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	*PECMailer*
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	*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 acceso (nombre de usuario y contraseña); • Datos de navegación (dirección IP, datos de registro); • Datos financieros (datos de facturación); • Datos adicionales (incluidas categorías especiales) presentes en los mensajes de Correo Electrónico Certificado (PEC) confiados al Encargado.
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 DE 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, fuera superior a la duración del Contrato. Una vez transcurridos 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 se permite también, 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 plazo 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 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	Confidencialidad: • El acceso a PECMailer solo se permite mediante protocolos TLS versión 1.2 o superior. • Cifrado de las credenciales de acceso de cuentas y operadores. • Gestión multibase de datos para garantizar la separación lógica/funcional de las cuentas de correo. • Integridad: • La integridad de los mensajes de correo electrónico certificado (PEC) se garantiza mediante la firma digital aplicada por el prestador del servicio. • El control de la integridad de los datos durante la transferencia se garantiza mediante cifrado TLS. Disponibilidad: Infraestructura de tres niveles con zonas de disponibilidad ubicadas dentro de la Comunidad Europea. Uso de Azure Storage Premium con instantáneas automáticas cada 24 horas y conservación de 14 días. Copias de seguridad diferenciales cada 12 horas con conservación semanal de 4 semanas. Recuperación a un punto en el tiempo cada 10 minutos con conservación de 7 días para las bases de datos. Resiliencia: Máquinas virtuales (VM) redundantes y con balanceo de carga configuradas para garantizar la continuidad del servicio.
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	Instantáneas automáticas cada 24 horas para el almacenamiento, con conservación de 14 días. • Recuperación a un punto en el tiempo cada 10 minutos para las bases de datos críticas. • Infraestructura distribuida en varias zonas de disponibilidad dentro de la Comunidad Europea.
Medidas de protección de los datos durante el almacenamiento	Datos almacenados en Azure Storage Premium con redundancia local. **Cifrado de las credenciales de acceso y de los datos en reposo.** • Integración con sistemas de autenticación federada para garantizar un acceso seguro.
Medidas para garantizar el registro de eventos	**Registros detallados de las actividades del servicio backend (ServicesActivity) y de las operaciones de los**

	usuarios (_SysEventsLog); • Trazabilidad completa de las actividades de los operadores: acceso, envío, lectura y supresión de mensajes; • Registros almacenados en bases de datos dedicadas a cada cliente, con opciones de consulta y análisis histórico.
Medidas para garantizar la configuración de los sistemas, incluida la configuración por defecto	Actualizaciones de seguridad periódicas aplicadas a las VM y a los servicios.
Medidas internas de gestión y gobernanza de TI y ciberseguridad	CrowdStrike EDR instalado en todas las máquinas.
Medidas para garantizar una conservación limitada de los datos	Políticas de conservación en la cuenta PEC (excluida PECMailer): configurables para los mensajes PEC (1 día, 3 días, 15 días).
Medidas para garantizar la responsabilidad proactiva (accountability)	Seguimiento exhaustivo de las actividades administrativas y de los usuarios mediante registros. Políticas de auditoría interna para verificar el cumplimiento de la normativa RGPD.
Medidas para posibilitar la portabilidad de los datos y garantizar su supresión	Exportaciónde datos a través del SDK de PECMailer para integraciones externas.

2. MEDIDAS ORGANIZATIVAS DE SEGURIDAD

TIPO DE MEDIDA	DESCRIPCIÓN
Procedimientos para probar, verificar y evaluar regularmente la eficacia de las medidas técnicas y organizativas destinadas a garantizar la seguridad del tratamiento	Se realizan pruebas de penetración semestrales, y el equipo de ciberseguridad efectúa evaluaciones de vulnerabilidades semanales, clasificando las vulnerabilidades como Críticas, Altas, Medias o Bajas, con SLA de subsanación definidos en función del nivel de gravedad.
Medidas de certificación/garantía de procesos y productos - Pruebas y verificación de seguridad	Pruebas y verificación de seguridad • Evaluaciones de vulnerabilidades y pruebas de penetración trimestrales. • Supervisión continua de vulnerabilidades y procesos de gestión de parches con SLA definidos. • Auditorías periódicas de las configuraciones de seguridad de las infraestructuras tanto en la nube como on-premise.

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

NOMBRE DE LA EMPRESA	DIRECCIÓN	LUGAR DE TRATAMIENTO	ÁMBITO DE ACTIVIDAD
Microsoft Ireland Operations Ltd	South County Business Park, Dublín D18, Irlanda	EEE	Servicios en la nube
Atlassian B.V.	Amsterdam, Singel 236 1016 AB Ámsterdam, 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)
Dynatrace S.r.l.	Viale Enrico Forlanini, 23 20134 Milán (MI) Italia	EEE	Supervisión de registros (log monitoring)