ANEXO III

FICHA DE TRATAMIENTO DE DATOS

Condiciones especiales en el marco del Acuerdo General de Encargo del Tratamiento de Datos Personales

Artículo 28 del Reglamento (UE) 2016/679 («**RGPD**»)

Entre

El **Responsable del Tratamiento**, según se identifica en el Acuerdo, representado por su representante legal investido de los poderes necesarios,

y

El **Encargado del Tratamiento**, según se identifica en el Acuerdo, representado por su representante legal investido de los poderes necesarios,

Asimismo, el Responsable y el Encargado podrán denominarse conjuntamente «**Partes**» e individualmente como «**Parte**».

CONSIDERANDO QUE

I. Las Partes han suscrito el Acuerdo Principal de Encargo del Tratamiento de Datos Personales («Acuerdo»), que regula los términos y modalidades del tratamiento de datos personales realizado por el Encargado en el marco de la prestación de los Servicios objeto del Contrato;
II. De conformidad con el citado Acuerdo, el tratamiento de datos personales relacionado con la prestación de Servicios concretos se regula mediante Fichas de Tratamiento de Datos que definen las características operativas, las categorías de datos tratados, las finalidades, las medidas de seguridad aplicadas y, en su caso, la intervención de subencargados del tratamiento;
III. La presente Ficha de Tratamiento de Datos especifica los detalles del Servicio de conformidad con el Acuerdo. Integra y completa las disposiciones generales del Acuerdo, constituyendo parte integrante y vinculante entre las Partes;
IV. En caso de conflicto entre las disposiciones de la presente Ficha de Tratamiento de Datos y las del Acuerdo, prevalecerán las disposiciones del Acuerdo, salvo que la Ficha de Tratamiento de Datos prevea expresamente excepciones acordadas entre las Partes;
V. Para los aspectos no previstos expresamente en el presente documento, se aplicarán las disposiciones y definiciones establecidas en el Acuerdo y en el Contrato, que quedan aquí íntegramente incorporadas por referencia.

Expuesto lo anterior, las Partes presentan, en la siguiente tabla, las especificaciones del tratamiento de Datos Personales relacionado con el Servicio, incluyendo información sobre las finalidades, las categorías de datos tratados, las medidas de seguridad aplicadas y cualquier otro detalle relevante a los efectos del Acuerdo.

	DESCRIPCIÓN
SERVICIO	**Módulo «AI SpinOff» para la funcionalidad de extracción automática de datos** El Módulo «AI SpinOff» es un componente opcional del software de gestión SpinOff on-premise de Namirial, dedicado a la extracción automática de datos contenidos en documentos o imágenes. El módulo utiliza modelos de inteligencia artificial para identificar y estructurar la información contenida en los documentos, devolviendo un Output en formato JSON validado. El tratamiento se estructura conforme al siguiente flujo operativo: Adquisición: el documento permanece dentro de la infraestructura del Responsable. El Módulo realiza localmente el tratamiento técnico necesario para preparar el contenido que se transmitirá a el Proveedor de IA, según

	los métodos que el Módulo admita en cada momento; Tratamiento por IA: el contenido del documento, o una representación técnica del mismo generada por el Módulo, se transmite a través de un canal cifrado al Proveedor de IA, que devuelve datos estructurados en formato JSON. Los datos transmitidos no son utilizados por el Proveedor de IA para entrenar sus propios modelos, de conformidad con las condiciones contractuales aplicables; Validación humana: el Módulo pone a disposición del operador del Responsable funcionalidades para verificar, comprobar y, en su caso, aprobar o modificar el Output antes de registrarlo en el software de gestión SpinOff, según las configuraciones aplicables; Registro: los datos validados se registran en la base de datos local SpinOff del Responsable.
ENTIDAD PRESTADORA	**Namirial S.p.A.** Cuando la Entidad Prestadora no coincida con el Proveedor identificado en la Propuesta Comercial, esta actuará como subencargado del tratamiento intragrupo por cuenta del Proveedor, operando en virtud de acuerdos intragrupo preexistentes entre las empresas del Grupo Namirial, conformes con el artículo 28 del RGPD.
NATURALEZA DEL TRATAMIENTO	El Encargado podrá tratar los Datos Personales del Cliente en el marco de la prestación del Servicio, dentro de los límites estrictamente necesarios para la ejecución de los servicios previstos en el Contrato, en términos de: recogida, registro, organización o estructuración, consulta, tratamiento, selección, extracción, cotejo, uso, comunicación, supresión o destrucción, así como el análisis automatizado del contenido de los documentos mediante modelos de inteligencia artificial (IA). El tratamiento se realiza exclusivamente por iniciativa y bajo el control del Responsable, que sigue siendo responsable de la exactitud e integridad de los datos introducidos en el software de gestión.
FINALIDAD DEL TRATAMIENTO	Ejecución del Contrato para la prestación del Módulo «IA integrada en SpinOff», que incluye: • cálculo y comunicación al operador de la Puntuación de Confianza (Confidence Score) de cada extracción, con el fin de apoyar la validación humana; • cumplimentación previa de los campos del software de gestión SpinOff para reducir la introducción manual y los errores de mecanografiado; • mejora de la eficiencia del proceso.
MODALIDAD DE PRESTACIÓN	*On-premise. El Módulo se instala directamente en la infraestructura del Responsable (servidores locales o red corporativa). Los documentos se tratan localmente mediante el Módulo, y el contenido necesario para el tratamiento por IA, o una representación técnica del mismo, se transmite de forma transitoria y cifrada al Proveedor de IA para su inferencia. No se prevé un almacenamiento persistente de datos personales en el Proveedor de IA.*
CATEGORÍAS DE INTERESADOS	• Empleados/colaboradores del Responsable; • Operadores del Responsable encargados de validar los Outputs de la IA y de registrarlos en el software de gestión SpinOff;

	• Terceros cuyos datos de identificación puedan figurar en los documentos (p. ej., clientes, destinatarios finales de las mercancías).
CATEGORÍAS DE DATOS PERSONALES TRATADOS	Los Datos Personales tratados por cuenta del Responsable son los contenidos en los documentos sometidos al Módulo de IA y pertenecen a las siguientes categorías. **DATOS COMUNES:** • Los datos contenidos en los documentos sometidos al Módulo de IA pueden incluir, a título de ejemplo y no exhaustivo: datos de identificación, datos de contacto, datos fiscales, datos comerciales, datos logísticos, datos administrativos; • Datos técnicos de tratamiento: Puntuación de Confianza de la extracción, marca de tiempo del tratamiento, tokens de API consumidos, tiempos de respuesta. **DATOS ESPECIALES (art. 9 del RGPD):** • No se prevé un tratamiento sistemático de categorías especiales de datos. No obstante, no puede excluirse que, en casos concretos, el contenido de los documentos incluya información atribuible a categorías especiales (p. ej., datos de salud en suministros sanitarios). El Responsable es el único responsable de evaluar y limitar el suministro de dichos datos al Módulo de IA.
UBICACIÓN DE ALMACENAMIENTO DE LOS DATOS	Instalaciones del Responsable (on-premise): los documentos originales, los registros técnicos y los datos registrados en el software de gestión SpinOff se almacenan exclusivamente en los servidores del Responsable del Tratamiento. Namirial no dispone de acceso remoto a los datos almacenados, salvo en intervenciones de soporte técnico expresamente autorizadas por el Responsable. Proveedor de IA (para tratamiento transitorio): la información extraída del documento se transmite a la API del Proveedor de IA exclusivamente para la inferencia de IA en tiempo real. El Proveedor de IA no almacena de forma persistente los datos enviados. La transferencia a los EE. UU., en su caso, se realiza de conformidad con el artículo 46 del RGPD, mediante Cláusulas Contractuales Tipo (SCC) adoptadas por la Comisión Europea mediante la Decisión de Ejecución 2021/914, de 4 de junio de 2021. Se entiende que Namirial podrá tratar métricas técnicas y de consumo relativas al uso del Módulo, tales como el número de tratamientos, las páginas procesadas, las marcas de tiempo, los resultados técnicos, los tokens u otros indicadores de consumo, a efectos de supervisión, elaboración de informes y facturación del servicio, sin acceso al contenido de los documentos tratados, salvo en intervenciones de soporte técnico expresamente autorizadas por el Responsable.
DURACIÓN DEL TRATAMIENTO DE DATOS PERSONALES	Los datos personales contenidos en los documentos cargados se tratan exclusivamente durante el tiempo necesario para la inferencia (tratamiento en tiempo real, sin almacenamiento persistente). Los resultados de la extracción en formato JSON están disponibles para el operador del Responsable durante la sesión de trabajo. Los registros técnicos locales se conservan en el servidor del Responsable durante un periodo máximo de 12 meses, salvo indicación distinta del Responsable u obligaciones

	legales específicas. Los datos registrados en el software de gestión SpinOff tras la validación humana quedan sujetos a las propias políticas de conservación del Responsable, definidas en función de las obligaciones fiscales y contables aplicables (habitualmente 10 años para documentos tributarios).
MEDIDAS DE SEGURIDAD	Ref. **Anexo III A - MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD**
SUBENCARGADOS DEL TRATAMIENTO	La Entidad Prestadora del Servicio (identificada en la fila anterior) recurre, para la prestación del Servicio, a otras empresas del Grupo Namirial y a terceros seleccionados que ofrecen garantías de confidencialidad de los datos. La lista actualizada se recoge en el Anexo III B, dividida en la **Tabla A** (empresas del Grupo Namirial que intervienen en la prestación del servicio, que operan en virtud de acuerdos intragrupo preexistentes conformes con el artículo 28 del RGPD y distintos del presente Acuerdo) y la **Tabla B** (subencargados del tratamiento terceros). Algunos de estos terceros pueden operar también fuera del Espacio Económico Europeo (EEE), incluidos los Estados Unidos. Para garantizar el cumplimiento del RGPD (artículos 44 a 49) y de la normativa de protección de datos personales, el Proveedor podrá utilizar mecanismos adecuados para la transferencia de datos. Estas entidades se seleccionan de conformidad con lo previsto en el Acuerdo, reciben instrucciones precisas sobre el tratamiento de datos y realizan únicamente las actividades necesarias, de conformidad con las directrices proporcionadas. La lista actualizada de dichas entidades se recoge en el Anexo III B del presente documento.

ANEXO III - A

MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

Las medidas de seguridad descritas en el presente Anexo se aplican de manera adicional a las previstas en el Acuerdo y constituyen un nivel de protección adicional para el tratamiento regulado por la Ficha de Tratamiento a la que se adjuntan. Se aplican a la Entidad Prestadora del Servicio a que se refiere el Contrato, que puede o no coincidir con el Encargado.

1. MEDIDAS TÉCNICAS DE SEGURIDAD

TIPO DE MEDIDA	DESCRIPCIÓN
Medidas para garantizar de forma permanente la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento	El Módulo de IA opera en la infraestructura on-premise del Responsable, con acceso limitado a los operadores autorizados mediante autenticación de la aplicación gestionada por SpinOff. • Las comunicaciones entre el Módulo de IA y la API del Proveedor de IA están protegidas mediante TLS y canales cifrados. Los contenidos o representaciones técnicas transmitidos al Proveedor de IA se tratan de forma transitoria durante el tiempo necesario para el procesamiento y no persisten localmente tras su envío. • Namirial mantiene el cumplimiento de la norma ISO/IEC 27001 en sus procesos de desarrollo y distribución de software. El contrato Enterprise con el Proveedor de IA incluye compromisos de seguridad certificados (ISO 27001, SOC 2 Tipo II).
Medidas para garantizar la capacidad de restablecer, de forma oportuna, la disponibilidad y el acceso a los datos personales en caso de incidente físico o técnico	La continuidad operativa del Módulo de IA depende de la infraestructura on-premise del Responsable (servidores locales, copias de seguridad corporativas) y de la disponibilidad del servicio del Proveedor de IA. • El Módulo está diseñado para ser resiliente frente a errores transitorios de la API (reintentos automáticos con backoff exponencial). En caso de indisponibilidad de la API del Proveedor de IA, el flujo de introducción manual en el software de gestión SpinOff permanece plenamente operativo, sin dependencia del Módulo de IA. • La Continuidad de Negocio de la infraestructura on-premise es responsabilidad del Responsable del Tratamiento, de conformidad con sus propias políticas internas.
Medidas de protección de los datos durante el almacenamiento	El Módulo de IA trata los documentos localmente en la infraestructura del Responsable y, cuando sea técnicamente necesario para el tratamiento por IA, genera una representación técnica del contenido relevante. Únicamente a efectos de inferencia, dicho contenido o representación técnica podrá transmitirse al Proveedor de IA a través de un canal cifrado, durante el tiempo estrictamente necesario para el tratamiento. **El Proveedor de IA garantiza que los datos enviados mediante la API no se utilizan para entrenar o mejorar sus propios modelos. Los datos enviados no se comparten con terceros ni son objeto de almacenamiento persistente en el Proveedor de IA.** • Cada llamada a la API se autentica mediante credenciales técnicas dedicadas, configuradas en el entorno de Namirial y asociadas al cliente o al servicio según las configuraciones aplicables. Las credenciales

	no se exponen en la interfaz de usuario ni en los registros de la aplicación.
Medidas para garantizar el registro de eventos	**Cada operación de extracción de documentos genera registros de aplicación locales que contienen:** • identificador único de la solicitud y del documento tratado; • marca de tiempo de inicio/fin del tratamiento; • Puntuación de Confianza calculada y detalle por campo; • número de los tokens de API consumidos y del coste estimado (USD); Los registros se almacenan localmente en el servidor del Responsable y son accesibles mediante endpoints de API dedicados (/api/v1/metrics, /api/v1/metrics/dashboard). La conservación se limita a 12 meses, salvo configuración distinta por parte del Responsable.
Medidas para garantizar la configuración del sistema, incluida la configuración por defecto	Las configuraciones del Módulo se establecen de manera que se ponga a disposición del operador una funcionalidad para verificar el Output de la IA y una indicación de su nivel de fiabilidad o de integridad, según los umbrales y parámetros configurados en cada momento. El principio de «protección de datos desde el diseño y por defecto» (art. 25 del RGPD) se implementa mediante: • el tratamiento local de los documentos en la infraestructura del Responsable, salvo la transmisión al Proveedor de IA del contenido o de la representación técnica estrictamente necesarios para el tratamiento; • la transmisión de datos al Proveedor de IA a través de canales cifrados y durante el tiempo estrictamente necesario para la inferencia de IA; • la configuración del Módulo de manera que permita al operador verificar, modificar, aprobar o rechazar el Output de la IA antes de su uso operativo, según las funcionalidades disponibles; • la minimización del Output devuelto por el Módulo a los datos y campos pertinentes para la funcionalidad concreta utilizada; • la inclusión de avisos informativos en la interfaz de usuario sobre la naturaleza automatizada y probabilística del Output de la IA y la necesidad de verificar su exactitud antes de su uso operativo, cuando así lo prevea la configuración del Módulo. • un aviso de exención de responsabilidad mostrado al operador en la interfaz de usuario sobre la naturaleza probabilística del Output de la IA.
Medidas internas de gestión y gobernanza de TI y ciberseguridad	El Módulo de IA se desarrolla y distribuye dentro del Sistema de Gestión de la Seguridad de la Información de Namirial, certificado conforme a la norma ISO/IEC 27001. Se aplican políticas internas para la gestión de accesos, el control de versiones del software (release management), la gestión de cambios y la evaluación periódica de los subencargados del tratamiento. La gobernanza de la IA se alinea progresivamente con los principios de la norma ISO/IEC 42001:2023, entre otros medios, mediante la documentación de las actividades de desarrollo, prueba y mantenimiento del Módulo de IA y el seguimiento de las versiones de los modelos utilizados. El Responsable es responsable de la gobernanza de TI de su propia infraestructura on-premise (acceso físico y lógico a los

	servidores, actualizaciones del sistema operativo, copias de seguridad).
Medidas para garantizar una conservación limitada de los datos	Los contenidos o representaciones técnicas generados para el tratamiento por IA se tratan durante el tiempo estrictamente necesario para el procesamiento y no son conservados por el Encargado de forma persistente, salvo en lo necesario para registros técnicos, métricas del servicio o actividades de soporte autorizadas. Los Outputs en formato JSON del tratamiento se mantienen en la memoria de la aplicación únicamente durante el tiempo necesario para la validación humana y el registro en el software de gestión. No son conservados por el Encargado de forma que permita la identificación de los interesados. Los registros técnicos se conservan durante un máximo de 12 meses y posteriormente se eliminan de forma automática o a solicitud del Responsable.
Medidas para garantizar la responsabilidad proactiva (accountability)	Cada ciclo de extracción de documentos se registra con un identificador único, la versión del modelo de IA utilizado y la Puntuación de Confianza. El Módulo pone a disposición funcionalidades que permiten al operador del Responsable verificar, validar, modificar o rechazar el Output de la IA antes de su uso operativo, según las configuraciones aplicables (en cumplimiento del artículo 22 del RGPD - prohibición de decisiones automatizadas con efectos jurídicos significativos). Namirial mantiene la documentación técnica del Módulo, el registro de versiones y los registros de los modelos de IA utilizados, en cumplimiento de los requisitos del AI Act (Reglamento (UE) 2024/1689) y de sus propias políticas internas.
Medidas para permitir la portabilidad de los datos y garantizar su supresión	Los datos tratados por el Módulo de IA se registran en el software de gestión SpinOff del Responsable y, por tanto, quedan sujetos a las propias políticas de portabilidad y supresión del Responsable. El Encargado no conserva copias de los datos personales tratados en la ejecución del Servicio y, por tanto, no es la entidad a la que dirigirse ante las solicitudes de acceso, rectificación, portabilidad o supresión de los interesados. A la finalización del Contrato, el Responsable podrá solicitar la desinstalación del Módulo y la eliminación de cualesquiera datos que pudieran estar almacenados en el sistema del Encargado (p. ej., claves de API, configuraciones del tenant). La eliminación se documentará y certificará.

ANEXO III - B

SUBENCARGADOS DEL TRATAMIENTO

El presente Anexo recoge los subencargados del tratamiento aprobados en la fecha de firma de la correspondiente Ficha de Tratamiento de Datos, de conformidad con el Acuerdo.

Las entidades relacionadas se han seleccionado con base en criterios de experiencia, fiabilidad y garantías de cumplimiento de la normativa aplicable, en particular lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679.

Actúan bajo la autoridad del Encargado, siguiendo las instrucciones recibidas y adoptando medidas de seguridad adecuadas para la protección de los Datos Personales tratados.

La lista de subencargados del tratamiento podrá actualizarse con el tiempo de conformidad con lo previsto en el Acuerdo.

TABLA A

EMPRESAS DEL GRUPO NAMIRIAL QUE INTERVIENEN EN LA PRESTACIÓN DEL SERVICIO

NOMBRE DE LA EMPRESA	DIRECCIÓN	UBICACIÓN DEL TRATAMIENTO	ÁMBITO DE ACTIVIDAD
Namirial SPA	Via Caduti sul Lavoro 4 – Senigallia (AN) Italia	EEE	Prestador de servicios

TABLA B

SUBENCARGADOS DEL TRATAMIENTO TERCEROS

NOMBRE DE LA EMPRESA	DIRECCIÓN	UBICACIÓN DEL TRATAMIENTO	ÁMBITO DE ACTIVIDAD
OpenAI LLC	3180 18th Street San Francisco, CA 94110 EE. UU.	EE. UU. (extra-UE) Transferencia conforme al art. 46 del RGPD SCC Decisión CE 2021/914	Inferencia de IA para la extracción de datos estructurados de documentos. Tratamiento transitorio: sin almacenamiento persistente de datos personales.
Zendesk Inc.	989 Market St, San Francisco, CA 94103	EEE	Gestión de tickets de soporte
Atlassian B.V.	Amsterdam, Singel 236 1016 AB, Netherlands	EEE	Gestión de tickets de soporte
Exalate NV	Roderveldlaan 2 bus 3, 2600 Berchem, Belgium	EEE	Sincronización de tickets de soporte