ACUERDO DE ENCARGADO DE TRATAMIENTO

1. AUDATEX ESPAÑA S.A. con domicilio en AV. DE BRUSELAS, 36, PLANTA 2ª, 28108 ALCOBENDAS-MADRID y CIF A28586550 en su calidad de ENCARGADO DEL TRATAMIENTO (en adelante también EL PRESTADOR DEL SERVICIO), se encuentra vinculado con el CLIENTE (en adelante también RESPONSABLE DEL TRATAMIENTO) en virtud de una relación contractual de carácter mercantil para la prestación del servicio VALORACIÓN DE DAÑOS, ASÍ COMO CONTROL, GESTIÓN Y ADMINISTRACIÓN DE LOS MISMOS que realiza EL PRESTADOR DEL SERVICIO al CLIENTE.

2. Para la prestación de dicho servicio es necesario que EL PRESTADOR DEL SERVICIO tenga acceso y realice tratamientos de datos de carácter personal del fichero de clientes responsabilidad del CLIENTE, por lo que asume las funciones y obligaciones que el Reglamento General de Protección de Datos, REGLAMENTO (UE) 2016/679 (en adelante RGPD), estipula como Encargado de dicho Tratamiento.

3. Ambas partes suscriben el presente ACUERDO DE ENCARGADO DE TRATAMIENTO DE DATOS PERSONALES de conformidad con las siguientes

ESTIPULACIONES

Primera.- OBJETO

Mediante las presentes cláusulas se habilita al PRESTADOR DEL SERVICIO, encargado del tratamiento, para tratar por cuenta de EL CLIENTE, responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio.

El tratamiento consistirá en las siguientes operaciones necesarias para la ejecución del contrato:

Conservación
Comunicación por transmisión
Interconexión

Segunda.- IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA Y CATEGORÍA DE INTERESADOS

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 siguiente información:

Nombres y apellidos	Dirección
DNI/ NIE/ Pasaporte	Teléfono
Datos de siniestro	Información fotográfica
Matrícula	

La información facilitada al ENCARGADO DEL TRATAMIENTO es referida a las siguientes categorías de interesados:

Clientes

Tercera.- DURACIÓN

El presente acuerdo de encargo de tratamiento estará en vigor en tanto que el Encargado del Tratamiento preste los servicios conforme al contrato de prestación de servicios del que el presente Anexo forma parte.

Cuarta.- OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

El ENCARGADO DEL TRATAMIENTO y todo su personal se obliga a:

a. Utilizar los datos personales objeto de 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.

El responsable autoriza de forma expresa al encargado a que pueda realizar, entre los usuarios, directamente o a través de un tercero, un estudio, análisis y control de calidad de los servicios prestados a sus clientes, a estos únicos efectos.

b. Tratar los datos de acuerdo con 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 miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del 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 el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

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

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los 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.

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 miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. Subcontratación:

No subcontratar ninguna de las prestaciones que formen parte del objeto de este acuerdo que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 15 días indicando los tratamientos que se pretende subcontratar e 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 establecido.

El subcontratista, que también tendrá 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…) 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 sub-encargado, 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 de carácter personal 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 comprometan, 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 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 al Responsable. 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. Derecho de información

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 24 horas, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

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:

a) 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.

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

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

d) 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.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

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 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 medidas de seguridad

El Encargado del Tratamiento implantará las medidas de seguridad técnicas y organizativas que se recogen en el Apéndice adjunto.

En todo caso, deberá implantar mecanismos para:

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

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

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

d) Seudonimizar y cifrar los datos personales, en su caso.

q. Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

Identidad	**Datos de contacto**
Corporación Europea de Inversiones S.A. A28433027	*C/ Fernanflor nº4 (28014) Madrid Tlfno: 914203301 dpo@audatex.es*

r. Destino de los datos

Destruir los datos, salvo indicación expresa del responsable, 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 boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Quinta.- OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

Corresponde al responsable del tratamiento:

a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.

b) 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 todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

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

f) Garantizar al encargado que el tratamiento de datos objeto del encargo se realiza de conformidad con toda la legislación en materia de protección de datos.

g) No facilitar al encargado ningún dato personal no recogido en este acuerdo sin previa notificación y formalización por escrito.

Sexta.- RESPONSABILIDADES

Las partes se comprometen a cumplir con sus respectivas obligaciones establecidas en el presente acuerdo y en la normativa vigente en materia de protección de datos.

Cada parte responderá de los incumplimientos de sus respectivas obligaciones en que hubiesen incurrido personalmente, manteniendo indemne a la parte contraria frente a cualquier reclamación, sanción o gasto que se derivase de dicho incumplimiento como consecuencia del cumplimiento del presente acuerdo.

Si el encargado del tratamiento infringe el RGPD al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Asimismo, el encargado del tratamiento será responsable, civil y administrativamente, en caso de incumplimiento de sus obligaciones previstas en el RGPD y demás normativa aplicable en materia de protección de datos, o actúe en contra o al margen de las instrucciones del responsable del tratamiento.

APÉNDICE AL "ACUERDO DE ENCARGADO DE TRATAMIENTO"

MEDIDAS DE SEGURIDAD

Conforme se indica en la cláusula cuarta "Obligaciones del Encargado del Tratamiento" apartado p) del anexo del que el presente apéndice forma parte integrante, el Encargado del Tratamiento debe implantar las siguientes medidas de seguridad organizativas y técnicas detalladas en este adjunto.

1) Disponer de una Política de Seguridad, aprobada por la dirección y comunicada a los empleados aplicable al tratamiento de datos personales automatizado y no automatizado.

2) Implantar todas y cada una de las siguientes medidas:

- Seguridad física

  - Los locales cuentan con medidas de seguridad para controlar su acceso y garantizar su integridad.

  - Exclusivamente el personal autorizado tiene acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

  - Los dispositivos de almacenamiento de los documentos disponen de mecanismos que obstaculicen su apertura o, en su defecto, existen medidas que impiden el acceso de personas no autorizadas.

  - El archivo de los soportes o documentos se realiza de forma que garantiza la correcta conservación de los documentos, la localización y consulta de la información y posibilita el ejercicio de derechos.

  - Los armarios, archivadores u otros elementos en los que se almacenan ficheros no automatizados con datos personales se encuentran en áreas en las que el acceso está protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas permanecen cerradas cuando no es preciso su acceso.

  - Se destruyen las copias o reproducciones desechadas con lo que se evita el acceso a la información contenida en las mismas o su recuperación posterior.

  - El acceso a la documentación se limita exclusivamente al personal autorizado.

- Definir las funciones y obligaciones del personal

  - Acceso a los datos de carácter personal y a los sistemas de información claramente definidos y documentados para cada rol o perfil de usuario y funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

  - Personal formado en las normas de seguridad que afectan al desarrollo de sus funciones así como las consecuencias de su incumplimiento.

- Registro de incidencias

  - Se dispone de un procedimiento de notificación y gestión de las incidencias, así como de un registro en el que consta el tipo de incidencia, el momento en que se ha producido o detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

  - Además, se consigna los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

- Control de acceso

  - Los usuarios tiene acceso únicamente a los recursos que precisan para el desarrollo de sus funciones.

  - Se dispone de una relación de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

  - Se dispone de mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

  - Exclusivamente el personal autorizado puede conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

  - El personal ajeno que tenga acceso a los recursos está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

  - De cada intento de acceso se guarda, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

  - En el caso de que el acceso haya sido autorizado, se guarda la información que permita identificar el registro accedido.

  - Los mecanismos que permiten el registro de accesos están bajo el control directo del responsable de seguridad competente sin que se pueda proceder a la desactivación ni la manipulación de los mismos.

  - El período mínimo de conservación de los datos registrados será de dos años.

  - El responsable de seguridad revisa, al menos una vez al mes, la información de control registrada y elabora un informe de las revisiones realizadas y los problemas detectados.

  - Se dispone de mecanismos que permiten identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

- Gestión de soportes y documentos

  - Los soportes y documentos que contienen datos personales permiten identificar el tipo de información que contienen, ser inventariados y solo son accesibles por el personal.

  - La salida de soportes y documentos que contengan datos personales, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo su control se realizan garantizando la máxima seguridad de los mismos. Durante el traslado de la documentación se adoptan las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido.

  - Se procede a la destrucción o borrado de cualquier documento o soporte, cuando vaya a desecharse, para evitar el acceso a la información que contiene o su recuperación posterior.

  - Se dispone de un sistema de registro de entrada y salida de soportes que permite, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción, debidamente autorizada.

  - Cuando se traten categorías de datos especiales:

    - La identificación de los soportes se realiza utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

    - La distribución de los soportes que contienen datos personales se realiza cifrando dichos datos o u otro mecanismo que garantizan que dicha información no es accesible o manipulada durante su transporte.

- Los datos que contienen los dispositivos portátiles se cifran cuando éstos se encuentran fuera de las instalaciones.

- No se permite el tratamiento de datos personales en dispositivos portátiles que no permitan su cifrado o medida de seguridad equivalente.

- Identificación y autenticación
  - Se garantiza la correcta identificación y autenticación de los usuarios, de forma inequívoca y personalizada, de todo aquel usuario que intenta acceder al sistema de información y la verificación de que está autorizado.
  - Existe un procedimiento de asignación, distribución y almacenamiento de contraseñas que garantiza su confidencialidad e integridad. La identidad de los usuarios es única y verificable.
  - Gestión de contraseñas con respecto a la complejidad, intentos fallidos, tiempos de inactividad, reutilización, caducidad, desbloqueo.

- Copias de respaldo y recuperación
  - Se dispone de un procedimiento de actuación para la realización de copias de respaldo.
  - Se dispone de procedimientos para la recuperación de los datos que garantiza en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción y se verifica periódicamente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
  - Se realizan pruebas anteriores a la implantación o modificación de los sistemas de información sin datos reales o previa copia de seguridad de éstos.
  - Se conserva una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, con las mismas medidas de seguridad o elementos que garantizan la integridad y recuperación de la información, de forma que sea posible su recuperación.

- Responsable de seguridad

  Se ha designado un responsable de seguridad encargados de coordinar y controlar las medidas.

- Auditoría

  Los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someten, al menos cada dos años, a una auditoría interna o externa.

- Telecomunicaciones

  La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realiza cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantiza que la información no sea inteligible ni manipulada por terceros.

- Gestión de continuidad del servicio

  Se dispone de un plan de contingencia para hacer frente a situaciones adversas que puedan poner en peligro la continuidad del servicio prestado.