ADENDA DE PRESTACIÓN DE SERVICIOS
CON ACCESO A DATOS PERSONALES
– SERVICIOS DE CONSULTORÍA, AUDITORIA Y FORMACIÓN –

La presente Adenda, que vincula al CLIENTE (en adelante, el responsable del tratamiento) y a CONSTRUYENDO FUTURO INFORMATICO S.L., con NIF B34222950 (en adelante, el encargado del tratamiento) regulará los derechos y obligaciones que deben cumplir ambas Partes siguiendo lo dispuesto en la normativa vigente de protección de datos personales.

Esta Adenda forma parte del Contrato de prestación de servicios subscrito entre el CLIENTE y CONSTRUYENDO FUTURO INFORMATICO S.L., con NIF B34222950 y entrará en vigor una vez que se haya iniciado la prestación del servicio objeto del Contrato.

Nota: en caso de que el indicado anteriormente como responsable del tratamiento actúe, para determinados tratamientos, como encargado del tratamiento para otros responsables involucrados en las operaciones de tratamiento a las que se refiere este acuerdo, deberá entenderse que es encargado del tratamiento para dichos tratamientos, y, en consecuencia, el mencionado como encargado del tratamiento deberá entenderse, para dichos tratamientos también, que es subencargado del tratamiento.

EXPONEN

1. Que ambas partes se reconocen capacidad legal suficiente para suscribir el presente Contrato.
2. Que el responsable del tratamiento ha contratado los servicios proporcionados por el encargado del tratamiento que más adelante se detallan.
3. Que la prestación de los servicios se realizará (i) en los locales del responsable del tratamiento; (ii) en los locales del encargado del tratamiento; (iii) por conexión remota. Asimismo, el encargado del tratamiento puede incorporar datos del responsable del tratamiento en sus sistemas.
4. Que el responsable del tratamiento ha decidido elegir a este encargado del tratamiento porque le ofrece garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas a la información facilitada, garantizando que el encargo de tratamiento se ajusta a la normativa vigente en materia de protección de datos personales y se protegen los derechos y libertades de los interesados.
5. Que de conformidad con el artículo 28 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 (en adelante, RGPD), y el artículo 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ambas partes convienen en suscribir el presente Contrato, el cual aceptan expresamente y de acuerdo a las siguientes:

CLÁUSULAS

I. Objeto del encargo

Mediante las presentes cláusulas se habilita al encargado del tratamiento para tratar, por cuenta del responsable del tratamiento, los datos personales necesarios para prestar el/los servicio/s de: consultoría, auditoría y formación.

El tratamiento consistirá en: servicios de consultoría, auditoría y formación en el ámbito de la protección de datos personales, la LSSICE, la continuidad de negocio y la gestión de la seguridad de la información y la ciberseguridad, en general.

Concreción de las operaciones a realizar: recogida; registro; conservación; consulta; modificación, interconexión, comunicación.

La prestación de los servicios puede ser en los locales del responsable del tratamiento, en los locales del encargado del tratamiento o de forma remota. Igualmente, el encargado del tratamiento puede incorporar

datos del responsable del tratamiento en sus sistemas.

II. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento pone a disposición del encargado del tratamiento la información que se describe a continuación:

a) Datos identificativos de clientes y usuarios.

b) Datos identificativos de proveedores y contactos.

c) Datos identificativos de personal y/o socios.

d) Datos alojados en los sistemas del responsable del tratamiento

La puesta a disposición de la información indicada anteriormente puede realizarse, bien proporcionando al encargado la información indicada, bien permitiéndole el acceso a la misma, o debido a que el responsable del tratamiento almacena dicha información en sistemas y/o instalaciones del encargado del tratamiento.

III. Duración

La duración del presente acuerdo es: Indefinida.

IV. Obligaciones del encargado del tratamiento

El encargado del tratamiento, y todo su personal se obliga a:

a) Utilizar los datos personales objeto del tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b) Tratar los datos de acuerdo a las instrucciones del responsable del tratamiento.

   Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembro, el encargado informará inmediatamente al responsable.

c) Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de cada responsable, que contenga:

   1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

   2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

   3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en su caso, de las transferencias indicadas en el artículo 49, párrafo segundo del RGPD, la documentación de garantías adecuadas, teniendo en cuenta, especialmente, el posible alojamiento de datos en servicios de computación en la nube (servicios *cloud*).

   4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

      i. La seudonimización y el cifrado de datos personales.

      ii. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

      iii. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

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

d) No comunicar datos a terceras personas (incluidas las transferencias de datos personales a terceros países u organizaciones internacionales), salvo que cuente con la autorización expresa del

responsable del tratamiento, en los supuestos legalmente admisibles. A tal efecto, en relación a los datos vinculados a los servicios prestados por el encargado, el responsable autoriza expresamente al encargado del tratamiento la realización de transferencias de datos personales a terceros países u organizaciones internacionales siempre que haya obtenido garantías apropiadas. El detalle de las transferencias de datos personales a terceros países u organizaciones internacionales, actualizado en todo momento, se encuentra en https://grupocfi.es/subcontrataciones/.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembro que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que el Derecho lo prohíba por razones importantes de interés público.

El encargado puede comunicar datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

e) Se autoriza al encargado a subcontratar con empresa o empresas más idóneas para la prestación de sus servicios; a tal efecto, la lista de empresas externas a las que el encargado del tratamiento subcontrata servicios se encuentra en https://grupocfi.es/subcontrataciones/. Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de 15 días. El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad, etc.) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f) Mantener el deber de secreto respecto a los datos personales a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g) Garantizar que las personas autorizadas para tratar datos personales se comprometen de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

   1. Acceso, rectificación, supresión y oposición.
   2. Limitación del tratamiento.
   3. Portabilidad de los datos.
   4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

   Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección dpo@grupocfi.es. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k) Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.

l) Notificación de violaciones de la seguridad de los datos:

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y, en cualquier caso, antes del plazo máximo de 36 horas las violaciones de la seguridad de los datos personales a su cargo de la que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia. Esta comunicación se realizará de la siguiente forma: enviando un correo electrónico a la dirección facilitada por el responsable (en caso de que no haya facilitado ninguna dirección en particular, se asumirá que es la que aparece en las Condiciones Particulares del Contrato).

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella, se facilitará, como mínimo, la información siguiente:

1. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

2. El nombre y datos de contacto del delegado de protección de datos o del otro punto de contacto en el que pueda obtenerse más información.

3. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

4. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

m) Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n) Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p) Implantar las medidas de seguridad siguientes:

Medidas de seguridad de acuerdo con la evaluación de riesgos realizada por el encargado del tratamiento:

1. Entorno seguro: los locales donde se tratan los datos deben contar con medios mínimos de seguridad como extintores, alarmas, etc.

2. Funciones y obligaciones del personal: las funciones y obligaciones de cada uno de los usuarios o perfiles de usuario con acceso a datos y a los sistemas estarán claramente definidas y documentadas.

3. Control de acceso: el personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Se deberán establecer mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Identificación y autenticación: se establecerá un sistema que permita la identificación inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información, y la debida autenticación para verificar la identidad del usuario.

5. Almacenamiento seguro de soportes y documentos: los dispositivos de almacenamiento de los soportes y documentos que contengan datos de carácter personal, deberán disponer de mecanismos que obstaculicen su apertura, mediante llaves u otros medios similares.

6. Software anti-malware: en los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema anti-malware que evite, en la medida de lo posible, el robo y la destrucción de la información y datos.

7. Copias de respaldo: se realizarán copias de respaldo periódicamente, en función del volumen y de la frecuencia de actualización de los datos.

8. Destrucción y reutilización de equipos y soportes: los desechos informáticos, de cualquier tipo, que puedan contener datos personales, deberán ser eliminados o destruidos de forma segura para garantizar que no se va a poder acceder a ellos.

9. Traslado seguro de soportes y documentos: cuando los soportes y/o documentos salgan fuera de los locales de tratamiento, se adoptarán las medidas necesarias para impedir la sustracción, pérdida o acceso indebido a la información durante el transporte.

10. Acceso a través de redes de comunicaciones: los accesos a los datos de carácter personal realizados a través de redes de comunicaciones, sean o no públicas, deberán realizarse de forma segura.

En todo caso, deberá implantar mecanismos para:

1. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

2. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

3. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

4. Seudonimizar y cifrar los datos personales, en su caso.

En particular, el encargado del tratamiento garantiza que los datos personales que integre en sus sistemas de tratamiento, por cuenta del responsable, sean albergados en servidores propios o subcontratados, los cuáles:

1. Son seguros, conforme a las exigencias detalladas anteriormente.

2. Están localizados en la Unión Europea (salvo que el responsable del tratamiento haya autorizado expresamente la transferencia de los datos a un tercer país o a una organización internacional, según se detalla en el apartado d) del punto IV de este contrato. En todo caso, la localización fuera de la Unión Europea debe respetar y cumplir estrictamente las condiciones previstas a este respecto en el presente contrato y en el RGPD).

q) El encargado del tratamiento dispondrá de un delegado de protección de datos designado, con el que se podrá contactar a través de estos medios:

- En la dirección https://grupocfi.es/dpd
- En el correo electrónico dpd@grupocfi.es
- En el teléfono 901 001 802

r) Destino de los datos una vez finalice la prestación de los servicios:

Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

V. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Entregar, o permitir el acceso, al encargado los datos a los que se refiere la cláusula II de este documento.

b) En su caso, realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.

c) Realizar las consultas previas que corresponda.

d) Velar, de forma previa y durante el tratamiento, por el cumplimiento del RGPD por parte del encargado.

e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

Fecha de última actualización: 23/05/2022.