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	Plataformas/plataformas AMC: FatturePlus; WOW Platform; SpinOff. (en adelante, los «Servicios AMC») Plataformas/plataformas TAX: SGAPro; Web Successions; Live CAF; Tax online; CAF Manager; CAF Center. (en adelante, los «Servicios Tax») Conjuntamente los «Servicios Tax/AMC».
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.
FINALIDAD DEL TRATAMIENTO	Celebración del Contrato y ejecución de los servicios objeto del contrato.
MODALIDAD DE PRESTACIÓN	*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 (para todos los Servicios Tax):** • Datos personales (nombre, apellidos, fecha de nacimiento, lugar de nacimiento, país, sexo, código fiscal, dirección de residencia/domicilio); • Datos de contacto (correo electrónico, número de teléfono); • Datos de navegación (dirección IP, datos de registro); • Datos de facturación (IBAN, datos de pago); Otros datos eventuales (para el servicio SGA Pro): • copia del documento de identidad de los usuarios; • información relativa a la actividad profesional desempeñada; • posibles inscripciones en fondos de seguridad social; • posibles procedimientos disciplinarios relativos a los usuarios. • Otros datos eventuales (para la WOW Platform y los Servicios Tax): • datos contenidos en las declaraciones del impuesto sobre la renta. • Otros datos eventuales (para SpinOff): • datos contenidos en los documentos cargados dentro del sistema de gestión. • **CATEGORÍAS ESPECIALES DE DATOS (para SGA Pro):** • datos relativos a posibles situaciones de exención por maternidad, lesión u otras circunstancias acreditadas mediante documentación.
UBICACIÓN DE ALMACENAMIENTO DE LOS DATOS	Los datos se almacenan en servidores del Encargado y/o de los subencargados del tratamiento ubicados dentro de la Unión Europea/EEE.
DURACIÓN DEL TRATAMIENTO	El tratamiento de los Datos Personales para la prestación

DE DATOS PERSONALES	de los Servicios tendrá la siguiente duración: toda la duración del Acuerdo con el Responsable; toda la duración del Contrato con el Responsable si, por cualquier motivo, fuera superior a la duración del Acuerdo. Una vez transcurridos los plazos anteriores, se permite al Encargado conservar ulteriormente los Datos Personales en la medida en que ello sea necesario para cumplir con obligaciones legales específicas o con órdenes de las Autoridades competentes. La conservación de los Datos Personales se permite también, exclusivamente, en la medida en que dichos Datos Personales sean necesarios para que el Encargado pueda establecer, ejercer o defender una reclamación legal, por un plazo máximo de 10 años. Para el servicio SGA Pro, el Encargado garantiza la conservación de los datos durante 1 (un) año a partir de la resolución del Acuerdo.
MEDIDAS DE SEGURIDAD	Ref. Anexo III A - MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD PARA EL SERVICIO SGA PRO Ref. Anexo II - MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD previstas en el Acuerdo para todos los Servicios Tax.
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 la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento de forma permanente	Medidas para garantizar que los datos personales no puedan ser leídos, copiados, alterados o eliminados por personas no autorizadas durante la transmisión electrónica ni durante el transporte o el almacenamiento en soportes de datos, y para garantizar que sea posible verificar y determinar a qué entidades se transmiten los datos personales. En particular, el Encargado implementa las siguientes medidas técnicas y organizativas: • acceso protegido con nombre de usuario y contraseña, con actualización obligatoria de la contraseña cada 90 días. La contraseña debe contener mayúsculas y minúsculas, 8 caracteres, 1 número y 1 carácter especial; • pruebas de penetración periódicas (al menos una vez al año); • evaluaciones de vulnerabilidades periódicas; • controles técnicos de calidad de los datos: funciones integradas en el código diseñadas para verificar la calidad de la información y cómo se estructuran los datos; • disponibilidad de registros en texto claro de los últimos 30 días y disponibilidad de todos los cambios de contraseña realizados por los usuarios del servicio; • todos los sitios de SGAPRO alojados en servidores web están protegidos por un WAF (Web Application Firewall) y un balanceador de carga que expone la IP pública para hacer accesibles los sitios; posibilidad de conectarse mediante SFTP (con contraseña privada) a un servidor de soporte que mapea una unidad compartida que contiene el código PHP de los sitios SGAPRO; posibilidad de acceder a la instancia RDS que alberga las bases de datos de los distintos servicios; cada uno de los métodos de acceso anteriores solo es posible tras establecer una conexión VPN a la red de Namirial.
Medidas para garantizar la capacidad de restablecer la disponibilidad y el acceso a los datos personales de forma oportuna en caso de incidente físico o técnico	Para garantizar la continuidad operativa y el restablecimiento oportuno de la disponibilidad y el acceso a los datos personales en caso de incidente físico o técnico, Namirial ha implementado las siguientes medidas técnicas y organizativas: • Copias de seguridad periódicas: las copias de seguridad de los datos se realizan cada 12 horas, garantizando su conservación y una rápida capacidad de recuperación. • Copias de seguridad horarias de los sistemas de aplicación: • se realiza una copia de seguridad horaria de la imagen del servidor web y del sistema de archivos, incluido el código PHP, con un plazo de conservación de 15 días; • la base de datos se somete a una copia de seguridad completa de toda la instancia RDS cada 24 horas, también

	con un plazo de conservación de 15 días. • Redundancia de infraestructura: • los servidores de desarrollo utilizan el mismo código que la plataforma de producción, garantizando la coherencia entre entornos y facilitando las intervenciones de emergencia; el servidor de producción se replica en cuatro máquinas, garantizando una alta disponibilidad del servicio; también se mantiene una copia del código en un entorno de pruebas dedicado. Gestión de las solicitudes de soporte y asistencia: el personal del Encargado utiliza la plataforma ZenDesk para gestionar las solicitudes de soporte de los usuarios; cada solicitud genera un ticket asignado y gestionado por el equipo de soporte de primer nivel; si se requiere una intervención técnica avanzada, la solicitud se remite al equipo de cloud a través de Jira Service Desk, garantizando un flujo de trabajo estructurado para la gestión y resolución de incidentes.
Medidas de protección de los datos durante el almacenamiento	Los datos están protegidos por cortafuegos (WAF) y balanceadores de carga, y solo son accesibles mediante una conexión VPN segura a la red de Namirial. **Además, los datos se cifran durante la transmisión y el almacenamiento, y se realizan pruebas de penetración y evaluaciones de vulnerabilidades periódicas para garantizar la seguridad.**
Medidas para garantizar el registro de eventos	**Todos los accesos y modificaciones de los sistemas se registran en logs detallados, que se conservan durante al menos 30 días y son fácilmente accesibles.** • Las operaciones de acceso y modificación son trazables gracias a una gestión segura de las credenciales (mediante contraseñas y autenticación basada en VPN). • Cada cambio realizado por los usuarios se registra y supervisa para garantizar la integridad y confidencialidad de los datos. Además, en caso de incidente, los registros y las copias de seguridad permiten un restablecimiento rápido y seguro de las operaciones.
Medidas para garantizar la configuración de los sistemas, incluida la configuración por defecto	Los sistemas se entregan en la nube mediante diversas configuraciones almacenadas en bases de datos. Todas las configuraciones están automatizadas y centralizadas dentro del gestor del sistema (AWS), y las configuraciones se heredan con cada recarga del sistema.
Medidas internas de gestión y gobernanza de TI y ciberseguridad	El sistema cumple con la certificación ISO/IEC 27001.
Medidas para garantizar una conservación limitada de los datos	Se realizan controles de seguridad WASP Secure Mobile Development (véase la Política de Codificación Segura del Grupo SCS-P08). Se realiza un análisis del perímetro de las aplicaciones web. Las solicitudes de supresión o devolución de información -ya

	sean datos personales u otros tipos de datos- se gestionan de conformidad con las instrucciones proporcionadas por el Cliente, en cumplimiento del artículo 28 del RGPD y de lo previsto en el Acuerdo.
Medidas para garantizar la responsabilidad proactiva (accountability)	El Modelo Organizativo de Gestión de Emergencias (MOGE) define la asignación de responsabilidades entre las distintas funciones corporativas para los procesos y actividades relacionados con la gestión de la continuidad de negocio. Todas las empresas afiliadas a Namirial dentro de la UE han suscrito un acuerdo marco común sobre protección de datos y encargo del tratamiento de datos como instrumento jurídico de conformidad con el artículo 28 del RGPD, con el fin de garantizar un estándar uniforme de protección de datos y seguridad en todo el grupo y de regular los derechos y obligaciones de cualquier encargo del tratamiento de datos.
Medidas para posibilitar la portabilidad de los datos y garantizar su supresión	Namirial implementa medidas para garantizar que las personas autorizadas a utilizar un sistema de tratamiento de datos solo puedan acceder a los datos para los que se les haya concedido autorización, y que los datos personales no puedan ser leídos, copiados, modificados o eliminados sin autorización durante el tratamiento, el uso y tras su almacenamiento.

ANEXO III - B

SUBENCARGADOS DEL TRATAMIENTO

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

Las entidades enumeradas han sido seleccionadas con arreglo a 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.

Operan bajo la autoridad del Encargado, ateniéndose a 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 previsto en el Acuerdo.

TABLA A

EMPRESAS DEL GRUPO NAMIRIAL QUE INTERVIENEN EN LA PRESTACIÓN DEL SERVICIO

NOMBRE DE LA EMPRESA	DIRECCIÓN	LUGAR DE TRATAMIENTO	ÁMBITO DE ACTIVIDAD
Namirial SPA	Via Caduti sul Lavoro 4 - Senigallia (AN) Italia	EEE	Proveedor del servicio

TABLA B

SUBENCARGADOS DEL TRATAMIENTO TERCEROS

SERVICIO	NOMBRE DE LA EMPRESA	DIRECCIÓN	LUGAR DE TRATAMIENTO	ÁMBITO DE ACTIVIDAD
SGA Pro SpinOff	**AWS EMEA SARL**	Luxemburgo, 38 Avenue John F. Kennedy L-1855	EEE	Servicios en la nube
Servicios AMC	**Microsoft Ireland Operations Ltd**	South County Business Park, Dublín D18, Irlanda	EEE	Servicios en la nube
Servicios Tax/AMC	**Atlassian B.V.**	Amsterdam, Singel 236 1016 AB Ámsterdam, Países Bajos	EEE	Plataforma de tickets (back-end)
Servicios Tax/AMC	**Zendesk Inc.**	989 Market St, San Francisco, CA 94103	EEE	Plataforma de tickets (front-end)
Servicios Tax/AMC	**Exalate NV**	Roderveldlaan 2 bus 3, 2600 Berchem, Bélgica	EEE	Sincronización de tickets
Servicios Tax/AMC	**Var Group S.p.A. (Yarix)**	Via della Piovola, 138 - 50053 - Empoli FI	EEE	SOC (Security Operation Center) y MOC (Monitoring Operation Center)

Servicios Tax	**Televideocom S.r.l.**	Z.I. Predda Niedda Nord Strada n. 5 - 07100 Sassari, Italia	EEE	Servicios en la nube
Servicios Tax	**Wiit S.p.A.**	Via Mercanti 12, Milán, Italia	EEE	Servicios de copia de seguridad
Servicios Tax/AMC	**Dynatrace S.r.l.**	Viale Enrico Forlanini, 23 20134 Milán (MI) Italia	EEE	Supervisión de registros (log monitoring)