMIENTO:

- D./Dña. **XXXX**
- Dirección: **XXXX**
- Teléfono: **XXXX** Fax: **XXXX**

CLIENTE / RESPONSABLE:

- D./Dña. **XXXXX**
- Dirección: **XXXX**
- Teléfono: **XXXX** Fax: **XXXX**

Cualquiera de las partes puede cambiar tales señas o datos mediante notificación escrita a la otra con al menos quince (15) días de antelación a la fecha efectiva del cambio.

DECIMOSEXTA.- NULIDAD Y ANULABILIDAD

En el supuesto de que cualquier cláusula de este contrato resulte anulable o nula, en su totalidad o en parte, esta nulidad o anulabilidad no afectará a la validez de otras cláusulas del mismo, las cuales permanecerán con plena eficacia y validez, salvo que la parte que alegue su nulidad o anulabilidad pruebe que sin la cláusula que resultare nula o anulable no podrán cumplirse los fines perseguidos por el presente contrato.

DECIMOSÉPTIMA.- LEGISLACIÓN APLICABLE

El presente Contrato se regirá de acuerdo con la normativa española y europea en materia de Protección de Datos de Carácter Personal, así como las resoluciones y directrices de la Agencia Española de Protección de Datos y otros organismos competentes en la materia. Para dirimir cualquier discrepancia con respecto a la interpretación y/o ejecución de lo establecido en el presente Contrato, ambas Partes se someten a la jurisdicción de los Juzgados y Tribunales de Oviedo, con renuncia expresa de cualquier otra legislación o fuero que les pudiera corresponder.

En prueba de conformidad con lo anterior, las partes firman el presente contrato en dos ejemplares a un solo efecto, en el lugar y la fecha arriba indicados.

Por la EMPRESA CONTRATISTA

Por el CLIENTE

Fdo: XXXX

Fdo: XXXX

ANEXO I

| Nivel de criticidad de la empresa contratista | Medidas de Seguridad previstas contractualmente (clausulado o instrucciones documentadas adicionales) | |
|---|--|---|
| Básico | Medidas técnicas y organizativas necesarias de conformidad con el RGPD, asegurando, concretamente, un nivel de seguridad adecuado al riesgo | |
| Medio | <u>1. Medidas de seguridad generales:</u> | |
| | Utilización de Sistemas Propios del Encargado del tratamiento | Utilización de Sistemas de EDPR |
| | <ul style="list-style-type: none"> • Identificación, difusión y documentación de las funciones y obligaciones del personal con acceso a los datos. • Llevar, por escrito, un registro de todas las actividades de tratamiento efectuadas por cuenta de EDPR, conforme con los requisitos del RGPD. • Mantenimiento de un registro interno que garantice que las personas a su cargo se hayan comprometido por escrito a mantener la confidencialidad de los datos personales tratados, que conocen las reglas y procedimientos que deben ser adoptados y de participación en acciones de formación sobre esta materia. • Definición e implantación de un procedimiento identificación y autenticación de los usuarios. • Definición e implantación de un procedimiento de control de acceso a los datos. • Definición e implantación de un procedimiento de registro de incidencias. • Definición e implantación de un procedimiento de copias de respaldo. • Implantación de un procedimiento de inventariado y control de entrada y salida de soportes y documentos. • Definición de los criterios de archivo de soportes y los dispositivos para su almacenamiento. • Definición e implantación de controles periódicos de Seguridad para probar, evaluar y valorar regularmente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. • Nombramiento de un responsable o responsables de seguridad o, en su caso, Data Protection Officer. • Definición e implantación de controles de acceso físico. • Definición e implantación de un plan de continuidad del servicio. • Definición e implantación de un procedimiento de seudonimización de los datos personales en los casos que sea técnicamente posible | <ul style="list-style-type: none"> • Identificación, difusión y documentación de las funciones y obligaciones del personal con acceso a los datos. • Llevar, por escrito, un registro de todas las actividades de tratamiento efectuadas por cuenta de EDPR, conforme con los requisitos del RGPD. • Mantenimiento de un registro interno que garantice que las personas a su cargo se hayan comprometido por escrito a mantener la confidencialidad de los datos personales tratados, que conocen las reglas y procedimientos que deben ser adoptados y de participación en acciones de formación sobre esta materia. • Definición e implantación de un procedimiento de registro de incidencias. • Implantación de un procedimiento de inventariado y control de entrada y salida de soportes y documentos. • Definición de los criterios de archivo de soportes y los dispositivos para su almacenamiento. • Nombramiento de un responsable o responsable de seguridad o, en su caso, Data Protection Officer. • Definición e implantación de controles de acceso físico, cuando corresponda. • Aplicación de las políticas y procedimientos de seguridad de EDPR |
| Alto | <u>1. Medidas de seguridad generales (similares a las que se aplican a encargados con nivel de criticidad medio)</u> | |

| <u>2. Medidas de seguridad especiales:</u> | |
|---|---|
| Utilización de Sistemas Propios del Encargado del Tratamiento | Utilización de Sistemas de EDPR |
| <ul style="list-style-type: none"> • Definición e implantación de un procedimiento de cifrado de soportes • Definición e implantación de un procedimiento de anonimización de los datos personales en los casos que sea técnicamente posible • Definición e implantación de un procedimiento de registro de acceso a los datos. • Definición e implantación de un procedimiento de cifrado de comunicaciones. • Definición e implantación de un procedimiento de copias de respaldo y recuperación. • Realización de auditorías independientes periódicas (como mínimo cada 2 años) sobre el cumplimiento de las disposiciones legales asociadas a la protección de datos personales, incluyendo el RGPD / Certificación independiente de la conformidad con el RGPD (cuando estén disponibles mecanismos de certificación). • Adhesión a código de conducta sobre protección de datos personales, conforme a la aplicación del RGPD • Definición e implantación de un procedimiento de destrucción o de devolución de datos y documentos, de forma segura y confidencial (imposibilitando su posterior recuperación y certificando la ausencia de copias), cuando termine la relación contractual (excepto cuando exista una obligación de conservación de los datos por uno período adicional, en cuyo caso deberán bloquearse los datos/documentos). | <ul style="list-style-type: none"> • Adhesión a código de conducta sobre protección de datos personales, conforme a la aplicación del RGPD • Definición e implantación de un procedimiento de destrucción o de devolución de datos y documentos, de forma segura y confidencial (imposibilitando su posterior recuperación y certificando la ausencia de copias), cuando termine la relación contractual (excepto cuando exista una obligación de conservación de los datos por uno período adicional, en cuyo caso deberán bloquearse los datos / documentos). |

ANEXO II

MECANISMOS DE SUPERVISIÓN DE ENCARGADOS DE TRATAMIENTO

El seguimiento de las obligaciones de los encargados del tratamiento en relación con el cumplimiento de las obligaciones relacionadas con el tratamiento de datos personales en el marco del RGPD, se realizará aplicando diferentes mecanismos en función del nivel de criticidad del contratista según el siguiente cuadro:

| Nivel de criticidad del Encargado del Tratamiento | Mecanismos de supervisión |
|---|--|
| Básico | Asegurar que en caso de necesidad, el encargado de tratamiento pondrá a disposición de EDPR toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el RGPD, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del EDPR o de otro auditor autorizado por EDPR, e informará inmediatamente a EDPR si, en su opinión, una instrucción infringe el RGPD u otras disposiciones en materia de protección de datos. |
| Medio | Adicionalmente a los mecanismos previstos en el nivel de criticidad "Bajo", deberán ser considerados los siguientes mecanismos específicos: <ul style="list-style-type: none"> - Envío periódico de declaración / auto-certificación de cumplimiento de las disposiciones legales y de cumplimiento de las condiciones definidas contractualmente en materia de protección de datos; - Información y envío de la documentación de soporte a EDPR de cualquier reclamación recibida de los titulares de los datos y de las diligencias tomadas con vistas a su resolución; - Información y envío de documentación de soporte a EDPR de cualesquiera solicitudes, consultas o inspecciones promovidas por la autoridad de control en materia de protección de datos, de las acciones desarrolladas y de las correspondientes consecuencias. |
| Alto | Adicionalmente a los mecanismos previstos en los niveles de criticidad "Básico" y "Medio", deberán ser considerados los siguientes mecanismos específicos: <ul style="list-style-type: none"> - Envío a EDPR de Informe de auditoría independiente periódico sobre el cumplimiento de las disposiciones legales asociadas a la protección de datos personales, incluyendo el RGPD; - Certificación independiente de la conformidad con el RGPD (cuando estén disponibles mecanismos de certificación); - Adhesión a código de conducta sobre protección de datos personales, conforme a la aplicación del RGPD; - Envío periódico a la EDPR de información relativa al sistema de gestión de cumplimiento de obligaciones legales de protección de datos (modelo de gobierno, identificación del DPO, políticas y procedimientos implementados, registro de actividades de tratamiento realizadas en nombre de la EDPR, descripción de las medidas técnicas y organizativas implementadas, planes de acción de mejora, etc.) - Envío periódico a la EDPR de evidencias respecto a la toma de conocimiento por los colaboradores de las reglas y procedimientos que deben ser adoptados y / o de participación en acciones de formación sobre esta materia; - Envío periódico a EDPR de evidencias sobre la toma de conocimiento por parte de los colaboradores del hecho de que sus datos se comparte con EDPR, cuando corresponda, para los fines de tratamiento relevantes (por ejemplo, gestión de accesos a sistemas EDPR, control de calidad, etc.); - Envío de evidencia de certificado de destrucción o de devolución de datos, de forma segura y confidencial (imposibilitando su posterior recuperación y certificando la ausencia de copias), cuando termine la relación contractual (excepto cuando exista una obligación de conservación de los datos por uno período adicional, en cuyo caso deberán bloquearse los datos). |