ANEXO I. CONTRATO DE ACCESO A DATOS PERSONALES POR CUENTA DE TERCEROS (ENCARGO DE TRATAMIENTO)

Mediante las siguientes cláusulas contractuales y de conformidad con el artículo 28 del RGPD Reglamento (UE) 2016/679 del 27 de abril 2016 y 33 de la LOPDGDD (E) *Ley Orgánica 3/2018, de 5 de diciembre* se establecerán los límites establecidos para el tratamiento de datos personales que ODILO TID S.L. encargada del tratamiento (en adelante ENCARGADO), tratará por cuenta de CLIENTE, responsable del tratamiento (en adelante RESPONSABLE), para prestar el servicio de **gestión de préstamo bibliotecario.**

Ambas partes se reconocen recíprocamente la capacidad legal necesaria para el suscribir el presente contrato de prestación de servicios con acceso a datos personales y establecen las siguientes

INSTRUCCIONES PARA EL TRATAMIENTO DE DATOS

1. Objeto, naturaleza y finalidad del encargo

El tratamiento de datos consistirá en: La gestión del préstamo bibliotecario de contenidos digitales a los usuarios autorizados por el responsable mediante:

- Un control de accesos de los perfiles de usuario definidos por el responsable
- El seguimiento y control de las condiciones de uso que el responsable establezca para sus usuarios, que serán gestionadas a través de estadísticas de uso en la plataforma.
    - Parte de esas estadísticas son necesarias para el correcto cumplimiento de las condiciones del préstamo establecidas por el responsable
    - Otra parte de esas estadísticas permiten al responsable gestionar de manera más eficiente los contenidos digitales elegidos para su plataforma

Las operaciones de tratamiento autorizadas serán las estrictamente necesarias para alcanzar la finalidad del encargo y se concretan en la recogida y captura de datos, su organización y estructuración, el almacenamiento, su uso o tratamiento, la limitación y su supresión o destrucción.

2. Tipo de datos personales y categoría de interesados

Los datos personales a que tendrá acceso el ENCARGADO corresponden a las siguientes categorías de interesados: **Usuarios de la plataforma**

Y se concretan en los siguientes datos o categorías de datos:

Identificativos: identificador y contraseña, ID reader asociado.

Datos de uso: perfilado de usuario en base a su actividad en la plataforma en relación con los contenidos digitales a los que accede. Estadísticas de uso.

Que se incluyen en los ficheros y actividades de tratamiento del responsable y que éste pone a su disposición para poder desarrollar el servicio contratado informándole que se les debe aplicar las necesarias medidas de seguridad conforme al artículo 32 del RGPD.

3. Obligaciones y derechos del RESPONSABLE

El RESPONSABLE garantiza que los datos facilitados al ENCARGADO se han obtenido lícitamente y que son adecuados, pertinentes y limitados a los fines del tratamiento de conformidad con los artículos 5,6 y 8 del RGPD o sus equivalentes en el estado miembro de aplicación.

Corresponderá al RESPONSABLE facilitar el derecho de información sobre el tratamiento de datos objeto del presente contrato de encargo y para facilitar esta tarea podrá disponer en la plataforma "espacios" habilitados a tal efecto donde podrá incluir la información necesaria conforme a los art. 13 y 14 del RGPD. En caso de no atender esta obligación el encargado lo pondrá en conocimiento del responsable para que lo subsane a la mayor brevedad posible.

El RESPONSABLE pondrá a disposición del ENCARGADO cuanta información sea necesaria para ejecutar las prestaciones objeto del encargo específicamente los datos de usuarios y contraseñas necesarios para verificar los accesos autorizados.

El RESPONSABLE deberá realizar, cuando sea necesario, la preceptiva evaluación del impacto a la protección de datos personales sobre aquellas operaciones de tratamiento a realizar por el encargado e igualmente en caso necesario las consultas previas a la Autoridad de Control.

El RESPONSABLE deberá velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado supervisando el tratamiento, incluida la realización de inspecciones y auditorías si lo considera necesario.

El RESPONSABLE advierte al ENCARGADO que, si determina por su cuenta los fines y los medios del tratamiento, será considerado responsable del tratamiento y estará sujeto a cumplir las disposiciones de la normativa vigente aplicables como tal.

4. Obligaciones y derechos del ENCARGADO

El ENCARGADO se obliga a respetar todas las obligaciones que pudieran corresponderle como encargado del tratamiento conforme lo dispuesto en la normativa vigente y cualquier otra disposición o regulación que le fuera igualmente aplicable.

El ENCARGADO no destinará, aplicará o utilizará los datos a los que tenga acceso para un fin distinto al del presente encargo o que suponga el incumplimiento de este contrato.

El ENCARGADO pondrá a disposición del RESPONSABLE la información necesaria para demostrar el cumplimiento del contrato, permitiendo las inspecciones y auditorías necesarias para evaluar el 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.

El ENCARGADO llevará, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable cuando proceda, todo ello conforme al art. 30.2 del RGPD.

5. Personal autorizado para realizar el tratamiento

El ENCARGADO garantiza que el personal autorizado para realizar el tratamiento se ha comprometido de forma expresa y por escrito a respetar la confidencialidad de los datos o que está sujeto a una obligación legal de confidencialidad.

El ENCARGADO tomará medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones del RESPONSABLE o esté obligada a ello en virtud de la legislación vigente.

El ENCARGADO garantiza que el personal autorizado para realizar el tratamiento ha recibido la formación necesaria para asegurar que no se pondrá en riesgo la protección de datos personales.

El ENCARGADO mantendrá a disposición del RESPONSABLE la documentación acreditativa del cumplimiento de la obligación establecida en el presente apartado.

6. Medidas de seguridad

El ENCARGADO manifiesta estar al corriente en lo que concierne a las obligaciones derivadas de la normativa de protección de datos, especialmente en lo que se refiere a la implantación de las medidas de seguridad para las diferentes categorías de datos y de tratamiento establecidas en el artículo 32 del RGPD.

El ENCARGADO garantiza que se implementarán adecuadamente dichas medidas de seguridad y cooperará con el RESPONSABLE para avalar su cumplimiento.

El RESPONSABLE realizará un análisis de los posibles riesgos derivados del tratamiento para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos de los interesados y, si determinara que existen riesgos, trasladará al ENCARGADO un informe con la evaluación de dichos riesgos para que proceda a la implementación de medidas adecuadas para evitarlos o mitigarlos.

El ENCARGADO, por su parte, deberá analizar los posibles riesgos y otras circunstancias que puedan incidir en la seguridad que le sean atribuibles, debiendo informar, si los hubiere, al RESPONSABLE para evaluar su impacto.

En cualquier caso, el ENCARGADO garantiza que se implementará, por defecto, las siguientes medidas de protección de datos, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento:

- Control de acceso individualizado de usuarios por contraseña y correo electrónico.
- Política de renovación periódica de contraseña y complejidad de la mismas.
- Comunicación cliente-servidor mediante protocolos seguros y encriptados (HTTPS).
- Uso de librerías de protección contra el código malicioso.
- Uso de cortafuegos en los servidores que despliegan soluciones de Odilo en SaaS
- Auditoría de acciones de usuarios y procesos ejecutados.
- Auditoría de accesos a la aplicación.
- Monitorización en tiempo real 24x7 del funcionamiento de los servicios y aplicaciones.
- Servicio de alertas de disponibilidad de las aplicaciones.
- Actualización constante del software base utilizado para ofrecer las máximas garantías de seguridad.
- Copias de seguridad diarias de los datos de forma geo-redundada.
- Servicio en SaaS gestionado con un referente mundial en provisión segura de servicios en la nube: Amazon Web Services.
- Simulación de escenarios de continuidad del negocio (restauración frente a contingencias).
- Panel de gestión de incidencias de seguridad.
- Habilitación de espacios para cumplimiento de obligaciones informativas: aviso legal, política de privacidad, normas de uso.

El tratamiento objeto del encargo dispone además de los estándares de certificación siguientes:

- ISO 27001 sistema de seguridad de la información
- ENS (Esquema Nacional de Seguridad) en categoría alta
- ISO 22301 Sistema de continuidad de negocio
- ISO 9001 sistema de gestión de calidad
- ISO 27017 – Controles de Seguridad para Servicios en la Nube
- ISO 27018 – Protección de Información Personal en la Nube
- ISO 27701 Gestión de Información de Privacidad

Por su parte el subprocesador elegido para el alojamiento cloud dispone igualmente de certificaciones propias https://aws.amazon.com/es/compliance/

Quedando así garantizada, a criterio de entidad independiente de certificación:

- La confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- La disponibilidad y el acceso a datos de forma rápida en caso de incidente físico o técnico.
- Procedimientos de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
- Y si fuese obligatorio además se podría aplicar una Seudonimización y cifrado de datos personales.

7. Violación de la seguridad

Las violaciones de seguridad que tenga conocimiento el ENCARGADO deberán notificarse, sin dilación indebida y en un máximo de 24/48 horas, al RESPONSABLE para su conocimiento, así como la aplicación de medidas para remediar y mitigar los efectos ocasionados. No será necesaria la notificación cuando sea improbable que comporte un riesgo para los derechos y las libertades de las personas físicas.

La notificación de una violación de seguridad se realizará conforme al art. 33 del RGPD y siguiendo los procedimientos de comunicación establecidos por las Autoridades de Control

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

8. Comunicación de los datos a terceros

El ENCARGADO no podrá comunicar los datos a otros destinatarios, salvo que hubiera obtenido una autorización previa y por escrito del RESPONSABLE; la cual, de existir, se anexará al presente contrato.
La transmisión de datos a Autoridades públicas en el ejercicio de sus funciones públicas no es considerada comunicaciones de datos, por lo que no se precisará de la autorización del RESPONSABLE si dichas transmisiones son necesarias para alcanzar la finalidad del encargo.

9. Transferencias internacionales de datos

El ENCARGADO no podrá realizar transferencias de datos a terceros países u organizaciones internacionales no establecidos en la UE, salvo que hubiera obtenido una autorización previa y por escrito del RESPONSABLE; la cual, de existir, se anexará al presente contrato.

10. Subprocesamiento de datos

Se autoriza al encargado a establecer el subprocesamiento correspondiente al alojamiento cloud en modalidad SaaS (Software como servicio) con la empresa Amazon Web Services

Alojamiento cloud en modalidad SaaS (Software como servicio)
Amazon Web Services EMEA SARL, sucursal en España
Calle Ramírez de Prado, 5, 28045 Madrid, España
Registro mercantil de Madrid • tomo 36.807, folio 1, hoja m-659089 • cif es w0185696b

Odilo despliega la solución (servidores y datos) en distintas ubicaciones dependiendo de la situación del cliente, concretamente:

- Todos los clientes de Europa se alojan en servidores AWS de la República de Irlanda, dentro de la Unión Europea.
  AWS incorpora de forma complementaria una adenda de procesamiento de datos "AWS GDPR" en sus términos de servicio que incluye la decisión de ejecución de la Comisión Europea 914/2021 entre encargados y por lo tanto, entendemos que ofrecen garantías suficientes en materia de privacidad cuando se realizan TID en aquellos casos en que un cliente europeo precisase alojar datos fuera de la UE. Consultar en este enlace:
- https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf

- Todos los clientes de Norteamérica se alojan en servidores AWS de Virginia del Norte (USA).
- Todos los clientes de Australia se alojan en servidores de AWS de Sidney.
- Para clientes ubicados en otras regiones distintas de las anteriores, se les ofrece la oportunidad de alojar el servicio en Irlanda o USA, a su elección dependiendo de las restricciones de tratamiento de datos personales y requerimientos de rendimiento de la aplicación.

Se autoriza al encargado a establecer el subprocesamiento correspondiente al Chatbot del Servicios Técnico de Atención al Clientes (SAT) con la empresa Zendesk Inc. Con domicilio social 1019 Market Street, San Francisco, CA 94.103 dirección en España Paseo de la Castellana 43,28046 Madrid. Que aporta como garantía para las Transferencias Internacionales de Datos cláusulas contractuales tipo de la Comisión versión 2021/914 y BCR de octubre de 2020 formalizadas a través de la autoridad de control de Irlanda y Holanda (Países Bajos) lo que a nuestro criterio garantiza un nivel de protección de datos equivalente al europeo. Política de privacidad Zendesk

El subprocesador, 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 subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

11. Derechos de los interesados

El ENCARGADO creará, siempre que sea posible y teniendo cuenta la naturaleza del tratamiento, las condiciones técnicas y organizativas necesarias para asistir al RESPONSABLE en su obligación de responder las solicitudes de los derechos del interesado.

En el caso que el ENCARGADO reciba una solicitud para el ejercicio de dichos derechos, deberá comunicarlo al RESPONSABLE de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente con otras informaciones que puedan ser relevantes para resolver la solicitud.

12. Delegado de Protección de Datos

El ENCARGADO tiene designado un delegado de protección de datos con el que podrá contactar en caso de considerarlo necesario en el siguiente email: dpo@odilo.us

13. Responsabilidad

Conforme el artículo 82 del RGPD, el ENCARGADO se hace responsable frente al RESPONSABLE por los daños y perjuicios causados a interesados o terceros incluidas las sanciones administrativas, que se deriven de reclamaciones judiciales o extrajudiciales o de procedimientos sancionadores de la Autoridad de control, que sean consecuencia de la inobservancia de las instrucciones asumidas en el presente contrato.

14. Duración

El presente acuerdo tiene una duración asociada a la duración del contrato de servicios establecida entre las partes o en su caso al plazo establecido en la licitación para la prestación del servicio.

15. Fin de la prestación de servicio

La finalización de prestación de servicios objeto de este contrato vendrá reglada por el siguiente procedimiento entre el ENCARGADO y el RESPONSABLE:

- Se comunicará entre ambas partes la **fecha de finalización de prestación del servicio** con al menos una semana de antelación, idealmente un mes antes si fuera posible, para la correcta gestión técnica de la desconexión.
- **Devolver** los datos de auditoría y/o estadísticas de uso asociadas a los usuarios durante la prestación del servicio; para ello el RESPONSABLE deberá descargar esa información antes de la

desconexión. Si estos datos no fueran exportables desde el portal de administración, el ENCARGADO realizará una exportación manual en formato Excel/CSV desde la base de datos.

- **Devolver** cualquier dato personal de los usuarios, en aquellos casos en que la prestación del servicio dispusiera de autorregistro de nuevos usuarios; para ello el RESPONSABLE deberá descargar esa información antes de la desconexión.
- En el caso de que el RESPONSABLE no disponga de los recursos digitales propios que importó como administrador en la solución, se podrán **devolver dichos recursos digitales propios** bajo demanda.
- En la fecha acordada para la finalización del servicio, **inhabilitar la URL** donde se aloja el servicio en SaaS (DNS) y **desconectar todas las integraciones** con servicios externos (por ejemplo, sistema de autenticación del RESPONSABLE, plataformas de descubrimiento,).
- Por último, el ENCARGADO procederá a la **supresión definitiva de la información** alojada en la base de datos. No procederá la supresión de datos cuando se requiera su conservación por una obligación legal, en cuyo caso el RESPONSABLE deberá informar previamente al ENCARGADO para que proceda a la custodia de los mismos bloqueando los datos y limitando su tratamiento en tanto que pudieran derivarse responsabilidades de su relación con el RESPONSABLE.

El ENCARGADO mantendrá el deber de secreto y confidencialidad de los datos incluso después de finalizar la relación objeto de este contrato. Y para que conste a los efectos oportunos, en prueba de conformidad de las partes, firman el presente contrato, por duplicado, en el lugar y la fecha indicados en el encabezamiento.

Fdo. El Responsable	23038433T RODRIGO RODRIGUEZ (R: B30856439) Firmado digitalmente por 23038433T RODRIGO RODRIGUEZ (R: B30856439) Fecha: 2022.12.22 16:11:03 +01'00' Fdo. El Encargado ODILO TID S.L. B30856439