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 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	*Building In Cloud (BIC)*
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/Colaboradores.
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, número de identificación fiscal, dirección de residencia/domicilio);** • **Datos de contacto (correo electrónico, número de teléfono);** • **Datos de registro (dirección IP).**
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 de forma permanente la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento	Medidas para garantizar que los datos personales no puedan ser leídos, copiados, alterados o eliminados por personas no autorizadas durante la transmisión electrónica o durante el transporte o el almacenamiento en soportes de datos, y que sea posible verificar y determinar a qué entidades se transmiten los datos personales. En concreto, se aplican las siguientes medidas técnicas y organizativas: • cifrado avanzado de los datos tanto en tránsito (TLS 1.3, VPN) como en reposo (AES-256); • protección física de los centros de datos con acceso biométrico y sistemas de alarma; • detección proactiva de amenazas cibernéticas mediante herramientas SIEM para una supervisión continua; • equilibrio de carga y redundancia de la infraestructura para garantizar la continuidad del servicio en caso de fallos; • pruebas de resiliencia y ataques simulados (Penetration Testing) para verificar la robustez del sistema.
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	Medidas capaces de restablecer rápidamente la disponibilidad y el acceso a los datos personales en caso de incidente físico o técnico. En concreto, se aplican las siguientes medidas técnicas y organizativas: • supervisión y notificación de las copias de seguridad; • restauración mediante herramientas de automatización; • concepto de copia de seguridad y proceso de recuperación basados en criticidades específicas y requisitos del cliente; • control del proceso de copia de seguridad; • pruebas periódicas del proceso de recuperación de datos y registro de los resultados; • almacenamiento de los soportes de copia de seguridad en un lugar seguro fuera de la sala de servidores.
Medidas de protección de los datos durante el almacenamiento	Medidas para garantizar la protección de los datos personales frente a la destrucción o pérdida accidental (SAI, climatización, protección contra incendios, copia de seguridad de datos, almacenamiento seguro de soportes de datos, protección antivirus, sistemas RAID, duplicación de discos, etc.). **MEDIDAS TÉCNICAS:** • cifrado de datos en reposo (Data at Rest Encryption) para garantizar la protección de los datos almacenados; • gestión centralizada de los permisos a los sistemas de archivos críticos; • sistemas de detección de incendios; • extintor en la sala de servidores; • control de la temperatura y la humedad en la sala de

	servidores; • control de la ventilación de la sala de servidores; • sistema de SAI y generadores diésel de emergencia; **sistema RAID / duplicación de disco duro;** • videovigilancia de la sala de servidores; • aviso de alarma en caso de acceso no autorizado a la sala de servidores; • destrucción segura de los soportes de almacenamiento al final de su ciclo de vida (desmagnetización, trituración certificada). • MEDIDAS ORGANIZATIVAS: servicio de copia de seguridad; ausencia de tuberías en la sala de servidores; almacenamiento de los soportes de copia de seguridad en un lugar seguro fuera de la sala de servidores; particiones separadas para sistemas operativos y datos, cuando sea necesario; supervisión del acceso a los datos almacenados, con alertas ante operaciones anómalas.
Medidas para garantizar el registro de eventos	**Medidas organizativas adoptadas por el Encargado del Tratamiento:** • registros de auditoría protegidos e inmutables, con acceso limitado a los administradores del sistema; • supervisión en tiempo real de las actividades críticas, con alarmas automáticas ante anomalías; • análisis periódico de los registros del sistema y correlación de eventos sospechosos; proceso documentado de detección y notificación de incidentes de seguridad/violaciones de la seguridad de los datos personales (véase la Política SCS-P04 Group Incident Management & Reporting Policy); • procedimiento formalizado de gestión de incidentes de seguridad (véase la Política SCS-P04 Group Incident Management & Reporting Policy); intervención del DPO y del CISO en los incidentes de seguridad y en las violaciones de la seguridad de los datos personales; documentación de los incidentes de seguridad y de las violaciones de la seguridad de los datos personales mediante el sistema de tickets (a través de la herramienta «Jira»); proceso formal de seguimiento de los incidentes de seguridad y de las violaciones de la seguridad de los datos personales.
Medidas para garantizar la configuración de los sistemas, incluida la configuración por defecto	El Encargado del Tratamiento aplica las siguientes medidas para garantizar la integridad de los sistemas: uso de cortafuegos actualizado periódicamente; uso de filtro antispam actualizado periódicamente; uso de antivirus actualizado periódicamente; sistema de detección de intrusiones (IDS) para los sistemas del Responsable del Tratamiento; sistema de prevención de intrusiones (IPS) para los sistemas del Responsable del Tratamiento.
Medidas internas de gestión	El sistema cumple con la certificación ISO/IEC 27001.

y gobernanza en materia de TI y ciberseguridad	
Medidas para garantizar una conservación limitada de los datos	Se aplican los controles de seguridad OWASP Secure Mobile Development (véase la Política SCS-P08 Group Secure Coding Policy); análisis perimetral de las aplicaciones web.
Medidas para garantizar la responsabilidad proactiva (accountability)	Los empleados del Encargado del Tratamiento reciben información y formación continuas en materia de protección de datos, y están vinculados contractualmente al secreto y la confidencialidad de los datos. Los terceros que puedan entrar en contacto con datos personales en el desempeño de su trabajo para el Encargado del Tratamiento están obligados a mantener el secreto y la confidencialidad de los datos, a fin de cumplir con la protección de datos y el secreto de los datos en virtud del NDA (Acuerdo de Confidencialidad) antes de comenzar a trabajar. Todas las empresas afiliadas al Encargado del Tratamiento dentro de la UE han suscrito un acuerdo marco común en materia de protección de datos y de encargo del tratamiento de datos, como instrumento jurídico conforme al artículo 28 del RGPD, con el fin de garantizar un estándar uniforme de protección de datos y de seguridad en todo el grupo y de regular los derechos y obligaciones relativos a cualquier encargo del tratamiento de datos.
Medidas para permitir la portabilidad de los datos y garantizar su supresión	El Encargado del Tratamiento adopta medidas para garantizar que las personas autorizadas a utilizar un sistema de tratamiento de datos solo puedan acceder a los datos objeto de su autorización de acceso, y que los datos personales no puedan ser leídos, copiados, modificados o eliminados sin autorización durante su tratamiento, uso y tras su almacenamiento.

2. MEDIDAS ORGANIZATIVAS DE SEGURIDAD

TIPO DE MEDIDA	DESCRIPCIÓN
Procedimientos de verificación, evaluación y prueba periódicas de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento	Las políticas internas relativas a las medidas de seguridad se revisan periódicamente y se confirma su adecuación y eficacia durante las auditorías internas en curso y, anualmente, por organismos de certificación independientes, externos y acreditados, en el marco de las auditorías de seguimiento y recertificación ISO 9001 e ISO 27001.

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 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.

Actúan 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

DENOMINACIÓN DE LA EMPRESA	DIRECCIÓN	UBICACIÓN DEL TRATAMIENTO	ÁMBITO DE ACTIVIDAD
Namirial SPA	Via Caduti sul Lavoro 4 - Senigallia (AN), Italia	EEE	Prestador del servicio

TABLA B

SUBENCARGADOS DEL TRATAMIENTO TERCEROS

DENOMINACIÓN DE LA EMPRESA	DIRECCIÓN	UBICACIÓN DEL TRATAMIENTO	ÁMBITO DE ACTIVIDAD
AWS EMEA SARL	Luxemburgo, 38 Avenue John F. Kennedy L-1855	EEE	Servicios en la nube
Zendesk Inc.	989 Market St, San Francisco, CA 94103	EEE	Gestión de tickets de soporte
Atlassian B.V.	Singel 236, 1016 AB Ámsterdam, Países Bajos	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