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	*ClickWrap*
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:** • Datos personales (nombre, apellidos); • Datos de contacto (correo electrónico, número de teléfono); • Datos de navegación (dirección IP, registro).
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 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	La solución permite el almacenamiento seguro de los paquetes de datos mediante el uso de una blockchain con permisos (permissioned) basada en el mecanismo de consenso Proof of Stake (PoS), que garantiza la inmutabilidad y la incorruptibilidad. Los datos en claro almacenados en los servidores AWS de ClickWrap se cifran mediante el sistema de cifrado de Amazon S3 antes de guardarse. • El acceso a la plataforma solo es posible mediante autenticación del usuario con identificador y contraseña, protegida por autenticación de dos factores (2FA) a través de una contraseña de un solo uso (OTP) enviada a la dirección de correo electrónico del Cliente. • Las API utilizadas para la comunicación con el proveedor de almacenamiento AWS están protegidas mediante autenticación de API.
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 blockchain no almacena directamente datos personales, sino únicamente un hash del archivo JSON, lo que permite verificar la integridad de los datos sin comprometer la seguridad. • Se envía un archivo JSON en texto claro a los servidores AWS de ClickWrap, de forma que el hash del archivo almacenado pueda compararse posteriormente con el registrado en la blockchain. • El sistema está diseñado para garantizar una alta disponibilidad, evitando problemas de congestión y de denegación de servicio mediante el uso de un servidor Available-To-Promise (ATP).
Medidas de protección de los datos durante el almacenamiento	Los datos almacenados en los servidores AWS se cifran antes de su almacenamiento y solo se descifran en el momento de la descarga. La plataforma utiliza bases de datos relacionales SQL, protegidas mediante defensas perimetrales, servidor ATP, cortafuegos de aplicaciones web (WAF) y cifrado a través de Amazon S3. • El sistema utiliza WORM (Write Once, Read Many) para garantizar la integridad de los datos y evitar modificaciones no autorizadas • Un WAF contribuye a proteger las aplicaciones web mediante el filtrado y la supervisión del tráfico HTTP entre la aplicación web e internet, defendiendo frente a ataques como la falsificación de solicitudes entre sitios (CSRF), la ejecución de secuencias de comandos entre sitios (XSS), la inclusión de archivos y la inyección SQL, entre otros.

	• Un WAF es una protección de la capa 7 (modelo OSI) y no está diseñado para defender frente a todos los tipos de ataques. Al colocar un WAF delante de una aplicación web, se crea un escudo protector entre la aplicación e internet.
Medidas para garantizar el registro de eventos	La solución garantiza el registro y la trazabilidad de las operaciones a través de la blockchain, que almacena un hash inmutable del archivo JSON asociado al consentimiento. • El hash del archivo JSON permite acreditar la autenticidad del consentimiento del usuario, verificando que no ha sido alterado con el tiempo. • Los registros de acceso a las bases de datos y a las API están protegidos y se supervisan para detectar cualquier actividad sospechosa.
Medidas para garantizar la configuración de los sistemas, incluida la configuración por defecto	La capa de aplicación de la plataforma es cloud-native y utiliza microservicios diseñados para activarse únicamente a demanda y eliminarse automáticamente después, reduciendo la exposición a código malicioso. La plataforma adopta un modelo de seguridad de mínimo privilegio, limitando el acceso estrictamente a los recursos necesarios. Todos los sistemas se supervisan y actualizan para prevenir vulnerabilidades de configuración.
Medidas internas de gestión y gobernanza en materia de TI y ciberseguridad	La blockchain utilizada es de tipo permissioned, lo que significa que el acceso está restringido a usuarios autorizados que deben autenticarse mediante certificados digitales u otros métodos de autenticación. Los validadores de la blockchain se seleccionan cuidadosamente tras una evaluación exhaustiva de su infraestructura informática y de otros elementos que garanticen un nivel adecuado de seguridad. Este tipo de solución es recomendado por las autoridades de protección de datos por ofrecer un mayor nivel de privacidad. El sistema está protegido mediante un cortafuegos de aplicaciones web (WAF) que filtra y supervisa el tráfico HTTP y previene ataques como la falsificación entre sitios, XSS, la inyección SQL y la inclusión de archivos.
Medidas para garantizar una conservación limitada de los datos	No se almacenan datos personales en claro en la blockchain, únicamente un hash del archivo JSON, que no puede utilizarse para reconstruir los datos originales. El hash almacenado en la blockchain es determinista, es decir, la misma entrada generará siempre la misma salida, lo que permite verificar la integridad de los datos sin necesidad de almacenar los datos originales. Las reglas de conservación se configuran para garantizar la minimización de datos de conformidad con el principio de protección de datos desde el diseño y por defecto.
Medidas para garantizar la responsabilidad proactiva (accountability)	El acceso a la plataforma está regulado por mecanismos de autenticación reforzada y de trazabilidad que permiten identificar cada operación realizada. La blockchain proporciona una prueba criptográfica inalterable de la operación realizada, garantizando el no repudio del consentimiento expresado por el usuario.

	Los validadores de la blockchain están sujetos a auditorías y controles para garantizar el cumplimiento de los requisitos de seguridad.
Medidas para permitir la portabilidad de los datos y garantizar su supresión	La solución permite exportar los datos en formato JSON, garantizando la portabilidad y la interoperabilidad con otros sistemas. El hash registrado en la blockchain puede verificarse en cualquier momento, garantizando la transparencia y la accesibilidad de los datos almacenados. Los datos en claro pueden suprimirse a petición, manteniendo el hash en la blockchain a efectos de auditoría, sin que ello suponga el almacenamiento de datos personales atribuibles al usuario.

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	El sistema de blockchain y cifrado se somete a pruebas periódicas para verificar la integridad del registro de hashes y la fiabilidad de la plataforma. • Se realizan pruebas de seguridad sobre las API y las infraestructuras en la nube para garantizar la fiabilidad de los controles de acceso. • La plataforma se somete a controles de cumplimiento con los estándares de seguridad y privacidad, de conformidad con las recomendaciones de las autoridades de protección de datos.

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	Almacenamiento de datos
Atlassian B.V.	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