

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

Mediante las siguientes cláusulas contractuales y de conformidad con la legislación Estatutaria de 1581 de 2012, ODILO se compromete a cumplir con las obligaciones pertinentes en materia de protección de datos personales.

Así mismo, de conformidad con el artículo 28 del RGPD Reglamento (UE) 2016/679 del 27 de abril 2016 y 33 de la LOPDGDD y la *Ley Orgánica 3/2018, de 5 de diciembre* se establecerán los límites establecidos para el tratamiento de datos personales que ODILO TID S.L. (España) encargada del tratamiento (en adelante ENCARGADO), tratará por cuenta de CLIENTE, responsable del tratamiento (en adelante RESPONSABLE), para prestar el servicio de **gestión de archivo y/o preservación digital**.

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 archivo y/o preservación digital por los usuarios autorizados por el responsable mediante:

- Un control de accesos de los perfiles de usuario definidos por el responsable
- Una monitorización de la actividad de los usuarios autorizados
- Un alojamiento en modalidad SaaS

Las operaciones de tratamiento autorizadas serán las estrictamente necesarias para alcanzar la finalidad del encargo.

RECOGIDA O CAPTURA DE DATOS MEDIANTE DIGITALIZACIÓN

X

ORGANIZACIÓN Y ESTRUCTURACIÓN

X

ALMACENAMIENTO/CONSERVACIÓN

X

LIMITACIÓN

X

SUPRESIÓN O DESTRUCCIÓN

X

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:

Empleados, Clientes / Usuarios, Proveedores, Asociados o miembros, Propietarios o Arrendatarios, Pacientes, Estudiantes, Personas de contacto, Padres o tutores. Representante legal, Solicitantes, Beneficiarios, Cargos Públicos

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

Identificativos

De características personales

De circunstancias sociales

Académicos y profesionales

De empleo

De información comercial

Económicos, financieros o de seguros

De transacciones

De categorías especiales de datos

Todos ellos contenidos en documentos y expedientes a digitalizar o preservar según corresponda y 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

El RESPONSABLE pondrá a disposición del ENCARGADO cuanta información sea necesaria para ejecutar las prestaciones objeto del encargo específicamente los documentos o expedientes objeto de digitalización o preservación y que incluyan datos de carácter personal.

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 REGP.

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 impacto 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 implementarán 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:

Política	Objetivos
Control de acceso individualizado de usuarios por contraseña y correo electrónico.	Uso de aplicaciones únicamente por personas autorizadas
Política de renovación periódica de contraseña y complejidad de la mismas.	Impedir vulneración de seguridad por contraseñas débiles.
Comunicación cliente-servidor mediante protocolos seguros y encriptados (HTTPS).	Métodos de comunicaciones y envío de datos mediante protocolos protegidos
Uso de librerías de protección contra el código malicioso.	Software seguro frente a intentos de ataques externos.
Uso de cortafuegos en los servidores que despliegan soluciones de Odilo en SaaS	Servidores seguros frente a intentos de ataques externos
Auditoría de acciones de usuarios y procesos ejecutados.	Control permanente de la seguridad del software y usuarios
Auditoría de accesos a la aplicación.	Control funcionamiento de las aplicaciones.
Monitorización en tiempo real 24x7 del funcionamiento de los servicios y aplicaciones.	Control de accesibilidad y disponibilidad de las aplicaciones
Servicio de alertas de disponibilidad de las aplicaciones.	Asistencia y atención inmediata en caso de fallos del servicio.
Actualización constante del software base utilizado para ofrecer las máximas garantías de seguridad.	Sistemas y aplicaciones actualizadas frente a nuevos bugs y fallos informáticos.
Copias de seguridad diarias de los datos de forma geo-redundada.	Capacidad de recuperación frente a contingencias
Servicio en SaaS gestionado con un referente mundial en provisión segura de servicios en la nube: Amazon Web Services.	Tecnología y aplicaciones en vanguardia y dispuesta para ofrecer las máximas prestaciones
Simulación de escenarios de continuidad del negocio (restauración frente a contingencias).	Preparación profesional y tecnológica para enfrentar situaciones extraordinarias
Panel de gestión de incidencias de seguridad.	Tratamiento y revisión de incidencias de la aplicación
Aviso legal incluyendo condiciones y términos de uso y política de privacidad.	Declaración de derechos, responsabilidades y limitaciones en tratamiento de la información.
Aviso sobre el tratamiento de la información en los portales de administración.	Declaración de las responsabilidades de ODILO y cliente sobre la información gestionada a través del producto.

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) nivel Alto
- ISO 22301 Sistema de continuidad de negocio
- ISO 9001 sistema de gestión de calidad
- ISO 14721 Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS).
- 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 y 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 conforme al art. 33 del RGPD deberá contener, como mínimo, la siguiente información:

- Descripción de la naturaleza de la violación.
- Categorías y el número aproximado de interesados afectados.
- Categorías y el número aproximado de registros de datos afectados.
- Posibles consecuencias.
- Medidas adoptadas o propuestas para remediar o mitigar los efectos.

- Datos de contacto donde pueda obtenerse más información (DPO, responsable de seguridad, etc.).

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 Inc.

*Alojamiento cloud en modalidad SaaS (Software como servicio)
Amazon Web Services Inc.
410 Terry Avenue North Seattle Washington 98109-5210
Mediante contrato firmado con fecha:24 de marzo de 2011.*

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.

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 como delegado de protección de datos a José Manuel Mulero con el que podrá contactar en caso de considerarlo necesario en el siguiente email: dpo@odilo.es

13. Responsabilidad

Conforme el artículo 82 del GDPR, 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

Una vez finalice la prestación de servicios objeto de este contrato, el ENCARGADO y el RESPONSABLE procederán de la siguiente forma:

- 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** los documentos, expedientes o informaciones archivadas y/o preservadas.
- 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, tramitadores de expedientes electrónicos, etc.).
- 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.



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.

