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 «**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 todo 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	*eInvoicing*
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 obtenidos en el marco de la prestación de las actividades de soporte y mantenimiento, 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, selección, supresión o destrucción.
FINALIDAD DEL TRATAMIENTO	Celebración del Contrato y ejecución de los servicios objeto del Contrato.
MODALIDAD DE PRESTACIÓN	*Cloud SaaS*
CATEGORÍAS DE INTERESADOS	• Clientes finales; • Usuarios del servicio; • Empleados.
CATEGORÍAS DE DATOS PERSONALES TRATADOS	Los Datos Personales tratados por el Encargado por cuenta del Responsable pertenecen a las siguientes categorías: **DATOS COMUNES:** • Datos personales (nombre, apellidos, fecha de nacimiento, lugar de nacimiento, nacionalidad, sexo, código fiscal, dirección de residencia/domicilio); • Datos de contacto (correo electrónico, número de teléfono); • Datos de navegación (dirección IP); • Datos de facturación (datos financieros, IBAN, información de pago).
UBICACIÓN DE ALMACENAMIENTO DE LOS DATOS	Los datos se almacenan en los servidores del Encargado y/o de los subencargados del tratamiento, ubicados dentro de la Unión Europea/EEE.
DURACIÓN DEL TRATAMIENTO DE LOS DATOS PERSONALES	El tratamiento de los Datos Personales para la prestación de los Servicios tendrá la siguiente duración: toda la duración del Contrato con el Responsable; toda la duración del Acuerdo con el Responsable si, por cualquier motivo, esta fuera superior a la duración del Contrato. Tras la expiración de los plazos mencionados, se permite al Encargado conservar ulteriormente los Datos Personales en la medida en que ello constituya el cumplimiento de obligaciones legales específicas o de órdenes de las Autoridades competentes. La conservación de los Datos Personales también está permitida exclusivamente en la medida en que dichos Datos Personales sean necesarios para que el Encargado pueda demostrar, ejercer o defender su propio derecho, por un período máximo de 10 años.
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 facilita en el Anexo III B, dividida en **Tabla A** (empresas del Grupo Namirial que participan en la prestación del servicio, que operan en virtud de acuerdos intragrupo preexistentes conformes con el artículo 28 del RGPD y separados del presente Acuerdo) y **Tabla B** (subencargados del tratamiento terceros).

	Algunos de estos terceros también pueden operar 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 los mecanismos apropiados para la transferencia de datos. Estas entidades se seleccionan de conformidad con lo dispuesto en el Acuerdo, reciben instrucciones precisas sobre el tratamiento de los datos y realizan únicamente las actividades necesarias, cumpliendo con las directrices proporcionadas. La lista actualizada de estas entidades se facilita 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 forma adicional a las previstas en el Acuerdo y constituyen un nivel de protección adicional para el tratamiento regulado por la Ficha de Tratamiento de Datos a la que se adjuntan. Se aplican a la Entidad Prestadora del Servicio a que se refiere el Contrato, que podrá coincidir o no con el Encargado.

1. MEDIDAS TÉCNICAS DE SEGURIDAD

TIPO DE MEDIDA	DESCRIPCIÓN
Medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento	Backup, Disaster Recovery, Firewall, IDS, IPS, antivirus, SOC.
Medidas para garantizar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma oportuna en caso de incidente físico o técnico	Copia de seguridad diaria con retención de 31 días: las copias de seguridad diarias garantizan la disponibilidad de los datos recientes durante un período de 31 días. • Copia de seguridad mensual con retención de 12 meses: las copias de seguridad mensuales garantizan la conservación de los datos hasta 12 meses. • Última copia de seguridad replicada en el sitio de Disaster Recovery: la replicación de la última copia de seguridad en el sitio de Disaster Recovery garantiza la disponibilidad de los datos en caso de incidente.
Medidas para proteger los datos durante su almacenamiento	Restricciones de acceso a los sistemas de archivos y a las bases de datos: las restricciones de acceso garantizan que únicamente el personal autorizado pueda acceder a los datos conservados.
Medidas para garantizar el registro de eventos	**Registros de aplicación en archivos locales: las actividades de la aplicación se registran en archivos de registro locales para el seguimiento y análisis de eventos.** • Registros de acceso almacenados en sistemas a prueba de manipulación con acceso restringido a los administradores del sistema: los registros de acceso se conservan en sistemas resistentes a la manipulación y solo pueden ser consultados por los administradores del sistema.
Medidas para garantizar la configuración del sistema, incluida la configuración predeterminada	Procedimiento de puesta en escena de servidores («staging»): el procedimiento de staging garantiza que los servidores estén correctamente configurados antes de pasar a producción. Evaluaciones de vulnerabilidad mensuales: se realizan evaluaciones de vulnerabilidad mensuales para identificar y solucionar posibles amenazas al sistema.
Medidas internas de gestión y gobierno de TI y	SOC (Security Operations Center)

ciberseguridad	El SOC es una estructura dedicada responsable de la gestión de la ciberseguridad de la organización. Su objetivo principal es supervisar, detectar, analizar y responder a los incidentes de seguridad en tiempo real. El SOC se basa en una combinación de tecnologías avanzadas, procesos y personal cualificado para garantizar la protección de los datos y sistemas de la organización.
Medidas para garantizar una conservación limitada de los datos	Procedimientos de depuración de datos configurados de acuerdo con las políticas contractuales: estos procedimientos garantizan que los datos se conserven únicamente durante el período necesario, de conformidad con las políticas contractuales de conservación.
Medidas para garantizar la responsabilidad proactiva	Seguimiento de los registros de acceso por parte de los administradores del sistema: la actividad de los administradores se registra y supervisa para garantizar la responsabilidad proactiva.
Medidas para permitir la portabilidad de los datos y garantizar su supresión	Exportación de archivos con metadatos en formato CSV: la exportación de archivos con metadatos en formato CSV facilita la portabilidad de los datos. Supresión programada a solicitud del cliente: la supresión programada garantiza que los datos se eliminen a solicitud del cliente.

2. MEDIDAS ORGANIZATIVAS DE SEGURIDAD

TIPO DE MEDIDA	DESCRIPCIÓN
Procedimientos para probar, evaluar y valorar regularmente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento	La evaluación de vulnerabilidad mensual genera un informe que es revisado por los Administradores del Sistema (ADS). Este procedimiento identifica y soluciona posibles amenazas a los sistemas, garantizando la seguridad y protección de los datos de la organización.

ANEXO III - B

SUBENCARGADOS DEL TRATAMIENTO

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

Las entidades enumeradas han sido seleccionadas con base en criterios de experiencia, fiabilidad y garantías de cumplimiento de la normativa aplicable, en particular de 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 a lo largo del tiempo de conformidad con lo dispuesto en el Acuerdo.

TABLA A

EMPRESAS DEL GRUPO NAMIRIAL QUE PARTICIPAN 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	Proveedor de servicios
Digital Technologies S.p.a.	Via Politi 10, Milano, Trezzano sul Naviglio, 20090	EEE	TI, almacenamiento y mantenimiento / Proveedor de servicios

TABLA B

SUBENCARGADOS DEL TRATAMIENTO TERCEROS

NOMBRE DE LA EMPRESA	DIRECCIÓN	UBICACIÓN DEL TRATAMIENTO	ÁMBITO DE ACTIVIDAD
Atlassian B.V.	Amsterdam, Singel 236 1016 AB Amsterdam, Países Bajos	EEE	Gestión de tickets de soporte
Zendesk Inc.	989 Market St, San Francisco, CA 94103	EEE	Gestión de tickets de soporte
Exalate NV	Roderveldlaan 2 bus 3, 2600 Berchem, Bélgica	EEE	Sincronización de tickets de soporte
Var Group S.p.A. (Yarix)	Via della Piovola, 138 - 50053 Empoli FI	EEE	SOC (Security Operation Center) y MOC (Monitoring Operation Center)