ANEXO DE TRATAMIENTO DE DATOS

En Madrid a

DE UNA PARTE,
El representante de **ONEY SERVICIOS FINANCIEROS E.F.C., S.A.U.** Salvador Loscertales Martín, mayor de edad con DNI 50834461E y con domicilio social Parque Empresarial Alvento, C/ Vía de los Poblados nº 1, planta 2ª, Edificio A,28033 (Madrid), en adelante **ONEY**.

Y DE OTRA,

En adelante

Ambos intervinientes manifiestan que, a la fecha de la firma del presente acuerdo, sus poderes no han sido revocados ni limitados, reconociéndose, en la representación que ostentan, la capacidad suficiente para la suscripción del presente acuerdo y, a tal efecto,

EXPONEN

I.- Que en fecha de de , ONEY SERVICIOS FINANCIEROS E.F.C., S.A.U. y suscribieron un acuerdo de colaboración para

II.- Que las condiciones de protección de datos aplicables a la relación entre las partes en la prestación del servicio son las siguientes:

Las Partes se comprometen a cumplir, en todo momento, las disposiciones contenidas en el 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 siendo ONEY SERVICIOS FINANCIEROS la responsable del tratamiento de los datos relativos a la prestación del servicio.

Si como consecuencia de la ejecución del contrato como encargado del tratamiento tuviera acceso y efectuara algún tipo de tratamiento de los datos de carácter personal incorporados en los ficheros de los que es responsable el Cliente, lo hará en su condición de "Encargado del Tratamiento", de conformidad con lo previsto en los artículos 28 del RGPD.

En consecuencia, en caso de que se produzca dicho acceso o tratamiento, el Encargado quedará obligado a:

a) Tratar los datos de carácter personal a los que tenga acceso conforme a las instrucciones del responsable del tratamiento.

b) Tratar los datos de carácter personal a los que tenga acceso con la exclusiva finalidad de prestar los servicios objeto del contrato y con sujeción a los criterios, requisitos y especificaciones previstos en el mismo o en sus sucesivas modificaciones, sin que pueda utilizar dichos datos para finalidad distinta.

c) Designar (si ello fuera preceptivo de conformidad con lo dispuesto en el artículo 37 del RGPD) un Delegado de Protección de Datos y comunicar su identidad y datos de contacto al responsable.

d) No comunicar los datos a terceros, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. No obstante lo anterior, el encargado podrá 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 debiese transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o del Derecho de un Estado miembro que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones de interés público.

e) Observar el secreto profesional respecto de los datos personales que trate, obligación que subsistirá aún después de la extinción por cualquier causa del presente contrato.

Oney Servicios Financieros E.F.C., S.A.U:
P.P. Salvador Loscertales Martín

P.P.

ANEXO_GDPR_S_01

f) El Encargado garantiza que las personas autorizadas para tratar datos personales se han comprometido, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que se les informará convenientemente por el encargado, que mantendrá a disposición del responsable la documentación acreditativa del cumplimiento de estas obligaciones.

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

h) Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos.

i) Notificar al responsable, en cuanto las reciba, y asistirle a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes de ejercicio de los derechos de acc eso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad de datos.

j) Facilitar la información relativa a los tratamientos de datos que se van a realizar en el momento de la recogida de los datos. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

k) Colaborar con el Cliente para que este pueda velar por que el tratamiento reúna las garantías para el cumplimiento de lo dispuesto en la normativa de protección de datos de carácter personal.

l) Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos y en la realización de las consultas previas a la autoridad de control.

m) A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros. No obstante lo anterior, el encargado tiene derecho a conservar una copia con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación contratada.

n) 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 a que hubiere lugar a instancia del responsable.

o) El encargado del tratamiento aplicará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

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

Cada Parte mantendrá indemne a la Contraparte frente a cualquier reclamación que derive del tratamiento de datos de carácter personal que se realice en relación con el objeto del presente contrato como consecuencia del incumplimiento de dicha normativa.

Asimismo, en el supuesto de que cualquiera de la Partes utilizara los datos de carácter personal a los que tuviera acceso para cualquier uso distinto al establecido en el presente contrato o contraviniendo la normativa aplicable en materia de tratamientos de datos de carácter personal, y siempre que este hecho resultare acreditado, se compromete a:

Hacerse cargo del pago de cualquier cantidad que por cualquier causa y concepto alguna de ellas se viera obligada a abonar, como consecuencia del uso indebido de los datos, incluidas sanciones administrativas y las eventuales indemnizaciones a cuyo pago fuera condenada ésta, en virtud del correspondiente procedimiento, administrativo o judicial. Asimismo, se comprometen al pago de las costas judiciales y los honorarios de abogados y procurador que se utilizaren en los eventuales procesos que se entablaran en su contra. Abonar la suma que en su momento ambas partes acuerden en concepto de indemnización de daños morales y de reputación comercial sufridos como consecuencia del uso indebido de los ficheros suministrados, cuya cantidad se fijará proporcionalmente a los perjuicios causados

Oney Servicios Financieros E.F.C., S.A.U:
P.P. Salvador Loscertales Martín

P.P.

ANEXO

MEDIDAS DE SEGURIDAD EXIGIBLES AL ENCARGADO DEL TRATAMIENTO

Marcar con una "x" las medidas que resulten de aplicación en cada caso en función de la naturaleza del servicio y de los tipos de datos tratados

1. Control de acceso a locales e instalaciones

Deberán adoptarse medidas para impedir el acceso físico no autorizado a locales e instalaciones en los que existan datos personales. Las medidas incluirán:

- ❒ Sistema de control de acceso.
- ❒ Lector de ID, tarjeta con banda magnética, tarjeta inteligente.
- ❒ (Emisión de) claves.
- ❒ Cierres de puertas (aperturas eléctricas de puertas, etc.).
- ❒ Instalaciones de vigilancia.
- ❒ Sistema de alarma, monitor de video/CCTV.
- ❒ Registro de entradas/salidas de las instalaciones.

2. Control de acceso a sistemas

Deberán adoptarse medidas para impedir el acceso no autorizado a sistemas de IT. Éstas deberán incluir las siguientes medidas técnicas y de organización de identificación y verificación de usuario:

- ❒ Procedimientos de contraseña (incluidos símbolos especiales, longitud mínima, cambio obligatorio de contraseña).
- ❒ Imposibilidad de acceso a usuarios invitados o a cuentas anónimas.
- ❒ Gestión central de acceso a sistemas.
- ❒ Acceso a sistemas de IT sujeto a aprobación por la dirección de RR.HH. y por los administradores de sistemas de IT.
- ❒ Implementación de sistema de seguridad de red, aplicaciones de dispositivos, bases de datos y plataforma.

3. Control de acceso a datos

Deberán adoptarse medidas para impedir que los usuarios autorizados accedan a datos que excedan sus derechos de acceso autorizado y para evitar la [entrada, lectura, copia, eliminación] modificación o revelación de datos no autorizada. Estas medidas incluirán:

- ❒ Derechos de acceso diferenciados.
- ❒ Derechos de acceso definidos conforme a funciones.
- ❒ Registro automático de acceso de usuarios a través de sistemas de IT.
- ❒ Medidas de seguridad de software.

4. Control de divulgación

Deberán adoptarse medidas para impedir el acceso, la modificación o eliminación no autorizados de datos durante una transferencia, y para garantizar que todas las transferencias son seguras y quedan registradas. Estas medidas incluirán:

- ❒ Uso obligatorio de una red privada de plena titularidad para todas las transferencias de datos
- ❒ La conexión de datos se realiza de manera segura mediante VPN, SFPT, etc
- ❒ Prohibición de dispositivos portátiles
- ❒ Creación de un seguimiento de auditoria de todas las transferencias de datos.

5. Control de entradas

Deberán adoptarse medidas para garantizar que se registra toda la gestión y mantenimiento de los datos, y deberá mantenerse un seguimiento de auditoría para verificar si se han producido entradas, modificaciones y retiradas (eliminación) de datos, y de quién las ha realizado. Las medidas deberán incluir:

- ❒ Registro de las actividades de usuarios en los sistemas de IT.

6. Control de trabajo

Deberán adoptarse medidas para garantizar que los datos son tratados en estricto cumplimiento con las instrucciones del importador de datos. Estas medidas deberán incluir:

- ❒ Redacción inequívoca de instrucciones contractuales.
- ❒ Control de cumplimiento contractual.
- ❒ Verificación de empleados.
- ❒ Supervisión de empleados.

7. Control de disponibilidad

Deberán adoptarse medidas para garantizar la protección de los datos frente a destrucción o pérdida accidental.
Estas medidas deberán incluir:

- ❒ Suministro de energía ininterrumpido (UPS por sus siglas en inglés).
- ❒ Procedimientos de continuidad de la actividad
- ❒ Almacenamiento remoto.
- ❒ Sistemas anti-virus/firewall.
- ❒ Copias de seguridad

8. Control de separación

Deberán adoptarse medidas para permitir que los datos recogidos con fines diferentes sean tratados de forma independiente.
Las mismas deberían de incluir:

- ❒ Restricción de acceso a datos almacenados con otros objetivos de acuerdo a las funciones del personal.
- ❒ Separación de sistemas informáticos empresariales.
- ❒ Separación de entornos de prueba y de producción de IT.

9. Control de almacenamiento

Deberán adoptarse medidas para proteger instalaciones comerciales, centros de datos, archivos en papel, servidores, sistemas de copias de seguridad y equipos informáticos, incluidos, a título orientativo y no limitativo, todos los dispositivos móviles y el resto de equipos con capacidad de almacenamiento de información.

Oney Servicios Financieros E.F.C., S.A.U:
P.P. Salvador Loscertales Martín

P.P.

MED_SEG_GDPR_S_01