Contrato para el encargo del tratamiento de datos personales

entre

Nombre
y direccion
del cliente

(«**Cliente**» / «**Controlador**»)

y

Emarsys North America, Inc.
10 W. Market Street, Suite 1350
IN 46204, Indiana
Estados Unidos
(«**Contratista**» / «**Procesador**»)

1. PREÁMBULO

Como parte de un contrato independiente y / o basándose en encargos individuales independientes (en lo sucesivo colectivamente denominados «**Contrato Principal**»), el Contratista deberá proporcionar al Cliente varios servicios de marketing, con especial énfasis en la planificación, implantación y análisis de comunicaciones por email (en lo sucesivo colectivamente denominados «**Servicios**»). Los Servicios se describen más detalladamente en el Contrato Principal y en las descripciones de cada Servicio correspondiente.

2. ASUNTO

2.1. Tratamiento de datos personales

El presente contrato (el «**Contrato**») proporcionará normas sobre el tratamiento de datos personales que el Contratista procese en nombre del Cliente mientras que se prestan los Servicios («**Datos**»). Los datos personales se refieren a cualquier información relativa a una persona física identificada o identificable. Los Datos incluyen, especialmente, los nombres, direcciones de email y áreas de interés de los destinatarios de los boletines por email del Cliente; otros datos relativos al tipo y categorías de los datos personales de los sujetos de datos se indican en el Contrato Principal y sus respectivas descripciones de Servicios.

2.2. Extensión del tratamiento de datos encargado

El asunto, duración, naturaleza y objeto del tratamiento de Datos se indican en el Contrato Principal y en las respectivas descripciones de Servicios.

3. OBLIGACIONES DEL CLIENTE (CONTROLADOR)

3.1. Cliente como controlador

El Cliente sigue siendo el único controlador en lo que a los Datos se refiere y es responsable de la legalidad del tratamiento de los Datos y de la protección de los derechos de los sujetos de datos. El Cliente informará a los sujetos de datos u obtendrá su consentimiento en lo que respecta al tratamiento de Datos, cuando así se precise.

3.2. Instrucciones

Hasta los límites en que el tratamiento de Datos lo realice el Contratista mediante el uso de software estándar proporcionado al Cliente para su uso online, el Cliente ejercerá normalmente su autoridad para dar instrucciones (ver punto 4.1) mediante la utilización de la interfaz online del software. Otras instrucciones del Cliente se deben dar usando la interfaz web proporcionada al Cliente por el Contratista o por escrito (incluido el formato electrónico); las instrucciones verbales deberán confirmarse por escrito sin demora indebida. El Cliente se reserva el derecho a dar tales instrucciones en cualquier momento. Si la extensión de las instrucciones recibidas del Cliente escapa a lo que se espera que realice el Contratista para el Cliente conforme al Contrato Principal, el Cliente realizará un pedido y compensará al Contratista por los servicios correspondientes de forma independiente.

3.3. Obligación de notificación

Si dentro del área de responsabilidad del Cliente, Datos que han sido tratados por el Contratista de conformidad con este Contrato pasan a ser conocidos de forma inadvertida por terceros no autorizados, el Cliente informará al Contratista a su debido tiempo para permitir al Contratista adoptar las medidas técnicas y organizativas necesarias por su parte.

3.4. Obligación de exención

Si un tercero (incluidas las autoridades) reclama o acusa al Contratista por incurrir en incumplimiento de contrato basándose en el incumplimiento por parte del Cliente de sus obligaciones, resultará de aplicación lo siguiente: El Cliente concederá al Contratista una exención contra estas reclamaciones, proporcionará al Contratista el apoyo adecuado para su defensa jurídica y eximirá al Contratista de los costes razonables de la defensa legal. La obligación de exención únicamente será válida si el Contratista informa al Cliente de cualquier reclamación efectuada por escrito y sin demora indebida, no realiza ninguna confesión ni ninguna otra declaración a tal efecto y permite al Cliente, asumiendo este sus costes y en la medida en que sea proceduralmente posible, realizar todos los trámites jurídicos y extrajudiciales pertinentes en lo que respecta a las reclamaciones.

4. DEBERES DEL CONTRATISTA (PROCESADOR)

4.1. Requisito de respetar las instrucciones

El Contratista tratará los datos de forma exclusiva como parte y a los efectos de su prestación de Servicios al Cliente y de conformidad con las instrucciones documentadas del mismo. El Contratista no tratará los datos personales de ninguna otra manera ni para ningún otro objeto, a menos que se le exija conforme a la legislación de la UE o de un Estado Miembro de la UE a la que el Contratista esté sujeto; en tal caso, el Contratista informará al Cliente de ese requisito legal antes del tratamiento, a menos que la ley prohíba dicha información basándose en fundamentos de interés público.

4.2. Obligación de informar

El Contratista informará de inmediato al Cliente si, en su opinión, una instrucción dada por el Cliente infringe las disposiciones aplicables en lo que respecta a la protección de datos. El Contratista tendrá derecho a suspender la ejecución de dicha instrucción hasta que esta sea confirmada o modificada por el Cliente. El Contratista no tiene obligación de llevar a cabo una revisión jurídica de las instrucciones.

4.3. Obligación de proporcionar soporte

El Contratista, a petición del Cliente, asistirá de forma adecuada al Cliente en caso de que este únicamente sea capaz de cumplir sus obligaciones con sujetos de datos (especialmente, la obligación de proporcionar a un sujeto de datos detalles relativos al tratamiento de sus datos personales) con la asistencia del Contratista. El Contratista reenviará al Cliente las solicitudes de sujetos de datos dirigidas al Contratista. El Contratista también, a petición del Cliente, asistirá al Cliente para garantizar el cumplimiento relativo a la seguridad de los datos personales (seguridad de tratamiento, notificación de un incumplimiento de datos personales a la autoridad supervisora, comunicación de un incumplimiento de datos personales al sujeto de datos), así como una evaluación del impacto de la protección de datos potencialmente necesaria y consultas previas, en cada caso teniendo en cuenta la naturaleza del tratamiento y la información disponible para el Contratista. El Cliente realizará un pedido y compensará al Contratista de manera independiente por el tiempo

y esfuerzo correspondiente hasta los límites en que dicho soporte escape al requerido por la legislación aplicable.

4.4. Rectificación, borrado y bloqueo

En caso de que sea necesario rectificar, borrar o bloquear datos personales, el Cliente se compromete a realizarlo por sí mismo empleando las funciones correspondientes disponibles en el software proporcionado. Si esto no es posible, el Contratista asumirá las tareas de rectificación, borrado y bloqueo según las instrucciones del Cliente. El punto 7.2 se aplica al borrado de los Datos al final de la vigencia del contrato.

4.5. Ubicación del tratamiento de datos

Los Datos se tratarán únicamente en la Unión Europea (UE) y / o sus estados miembros, los cuales se incluyen en el contrato que cubre el Espacio Económico Europeo (EEE), siempre que el Cliente no haya permitido al Contratista tratar los Datos en un país fuera de la UE y del EEE en este Contrato o de cualquier otra manera.

4.6. Responsable de la protección de datos

El Contratista contará con un responsable de la protección de datos designado. El Contratista proporcionará los datos de contacto del responsable de la protección de datos al Cliente cuando este se los solicite.

4.7. Confidencialidad de los Datos

El Contratista facilitará formación a sus empleados encargados de la tarea de tratamiento de datos personales sobre las disposiciones reglamentarias de la protección de datos y obtendrá su compromiso por escrito para mantener la confidencialidad y el secreto de los datos. Esta obligación de secreto resulta especialmente de aplicación a personas encargadas de la tarea del tratamiento de datos y en lo que respecta a datos relativos a organismos jurídicos o una asociación y seguirá siendo de aplicación para el Contratista incluso cuando haya finalizado el empleo.

4.8. Obligación de notificación

Si los Datos del Cliente pasan a ser conocidos por terceros no autorizados de forma ilícita, p.e., por un incumplimiento de la legislación en materia de protección de datos aplicable, el presente Contrato o instrucciones dadas por el Cliente, el Contratista deberá informar de inmediato al Cliente sobre este hecho.

4.9. Medidas técnicas y organizativas

Teniendo en cuenta el estado de la tecnología, los costes de implantación y la naturaleza, alcance, contexto y objetos del tratamiento, así como el riesgo de variar la probabilidad e independencia de los derechos y libertades de las personas, el Contratista implantará medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado para el riesgo. El Contratista, en concreto, implantará las medidas técnicas y organizativas especificadas en el Anexo 1 de este Contrato en su área de responsabilidad para garantizar la seguridad del tratamiento. Además, el Contratista dará los pasos necesarios para garantizar que cualquier persona que actúe bajo su autoridad y que tenga acceso a los Datos personales no los trate más que según las instrucciones del Cliente, a menos que se le exija hacerlo conforme a la legislación de la UE o de un Estado Miembro de la UE.

4.10. Seguro

El Contratista contará con una cobertura de seguro adecuada a lo largo de la vigencia de este Contrato para posibles reclamaciones de responsabilidad derivadas de o relacionadas con este Contrato.

4.11. Obligación de exención

Si un tercero (incluidas las autoridades) reclama o acusa al Cliente por incurrir en incumplimiento de contrato basándose en el incumplimiento por parte del Contratista de sus obligaciones, resultará de aplicación lo siguiente: El Contratista concederá al Cliente una exención contra estas reclamaciones, proporcionará al Cliente el apoyo adecuado para su defensa jurídica y eximirá al Cliente de los costes razonables de la defensa legal. La obligación de exención únicamente será válida si el Cliente informa al Contratista de cualquier reclamación efectuada por escrito y sin demora indebida, no realiza ninguna confesión ni ninguna otra declaración a tal efecto y permite al Contratista, asumiendo este sus costes y en la medida en que sea proceduralmente posible, realizar todos los trámites jurídicos y extrajudiciales pertinentes en lo que respecta a las reclamaciones.

5. DERECHO DEL CLIENTE A REALIZAR AUDITORÍAS

5.1. Certificación

El Contratista debe utilizar un sistema de gestión de la seguridad de la información certificado conforme a la ISO 27001 durante la vigencia de este Contrato y deberá proporcionar prueba del mismo a petición.

5.2. Auditorías

Hasta los límites exigidos, se permite al Cliente auditar (o hacer que otro auditor, encargado por el Cliente, audite) el cumplimiento por parte del Contratista de: a) las normas jurídicas relativas a la protección de datos, b) los acuerdos contractuales realizados por las partes y c) las instrucciones del Cliente. El Contratista contribuirá en tales auditorías y pondrá a disposición del Cliente toda la información necesaria para demostrar su cumplimiento. El Cliente debe notificar con al menos dos semanas de antelación su intención de realizar auditorías en las instalaciones empresariales del Contratista. Las auditorías las realizará el Cliente durante la jornada laboral normal y sin causar inconvenientes significativos en el curso de las operaciones empresariales. Las partes correrán con sus propios costes de o relacionados con las auditorías.

5.3. Costes

El Cliente correrá con los costes de o relacionados con las auditorías. Esto también incluirá la remuneración por las horas de trabajo incurridas por el personal del Contratista.

5.4. Intereses legítimos del Contratista

Si, durante la realización de las auditorías pueden revelarse secretos comerciales o empresariales del Contratista o se puede comprometer propiedad intelectual que pertenece al Contratista, el Cliente deberá realizar las auditorías a través de un tercero especialista independiente que tenga la obligación de preservar la confidencialidad en lo que respecta al Contratista.

6. SUBCONTRATACIÓN

6.1. Empleo de subcontratistas

El Contratista estará autorizado para emplear subcontratistas para el tratamiento de Datos si el Contratista suscribe un contrato por escrito o electrónico con el subcontratista en lo que respecta al tratamiento de Datos y el nivel de protección proporcionado por dicho contrato es igual o superior al de este Contrato y si el Cliente da su consentimiento previo por escrito o electrónico para emplear al subcontratista. El Contratista informará al Cliente por escrito o en formato electrónico sobre cualquier cambio pretendido relativo a la adición o reemplazo de subcontratistas, dando así al Cliente la posibilidad de oponerse a dichos cambios. Se considerará que el Cliente ha dado su consentimiento si este no se opone por escrito o en formato electrónico en el plazo de un mes tras la recepción de esta información.

6.2. Subcontratistas aprobados

El Cliente por la presente conviene contratar a los subcontratistas especificados en el Anexo 2.

6.3. Responsabilidad de los subcontratistas

Cuando un subcontratista incumpla sus obligaciones de protección de datos, el Contratista seguirá siendo plenamente responsable ante el Cliente por el cumplimiento de las obligaciones del subcontratista.

7. VIGENCIA

7.1. Vigencia

La vigencia de este Contrato se corresponderá con la del Contrato Principal más 30 días adicionales. El derecho de rescisión por buena causa no se verá afectado.

7.2. Datos en el punto de rescisión del contrato

El Contratista borrará los Datos del Cliente de sus medios de almacenamiento de datos y destruirá cualquier documentación relevante de que disponga en el plazo de 30 días tras la finalización del Contrato Principal, siempre que el Contratista no esté jurídicamente obligado a continuar almacenándolo. El Cliente será responsable de la exportación de los Datos de forma puntual antes del fin de este periodo y de guardarlos para su propio uso continuado. El cliente encargará y remunerará de forma independiente al Contratista por los Datos que se publiquen o exporten de una manera no cubierta por los servicios incluidos en las funciones estándar (p.e., descarga de archivos).

7.3. Copias de seguridad

La obligación anterior de borrar los datos no se aplicará a copias de los mismos incluidas en las copias de seguridad regularmente generadas de los conjuntos completos de datos del Contratista, pues esto requeriría una inversión significativa de recursos por parte del Contratista para conseguir un borrado aislado y que se borrarán o reemplazarán automáticamente después de un máximo de 14 días como parte del ciclo de seguridad que aplica el Contratista. Hasta que se produzca el borrado o reemplazo automático, cualquier recuperación u otro uso de dichas copias queda prohibido tras la finalización de este Contrato. El Cliente puede solicitar que el Contratista borre dichas copias de seguridad de inmediato, si el Cliente reembolsa al Contratista el coste razonable incurrido en ello; esto también incluye una compensación por las horas de trabajo incurridas por el personal del Contratista.

8. DISPOSICIONES FINALES

8.1. Legislación aplicable

Únicamente será de aplicación la legislación federal y estatal aplicable en Indiana, EE.UU., a este Contrato (sin posibles referencias a otros ordenamientos jurídicos y excluyendo la Convención de NU sobre Contratos para la Venta Internacional de Mercancías), siempre que el Contrato Principal no establezca el sometimiento a cualquier otra legislación aplicable.

8.2. Lugar de jurisdicción

A menos que el Contrato Principal establezca otro lugar, el lugar de jurisdicción para discrepancias resultantes de o relacionadas con este Contrato será Marion County, Indiana, EE.UU.

8.3. Invalidez parcial

En caso de que las disposiciones particulares de este Contrato sean o resulten inválidas, esto no afectará a la validez del resto de disposiciones. Una disposición que contenga la intención económica original de las partes ocupará

el lugar de la disposición inválida. Lo mismo resulta de aplicación a cualquier omisión inintencionada de este Contrato.

Cliente / Controlador:		**Contratista / Procesador:**	Emarsys North America Inc.
Firma:		**Firma:**	
Nombre:		**Nombre:**	Sean Brady
Cargo:		**Cargo:**	General Manager
Fecha:		**Fecha:**	7 de Mayo, 2018

ANEXO 1: MEDIAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DEL TRATAMIENTO

1. PSEUDO-ANONIMIZACIÓN Y ENCRIPTACIÓN DE DATOS PERSONALES

Medidas que generalmente evitan el tratamiento de datos personales no autorizado:

- Los datos personales están encriptados cuando se transmiten.
- Hasta los límites razonablemente posibles (sin evitar la prestación de los servicios acordados), los datos personales son anónimos y / o pseudo-anónimos mediante una referencia de una base de datos en la que se almacenan los datos personales.

2. CAPACIDAD PARA GARANTIZAR LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y RESILIENCIA CONTINUA DE LOS SISTEMAS Y SERVICIOS DE TRATAMIENTO

CONTROL DE ACCESO FÍSICO

Medidas que evitan que personas no autorizadas accedan a los sistemas de tratamiento de datos que procesan o usan datos personales:

- Implantación de prevención de acceso:
  - El área que se debe proteger está asegurada usando una construcción adecuada.
  - Todas las maneras de acceso posibles están salvaguardadas contra el acceso no autorizado.
  - Existe un sistema de autenticación de acceso que es obligatorio para todos (clave o tarjeta inteligente).
  - Se ha instaurado un sistema de control de acceso.
- Gestión y documentación de autorizaciones personales de acceso:
  - Hay normas organizativas relativas a las autorizaciones del acceso a las áreas operativas.
  - Existe documentación relativa a la asignación de claves.
- Supervisión de visitantes y personal externo:
  - Hay directrices para el control de visitantes y personal externo (supervisión, pase de visitante, identificación, etc.).
  - Hay normas para controlar al personal de mantenimiento (supervisión, registro previo, control de la identidad, etc.).

CONTROL DE ACCESO AL SISTEMA

Medidas para evitar que personas no autorizadas puedan usar sistemas de tratamiento de datos (incluidos procesos de encriptado):

- Protección de acceso (autenticación):
  - Hay autenticación de usuario para proteger el acceso a sistemas de tratamiento de datos.
  - Se realizan comprobaciones para garantizar la implantación de las medidas que protegen el acceso.
  - Se usa un generador de contraseñas para generar contraseñas aleatorias.
- Transmisión segura de credenciales de autenticación dentro de la red:
  - Las credenciales de autenticación están encriptadas cuando se transmiten por toda la red.
- Bloqueo del acceso en caso de intentos de inicio de sesión fallidos / inactividad y proceso para restablecer IDs de usuario bloqueadas:
  - Hay un procedimiento seguro de restablecimiento tras haberse bloqueado el acceso, p.e., asignación de nuevas IDs de usuario.
- Prohibición de guardar contraseñas y / o entradas de formularios en el sistema local:
  - Las contraseñas de acceso y / o entradas de formularios no se almacenan en el cliente o su entorno (p.e., guardado en un navegador o notas).
  - Se dan instrucciones a los usuarios sobre estos requisitos.
- Determinación de las personas autorizadas:
  - Hay un concepto de papel (perfiles de usuario predefinidos).
  - Las autorizaciones de acceso siempre se asignan de forma individual (personal).
  - El número de personas autorizadas se mantienen en el mínimo absoluto necesario para el funcionamiento.
- Gestión y documentación de dispositivos de autorizaciones personales y autorizaciones de acceso:
  - Se ha establecido, descrito y se deberá usar un proceso para solicitar, aprobar, asignar y retirar dispositivos de autenticación y autorizaciones de acceso.
  - Se debe especificar una persona para asignar autorizaciones de acceso.
  - Hay normas para la delegación en caso de que la persona principal responsable no esté disponible.
- Bloqueo automático de acceso:
  - Se activará automáticamente un salvapantallas protegido con contraseña mediante el uso de la propia tecnología integrada del sistema operativo en caso de que una estación de trabajo o terminal permanezca inactivo durante más de 30 minutos.
- Bloqueo manual de acceso:
  - Hay directrices para proteger las estaciones de trabajo y los terminales contra el uso no autorizado cuando el lugar de trabajo está temporalmente vacante, p.e., mediante la activación automática o manual del salvapantallas protegido con contraseña.
  - Los empleados recibirán formación relativa a la necesidad de usar estas medidas.

CONTROL DE ACCESO A LOS DATOS

Medidas para garantizar que las personas autorizadas para usar un sistema de tratamiento de datos tengan acceso únicamente a los datos para los que tienen autorización y que los datos personales no puedan leerse, copiarse, modificarse o eliminarse sin autorización durante el tratamiento o utilización y después de haberse guardado (incluidos los procesos de encriptado):

- Concepto de autorización / implantación de restricciones de acceso:
  - Hay normas relativas a la creación, modificación y borrado de perfiles de autorización.
  - Cada persona autorizada con acceso únicamente puede acceder a los Datos que él o ella requiera específicamente para llevar a cabo el proceso actual conforme a los métodos de tratamiento acordados en este Contrato y que se han establecido en el perfil de autorización individual.
  - Si se guardan en una base de datos o procesan conjuntos de datos que incluyen varios Clientes usando el mismo sistema de tratamiento de datos, se ha instaurado un método de restricción de acceso lógico para organizar el tratamiento de datos para cada Cliente respectivo (capacidad multi-cliente).
- Gestión y documentación de autorizaciones personales de acceso:
  - Se ha establecido un proceso para solicitar, aprobar, asignar y retirar autenticaciones de acceso.
  - Las autenticaciones están vinculadas a una ID de usuario personal y a una cuenta.
  - Si la base para tener una autorización ya no está en vigor (p.e., en caso de cambio de función), esta autorización se retirará de inmediato.
- Registro del acceso a los datos:
  - Todas las operaciones relativas a la lectura, entrada, modificación y borrado se registran.
  - Se realizan evaluaciones regulares de forma aleatoria para identificar cualquier posible mal uso.

CONTROLES DE TRANSMISIÓN

Medidas para garantizar que los datos personales no puedan leerse, copiarse, alterarse o eliminarse sin autorización durante la transmisión electrónica o transporte o mientras se guardan en medios de almacenamiento de datos y que sea posible determinar y establecer a qué áreas se van a transferir los datos personales usando las instalaciones de transmisión de datos (incluyendo los procesos de encriptado):

- Registro:
  - Se debe mantener un registro de las áreas de envío y recepción.
  - La tarea se documenta y hace saber a los empleados afectados.
- Transmisión segura de datos entre el servidor y el cliente:
  - La transmisión de datos entre clientes y servidores está encriptada (SSL, SSH, SFTP o VPN).
- Transmisión de back-end:
  - La conexión a sistemas de back-end está protegida.
  - Los datos con altos requisitos de protección están encriptados.
- Minimización de riesgos a través de segmentación de redes:
  - Se ha realizado la segmentación de redes con el objetivo de garantizar que la transmisión de datos se realice sobre una cantidad mínima de elementos de red.
  - Se ha creado un diagrama de red.
  - El sistema relevante se encuentra en un DMZ.
- Portales de seguridad para puntos de transferencia de red:
  - Hay cortafuegos en los puntos de transferencia de red.
  - Los cortafuegos siempre están activos.
  - El usuario no puede desactivar los cortafuegos.
- Fortalecimiento de sistemas de back-end:
  - Las cuentas / contraseñas de servicio preinstaladas se han desactivado.
  - Hay procedimientos operativos estándar en caso de sospecha de mal uso.
  - Hay software antivirus actualizado.
- Descripción de todas las interfaces y campos de datos personales que se van a transmitir:
  - Hay una especificación de interfaz documentada.
  - Hay requisitos procedimentales a la hora de transmitir.
  - Hay una descripción de todos los campos de datos personales que se van a transmitir.
- Autenticación humano-máquina:
  - Autenticación de doble sentido usando procesos criptográficos.
- Acceso a caché local:
  - Todo acceso a cualquier caché local o bases de datos que contienen datos de clientes desde el Cliente con el objeto de y / o para el uso con aplicaciones que el Cliente no ha autorizado queda denegado usando la tecnología incluida.
- Los datos personales no deben transmitirse a través del correo ordinario.
- Proceso de recolección y eliminación:

- Hay normas relativas a la destrucción de medios de almacenamiento de datos de manera que se cumpla con la legislación en materia de protección de datos.
- Hay normas relativas a la destrucción de documentos de manera que se cumpla con la legislación en materia de protección de datos.

- Procedimientos de borrado y destrucción conformes a la legislación en materia de protección de datos:
  - Los medios de almacenamiento de datos deben limpiarse conforme a la legislación en materia de protección de datos antes de ser usados por otro usuario; la recuperación de los datos borrados no es posible o únicamente lo es invirtiendo una cantidad desproporcionada de tiempo y esfuerzo.
  - Los componentes de hardware o los documentos deben destruirse de tal manera que su recuperación no sea posible o únicamente lo sea invirtiendo una cantidad desproporcionada de tiempo y esfuerzo.

CONTROL DE ENTRADA

Medidas para garantizar que es posible, después de la actividad, comprobar y aseverar si se ha entrado, alterado o eliminado datos personales de los sistemas de tratamiento de datos y, en caso afirmativo, quién lo ha hecho (control de entrada):

- Existe documentación relativa a las personas con autorización y responsables del acceso, alteración o eliminación de datos personales en el sistema de tratamiento de datos basándose en sus tareas asignadas.

INSPECCIÓN DE CUMPLIMIENTO DURANTE EL ENCARGO

Medidas para garantizar que el tratamiento de datos personales encargado únicamente se realizará de conformidad con las instrucciones dadas por el Cliente (control del contrato):

- Únicamente el Cliente tiene autorización para controlar encargos en el sistema.
- Ejercicio de la obligación de inspección:
  - El Contratista prestará apoyo al Cliente para cumplir con esta obligación de inspección.
  - Todos los incidentes que se produzcan se informarán al Cliente.
  - El Contratista informará a todos los empleados sobre su obligación de proporcionar información acerca de incidentes.
- Registro de la ejecución del encargo por parte del Contratista:
  - Existen registro que garantizan la total trazabilidad de los pasos operativos individuales realizados como parte de la ejecución del encargo. Se pueden aportar evidencias a petición de que el encargo correspondiente se haya realizado en estricta conformidad con las instrucciones del Cliente (información mínima: cliente/consumidor, acción/pedido parcial, especificación exacta de las fases del proceso/parámetros, personas autorizadas para el tratamiento, fechas, destinatario, si procede).

3. CAPACIDAD PARA RESTAURAR LA DISPONIBILIDAD Y ACCESO A DATOS PERSONALES DE MANERA PUNTUAL EN CASO DE INCIDENTE FÍSICO O TÉCNICO

INSPECCIÓN DE DISPONIBILIDAD

Medidas para garantizar que los datos personales estén protegidos contra la destrucción o pérdida accidental (inspección de disponibilidad):

- Procedimiento de copia de seguridad:
  - Existe un procedimiento de copia de seguridad.
  - Las copias de seguridad se realizan con regularidad.
  - Se especifica una persona o responsable delegado para las copias de seguridad.
  - Se realizarán comprobaciones regulares para determinar si es posible restaurar una copia de seguridad.
- Plan de contingencias:
  - Existe un plan de contingencias que detalla los pasos que deben adoptarse y define qué personas, especialmente por parte del Cliente, tienen que estar informadas del incidente.
- Prueba de los dispositivos para contingencias:
  - Se prueban los generadores de potencia y los dispositivos de protección de exceso de voltaje de forma regular y los parámetros operativos están en vigilancia constante.

LIMITACIONES SOBRE EL USO

Medidas para garantizar que los datos recolectados para distintos propósitos pueden tratarse de forma independiente.

- Los datos de los distintos clientes del Contratista deben guardarse en archivos independientes y en directorios independientes y no deben fusionarse.

4. PROCESO PARA PROBAR, EVALUAR Y ANALIZAR REGULARMENTE LA EFICACIA DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DEL TRATAMIENTO

CONTROL ORGANIZATIVO

- Definición del proceso / control:
  - Hay instrucciones de procedimiento.
  - Se definen procesos y procedimientos operativos para el tratamiento de datos en la empresa.
  - Se realizan comprobaciones sobre la implantación y cumplimiento de los procesos.
- Formación / obligación:
  - Principios de protección de datos, incluyendo medidas técnicas y organizativas.
  - Obligación de mantener la confidencialidad en lo que respecta a secretos comerciales y empresariales, incluyendo los procedimientos del Cliente.
  - Manejo de datos, archivos, medios de almacenamiento y otra documentación en el debido formato y con gran cuidado.
  - Se mantienen registros sobre las sesiones de formación.
  - Las sesiones de formación se repetirán con regularidad, al menos una vez cada tres años.
- Formación / obligación para personal externo:
  - El personal externo únicamente tendrá acceso a sistemas de tratamiento de datos y se le permitirá operar con ellos una vez se haya comprometido a y haya sido formado en confidencialidad de datos y telecomunicaciones y otras obligaciones de confidencialidad.
- Asignación interna de deberes:
  - Las funciones operativas y administrativas se mantienen independientes.
- Nombramiento de sustitutos:
  - Se ha designado un sustituto para todos aquellos deberes / funciones críticas para el funcionamiento de la empresa.

ANEXO 2: SUBCONTRATISTAS

Subcontratista	Servicios prestados por el Subcontratista
Emarsys eMarketing Systems AG Märzstraße 1 1150 Viena Austria	Desarrollo y prestación de la plataforma de marketing.
Emarsys Technologies Kft Kossuth Lajos utca 7-9 First Site Hotel & Business Complex Floor 2 1053 Budapest Ungría	Desarrollo y prestación de la plataforma de marketing.
Emarsys Interactive Services GmbH Stralauer Platz 34 10243 Berlin Alemania	Servicios de agencia relativos a la planificación, ejecución y análisis de la comunicación de marketing.
Emarsys UK Ltd Focus Point 21 Caledonian Road Londres N1 9DX Reino Unido	Soporte al cliente.
LINFORGE Technologies GmbH Brehmstraße 10 1110 Viena Austria	Socio de servicios para la administración del sistema operativo.
CloudAMQP / 84codes AB Sveavägen 98 113 50 Estocolmo Suecia	Mensaje intermediario como servicio.
CDNetworks Europe, Co. Ltd. 85 Gresham St Londres EC2V 7NQ Reino Unido	Red de entrega de contenidos.
Heroku, Inc. The Landmark @ 1 Market St. Suite 300 San Francisco, CA 94105 EE. UU.	Plataforma como servicio. Todo el tratamiento de datos personales tiene lugar dentro de la Unión Europea.
Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 EE. UU.	Motor de almacenamiento de datos. Todo el tratamiento de datos personales tiene lugar dentro de la Unión Europea.
Compose / IBM Corp. 1 New Orchard Road Armonk, New York 10504-1722 EE. UU.	Base de datos como servicio. Todo el tratamiento de datos personales tiene lugar dentro de la Unión Europea.