Acuerdo de tratamiento de los datos

Responsable del Tratamiento: cliente ubicado en la UE (en lo sucesivo, el «**Responsable del Tratamiento**») y

	Encargado del Tratamiento:
Empresa:	One.com Group AB
N.º de registro:	559205-2400
Ciudad:	Malmö
País de registro:	Suecia

(en lo sucesivo, el «**Encargado del Tratamiento**»)
(en lo sucesivo por separado como una «**Parte**» y, de manera colectiva, las «**Partes**»)

han celebrado este:

ACUERDO DE TRATAMIENTO DE LOS DATOS

(en lo sucesivo, el «**Acuerdo**»)
relativo al tratamiento de datos personales por parte del Encargado del Tratamiento en nombre del Responsable del Tratamiento.

1. Los datos personales tratados

1.1 Este Acuerdo se ha celebrado en relación con el uso por parte del Responsable del Tratamiento de los servicios del Encargado del Tratamiento como parte de la suscripción y los servicios adicionales descritos en los «Términos y Condiciones de One.com» (en lo sucesivo, el «**Acuerdo Principal**»).

1.2 El Encargado del Tratamiento trata los tipos de datos personales en nombre del Responsable del Tratamiento en relación con los interesados relevantes según lo especificado en el **Anexo 1**. Los datos personales se refieren a los interesados enumerados en el **Anexo 1**.

1.3 El Encargado del Tratamiento puede iniciar el tratamiento de datos personales en nombre del Responsable del Tratamiento tras la entrada en vigor del Acuerdo. El tratamiento tiene la duración especificada en las instrucciones del **Anexo 1** del Acuerdo.

1.4 El Acuerdo y el Acuerdo Principal son interdependientes y no pueden rescindirse por separado. No obstante, el Acuerdo puede sustituirse por otro acuerdo de tratamiento de datos válido sin rescindir el Acuerdo Principal.

2. Fin

2.1 El Encargado del Tratamiento solo debe tratar los datos personales para los fines que sean necesarios para cumplir con las obligaciones del Encargado del Tratamiento y, en esto, para prestar los servicios establecidos en el Acuerdo Principal.

3. Obligaciones del Responsable del Tratamiento

3.1 El Responsable del Tratamiento garantiza que los datos personales se tratan con fines legítimos y objetivos, y que el Encargado del Tratamiento no trata más datos personales de los necesarios para cumplir con dichos fines.

3.2 El Responsable del Tratamiento es responsable de asegurar que existe una base jurídica válida para el tratamiento en el momento de transferir los datos personales al Encargado del Tratamiento. A petición del Encargado del Tratamiento, el Responsable del Tratamiento se

compromete, por escrito, a rendir cuentas y/o a proporcionar documentación sobre la base del tratamiento.

3.3 Además, el Responsable del Tratamiento garantiza que los interesados a los que pertenecen los datos personales han recibido información suficiente sobre el tratamiento de sus datos personales.

4. Obligaciones del Encargado del Tratamiento

4.1 Todo el tratamiento por parte del Encargado del Tratamiento de los datos personales proporcionados por el Responsable del Tratamiento debe ser de conformidad con las instrucciones preparadas por el Responsable del Tratamiento, y el Encargado del Tratamiento está obligado, además, a cumplir con toda la legislación en materia de protección de datos vigente en dicho momento. Si el Derecho de la Unión o de un Estado miembro de la UE a la que esté sujeto el Encargado del Tratamiento estipula que este debe tratar los datos personales enumerados en el **Anexo 1**, el Encargado del Tratamiento deberá informar al Responsable del Tratamiento de ese requisito legal antes de proceder al tratamiento. No obstante, esto no se aplica si esta legislación prohíbe dicha información por razones importantes de interés público. El Encargado del Tratamiento debe informar inmediatamente al Responsable del Tratamiento si, en su opinión, una instrucción infringe el Reglamento General de Protección de Datos u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4.2 El Encargado del Tratamiento deberá adoptar todas las medidas de seguridad técnicas y organizativas necesarias, incluida cualquier medida adicional, para garantizar que los datos personales no se destruyan, pierdan o deterioren de manera accidental o ilegal, ni se pongan en conocimiento de terceros no autorizados, ni se utilicen de manera abusiva o de cualquier otra forma que sea contraria a la legislación en materia de protección de datos vigente en dicho momento. Estas medidas se describen con más detalle en el **Anexo 2**.

4.3 El Encargado del Tratamiento deberá garantizar que los empleados autorizados para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

4.4 Si así lo solicita el Responsable del Tratamiento, el Encargado del Tratamiento debe declarar y/o documentar que cumple con los requisitos de la legislación aplicable en materia de protección de datos, incluida la documentación relativa a los flujos de datos del Encargado del Tratamiento, así como con los procedimientos/políticas de tratamiento de datos personales.

4.5 Teniendo cuenta la naturaleza del tratamiento, el Encargado del Tratamiento asistirá al Responsable, 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 que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del Reglamento General de Protección de Datos.

4.6 El Encargado del Tratamiento u otro encargado del tratamiento (en lo sucesivo, el «subencargado del tratamiento») debe enviar las solicitudes y objeciones de los interesados al Responsable del Tratamiento, para el tratamiento posterior del Responsable del Tratamiento, a menos que el Encargado del Tratamiento tenga derecho a tramitar dicha solicitud por sí mismo. Si el Responsable del Tratamiento lo solicita, el Encargado del Tratamiento deberá ayudar al Responsable del Tratamiento a responder a dichas solicitudes y/u objeciones.

4.7 Si el Encargado del Tratamiento trata datos personales en otro estado miembro de la UE, el Encargado del Tratamiento debe cumplir con la legislación relativa a las medidas de seguridad en dicho Estado miembro.

4.8 El Encargado del Tratamiento debe notificar al Responsable del Tratamiento cuando se produzca una interrupción en la operación, una sospecha de que se han infringido las normas en materia de protección de datos o se produzcan otras irregularidades en relación con el

tratamiento de los datos personales. El plazo del Encargado del Tratamiento para notificar al Responsable del Tratamiento de una violación de seguridad es de 24 horas desde el momento en que el Encargado del Tratamiento tiene conocimiento de dicha violación. Si el Responsable del Tratamiento lo solicita, el Encargado del Tratamiento deberá asistir al Responsable del Tratamiento en relación con la aclaración del alcance de la violación de la seguridad, incluida la preparación de cualquier notificación a la agencia de protección de datos pertinente y/o a los interesados.

4.9 El Encargado del Tratamiento debe poner a disposición del Responsable del Tratamiento toda la información necesaria para demostrar el cumplimiento del artículo 28 del Reglamento General de Protección de Datos y del Acuerdo. En este marco, el Encargado del Tratamiento permite y contribuye a las auditorías, incluidas las inspecciones, realizadas por el Responsable del Tratamiento o por otro auditor encargado por el Responsable del Tratamiento.

4.10 Además de lo anterior, el Encargado del Tratamiento debe asistir al Responsable del Tratamiento a la hora de garantizar el cumplimiento de las obligaciones del Responsable del Tratamiento en virtud de los arts. 32-36 del Reglamento General de Protección de Datos. Esta asistencia tendrá en cuenta la naturaleza del tratamiento y la información disponible para el Encargado del Tratamiento.

5. Transferencia de datos a subencargados o terceros

5.1 El Encargado del Tratamiento debe cumplir con las condiciones establecidas en el artículo 28, apartado 2 y 4 del Reglamento General de Protección de Datos para recurrir a otro encargado del tratamiento (subencargado del tratamiento). Esto implica que el Encargado del Tratamiento no recurrirá a otro Encargado del Tratamiento (subencargado del tratamiento) para la ejecución del Acuerdo sin la aprobación previa específica o general y por escrito del Responsable del Tratamiento.

5.2 El Responsable del Tratamiento otorga por la presente al Encargado del Tratamiento un poder general para celebrar acuerdos con subencargados del tratamiento. El Encargado del Tratamiento debe notificar al Responsable del Tratamiento cualquier cambio relativo a la adición o sustitución de subencargados del tratamiento a más tardar 30 días antes de que un nuevo subencargado comience a tratar los datos personales. El Responsable del Tratamiento puede objetar de manera razonable y pertinente contra dichos cambios en un plazo de 14 días a partir de la recepción de la notificación. Si el Encargado del Tratamiento sigue deseando recurrir a un subencargado del tratamiento al que el Controlador de Datos ha objetado, las Partes tienen derecho a rescindir el Acuerdo (véase el art. 7).

5.3 Cuando el Responsable del Tratamiento haya aprobado que el Encargado del Tratamiento puede recurrir a un subencargado del tratamiento, este deberá imponer al subencargado las mismas obligaciones que se establecen en el Acuerdo. Esto se ejecuta a través de un contrato u otro acto jurídico en virtud de la legislación europea o de un Estado miembro. Debe asegurarse, por ejemplo, que el subencargado del tratamiento de datos ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas de manera que el tratamiento cumpla con los requisitos del Reglamento General de Protección de Datos (términos «back-to-back»).

5.4 Si el subencargado del tratamiento incumple sus obligaciones en materia de protección de datos, el Encargado del Tratamiento seguirá siendo plenamente responsable ante el Responsable del Tratamiento por el cumplimiento de las obligaciones del subencargado.

5.5 La divulgación y la transferencia a terceros países u organizaciones internacionales de los datos personales del Responsable del Tratamiento y el uso interno por parte de estos solo puede tener lugar de conformidad con las instrucciones documentadas del Responsable del Tratamiento, a menos que lo estipule la legislación de la UE o de un Estado miembro al que esté sujeto el Responsable del Tratamiento. En este caso, el Encargado del Tratamiento debe

notificar al Responsable del Tratamiento de este requisito legal antes del tratamiento, a menos que la ley prohíba dicha notificación por razones importantes de interés público.

5.6 Si los datos personales estipulados en el **Anexo** 1 se transfieren a subencargados fuera de la UE/del EEE, deberá indicarse en dicho acuerdo que la legislación en materia de protección de datos aplicable en el país del Responsable del Tratamiento se aplica a los subencargados. Además, si el subencargado del tratamiento receptor está establecido dentro de la UE/del EEE, debe indicarse en dicho acuerdo de tratamiento de los datos que deben cumplirse los requisitos legales específicos del país receptor de la UE relativos a los encargados del tratamiento, por ejemplo, en lo que respecta a las exigencias de notificación a las autoridades nacionales.

5.7 El Encargado del Tratamiento está obligado a firmar acuerdos escritos de tratamiento de datos con subencargados dentro de la UE/del EEE. En cuanto a los subencargados fuera de la UE/del EEE, el Encargado del Tratamiento debe garantizar mecanismos de transferencia suficientes y celebrar un acuerdo de subtratamiento de los datos mediante la celebración de acuerdos estándar de conformidad con las cláusulas contractuales tipo de la Comisión Europea (en lo sucesivo, los **«contratos tipo**») basados en el Reglamento 2021/914/UE de 4 de junio de 2021.

5.8 En el momento de la firma de este Acuerdo, el Encargado del Tratamiento recurre a los subencargados enumerados en el **Anexo 3**.

6. Responsabilidad

6.1 La responsabilidad de las Partes se rige por el Acuerdo Principal.

6.2 La responsabilidad de las Partes en caso de daños y perjuicios según este Acuerdo se rige por el Acuerdo Principal.

7. Fecha de entrada en vigor y terminación

7.1 Este Acuerdo entra en vigor al mismo tiempo que el Acuerdo Principal. En caso de terminación del Acuerdo Principal, este Acuerdo también terminará. No obstante, el Encargado del Tratamiento seguirá estando sujeto a las obligaciones estipuladas en este Acuerdo, siempre y cuando el Encargado del Tratamiento trate datos personales en nombre del Responsable del Tratamiento.

7.2 Una vez finalizados los servicios de tratamiento, el Encargado del Tratamiento está obligado, a petición del Responsable del Tratamiento, a eliminar o devolver todos los datos personales al Responsable del Tratamiento, así como a eliminar las copias existentes, a menos que la retención de los datos personales esté prescrita por la legislación nacional o de la UE.

8. Legislación aplicable y jurisdicción

8.1 Cualquier reclamación o disputa que surja de o en relación con este Acuerdo debe resolverse por un juzgado competente de primera instancia en la misma jurisdicción y con la misma elección de la legislación que se establece en el Acuerdo Principal.

9. Firmas

En nombre del Responsable del Tratamiento:

_____

[Nombre] [Título]

En nombre del Encargado del Tratamiento:

Ronni Engelhardt, CEO

Anexo 1
Categorías de interesados, tipos de datos personales e instrucciones

1. Categorías de interesados:

- El Encargado del Tratamiento tratará información de contacto de los clientes actuales, potenciales o antiguos y de miembros, empleados, proveedores, socios comerciales, colaboradores y afiliados del Responsable del Tratamiento.
- El Encargado del Tratamiento puso su sistema a disposición del Responsable del Tratamiento como un servicio alojado y este no puede determinar todas las categorías de interesados. Si el Responsable del Tratamiento alberga datos sobre otras categorías de interesados en el sistema del Encargado del Tratamiento, será obligación del Responsable del Tratamiento registrar esta información.

2. Tipos de datos personales:

- Información de contacto y de identificación, incluido el correo electrónico
- Direcciones IP
- Nombres de dominio
- Nombres de usuario
- Información sobre membresías

- Datos analíticos y de uso
- Historial de pedidos e información
- Contratos
- Comunicación
- Soporte
- Fotografías
- Pueden darse otros tipos de datos personales

3. Instrucciones

Servicio

El Encargado del Tratamiento puede tratar datos personales relativos a los interesados con el fin de entregar, desarrollar, gestionar, administrar y manejar los servicios del Acuerdo Principal, incluyendo asegurar la estabilidad y el tiempo de actividad de nuestros servidores, y cumplir con los requisitos legales.

Plazo de conservación

Los datos personales almacenados/alojados en nuestros sistemas se eliminan o se anonimizan en un plazo razonable después de que el Responsable del Tratamiento haya rescindido completamente el Acuerdo Principal. Excepciones son los datos en los que existe un requisito legal para que el Encargado del Tratamiento los guarde durante más tiempo. Este tipo de datos suele eliminarse por regla general en un plazo de ocho semanas, pero puede eliminarse antes. Los otros tipos de datos que se almacenan en registros, etc., se eliminarán pasado un tiempo razonable, por regla general en un plazo de 8 semanas, tras lo cual se eliminarán del sistema del Encargado del Tratamiento.

Lugar de tratamiento

El tratamiento de los datos personales cubiertos por el Acuerdo no debe realizarse sin el consentimiento previo y por escrito del Responsable del Tratamiento en lugares distintos de la dirección del Responsable del Tratamiento y de la dirección de los subencargados de datos enumerados en el Anexo 3.

Inspección del Encargado del Tratamiento

El Encargado del Tratamiento debe obtener una vez al año, a sus expensas, un informe de auditoría/inspección de un tercero sobre el cumplimiento por parte del Encargado del Tratamiento de este Acuerdo y los Anexos. El informe u otro formato de auditoría debe remitirse al Responsable del Tratamiento o publicarse en el sitio web de este lo antes posible una vez preparado.

Anexo n.° 2
Medidas de seguridad

Dominio	Prácticas
Organización de la seguridad de la información	**Propiedad de la seguridad**. One.com ha designado a un responsable de seguridad encargado de coordinar y supervisar las normas y procedimientos de seguridad. Una gobernanza formada por personas de nivel C asiste y guía al responsable de seguridad. **Papeles de seguridad y responsabilidades**. El personal de One.com con acceso a los datos de los clientes está sujeto a

Dominio	Prácticas
	obligaciones de confidencialidad, lo que se enfatiza en el momento de la contratación y se recuerda continuamente. **Gestión de riesgos**. One.com realiza continuamente evaluaciones de riesgos, que forman parte de la gestión de riesgos, antes de tratar los datos de los clientes o de lanzar los servicios. La pista de la gestión de riesgos sí permite centrarse en amenazas relevantes, priorizando, estructurando y mitigando los riesgos por encima de lo aceptado. Se implementa la copia de seguridad. El Encargado del Tratamiento conserva sus documentos de seguridad según sus requisitos de retención después de que hayan dejado de estar en vigor.
Gestión de activos	**Inventario de activos**. El Encargado del Tratamiento mantiene un inventario de todos los soportes en los que se almacenan los datos de los clientes. El acceso a los inventarios de dichos soportes está restringido al personal del Encargado del Tratamiento autorizado por escrito a tener dicho acceso. **Manejo de activos** - One.com clasifica los datos de los clientes para ayudar a identificarlos y permitir que el acceso a los mismos esté debidamente restringido. - El personal del Encargado del Tratamiento debe obtener la autorización del Encargado del Tratamiento antes de almacenar los datos de los clientes en dispositivos portátiles, acceder de manera remota a los datos de los clientes o tratar los datos de los clientes fuera de las instalaciones del Encargado del Tratamiento.
Seguridad de los Recursos Humanos	**Formación en seguridad**. One.com informa a su personal sobre los procedimientos de seguridad pertinentes y sus respectivas funciones, así como aborda las nuevas amenazas, etc., en las que los empleados desempeñan un papel vital.
Seguridad física y medioambiental	**Acceso físico a las instalaciones**. One.com limita el acceso a las instalaciones donde se encuentran los sistemas de información que tratan los datos de los clientes a las personas autorizadas identificadas. **Acceso físico a los componentes**. One.com garantiza restricciones suficientes de los soportes que contienen datos de los clientes. **Protección contra las interrupciones**. One.com utiliza una serie de sistemas estándar de la industria para protegerse contra la pérdida de datos debida a un fallo en el suministro eléctrico, una inundación, un incendio o una interferencia en la línea. **Eliminación de componentes**. One.com utiliza procesos estándar de la industria para eliminar los datos de los clientes cuando ya no son necesarios.
Gestión de comunicaciones y operaciones	**Política operativa**. One.com mantiene documentos de seguridad que describen sus medidas de seguridad y los procedimientos y responsabilidades pertinentes de su personal que tiene acceso a los datos de los clientes. **Procedimientos de recuperación de datos**

Dominio	Prácticas
	- One.com almacena copias de los datos de los clientes y procedimientos de recuperación de los datos en un lugar diferente del que se encuentra el equipo informático principal que trata los datos de los clientes. - One.com cuenta con procedimientos específicos implementados que regulan el acceso a las copias de los datos de los clientes. **Programas malignos.** One.com cuenta con controles antiprogramas malignos para ayudar a evitar que programas malignos obtengan acceso no autorizado a los datos de los clientes, incluidos aquellos procedentes de redes públicas. También se ha implementado un antivirus. **Registro de eventos**. One.com registra, o permite que el cliente registre, el acceso y el uso de los sistemas de información que contienen datos del cliente, registrando el identificador de acceso, la hora, la autorización concedida o denegada y la actividad relevante. **Encriptación.** Las comunicaciones por Internet entre los sistemas que manejan datos personales están encriptadas.
Control de acceso	**Política de acceso**. One.com mantiene un registro de los privilegios de seguridad de las personas que tienen acceso a los datos de los clientes. **Autorización de acceso** - One.com desactiva las credenciales de autentificación que no se han utilizado durante un periodo de tiempo que no excede los seis meses. - One.com identifica al personal que puede conceder, modificar o cancelar el acceso autorizado a los datos y recursos. - One.com se asegura de que, cuando más de una persona tenga acceso a los sistemas que contienen datos de los clientes, las personas tendrán identificadores/credenciales separados. **Principio de mínimo privilegio** - One.com restringe el acceso a los datos de los clientes solo a aquellas personas que requieren dicho acceso para realizar su labor. **Integridad y confidencialidad** - One.com instruye a su personal para que desactive las sesiones administrativas cuando abandone las instalaciones o deje desatendidos los ordenadores. - One.com almacena las contraseñas de manera que sean ininteligibles mientras estén vigentes. **Autenticación** - One.com utiliza prácticas estándar de la industria para identificar y autenticar a los usuarios que intentan acceder a los sistemas de información. - Cuando los mecanismos de autenticación se basan en contraseñas, el Encargado del Tratamiento requiere que las contraseñas se renueven regularmente.

Dominio	Prácticas
	- One.com garantiza que los identificadores desactivados o caducados no se concedan a otras personas. - One.com monitoriza, o permite al cliente monitorizar, los intentos repetidos de acceder al sistema de información utilizando una contraseña no válida. - One.com mantiene procedimientos estándar de la industria para desactivar las contraseñas corrompidas o reveladas inadvertidamente. - One.com utiliza prácticas de protección de contraseñas estándar de la industria, incluyendo prácticas diseñadas para mantener la confidencialidad e integridad de las contraseñas, cuando se asignan y distribuyen, y durante su almacenamiento. **Diseño de la red**. One.com dispone de controles para evitar que las personas asuman derechos de acceso que no se les han asignado para acceder a datos de clientes a los que no están autorizados a acceder.
Gestión de incidentes de seguridad de la información	**Proceso de respuesta a incidentes** - One.com mantiene un registro de las violaciones de la seguridad con una descripción de la violación, el período de tiempo, las consecuencias de la violación, el nombre del informante y a quién se informó de la violación, y el procedimiento para recuperar los datos. - Para cada violación de la seguridad que constituya un incidente de seguridad, la notificación por parte de One.com se realizará sin demora indebida y, en cualquier caso, en un plazo de 72 horas. - One.com hace un seguimiento, o permite al cliente hacer un seguimiento, de las divulgaciones de datos de los clientes, incluyendo qué datos se han divulgado, a quién y en qué momento.
Gestión de continuidad del negocio	- One.com mantiene planes de emergencia y de contingencia para las instalaciones en las que se encuentran los sistemas de información del Encargado del Tratamiento que tratan datos de clientes. - El almacenamiento redundante de One.com y sus procedimientos de recuperación de los datos están diseñados para intentar reconstruir los datos de los clientes en su estado original o replicado por última vez antes del momento en que se perdieron o destruyeron.

Anexo n.° 3
Lista de subencargados del tratamiento

Proveedor	Ubicación	Función	Actualizado
Global Connect A/S	DK	Centro de datos	22/02/2021
Interxion	DK	Centro de datos	12/04/2021
Interxion	DK/UK/NL/FR/DE	PoP (punto de presencia)	12/04/2021
Equinix	SE	PoP (punto de presencia)	12/04/2021