ANEXO III

FICHA DE TRATAMIENTO DE DATOS

Condiciones especiales en virtud del Acuerdo General de Tratamiento de Datos Personales

Artículo 28 del Reglamento (UE) 2016/679 (el «**RGPD**»)

Entre

El **Responsable del Tratamiento**, tal como se identifica en el Acuerdo, representado por su representante legal facultado con los poderes necesarios,

y

El **Encargado del Tratamiento**, tal como se identifica en el Acuerdo, representado por su representante legal facultado con los poderes necesarios,

Asimismo, el Responsable del Tratamiento y el Encargado del Tratamiento podrán denominarse conjuntamente las «**Partes**» e individualmente la «**Parte**».

CONSIDERANDO QUE

I. Las Partes han suscrito el Acuerdo Principal de Tratamiento de Datos Personales («Acuerdo»), que regula los términos y métodos del tratamiento de datos personales realizado por el Encargado del Tratamiento en el contexto de la prestación de los Servicios objeto del Contrato;
II. En virtud del Acuerdo antes mencionado, el tratamiento de datos personales relacionado con la prestación de Servicios específicos 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 la eventual participación 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 una 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 las cuestiones no previstas expresamente en el presente documento, se aplicarán las disposiciones y definiciones establecidas en el Acuerdo y el Contrato, que quedan aquí íntegramente incorporadas por referencia.

Habiendo expuesto todo lo anterior, las Partes presentan, en la siguiente tabla, las especificaciones del tratamiento de Datos Personales relativo al 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	Servicio de Entrega Electrónica Certificada (SERC) y Servicio de Entrega Electrónica Certificada Cualificado (SERCQ)
ENTIDAD PRESTADORA	**Namirial S.p.A.** Cuando la Entidad Prestadora no coincida con el Proveedor identificado en la Propuesta Comercial, 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	Namirial S.p.A. actúa en este Servicio con una doble función: como encargado del tratamiento conforme al art. 4(8) del RGPD respecto de sus clientes (Responsables del Tratamiento), y como responsable del tratamiento

	autónomo conforme al art. 4(7) del RGPD para las actividades determinadas por la ley (obligaciones eIDAS como prestador cualificado de servicios de confianza y demás obligaciones establecidas por la normativa sobre entrega electrónica certificada (SERC/SERCQ)). Namirial trata datos personales como Encargado del Tratamiento respecto de sus clientes (Responsables del Tratamiento) en relación con: (a) los datos contenidos en el cuerpo de las comunicaciones SERCQ (texto, adjuntos y datos personales del destinatario comunicados por el remitente-cliente); (b) las actividades de asistencia y soporte de la plataforma. Las operaciones de tratamiento, dentro de los límites estrictamente necesarios para la prestación de los servicios previstos en el Contrato, incluyen: recogida, registro, organización o estructuración, consulta, tratamiento, selección, extracción, cotejo, uso, comunicación, supresión o destrucción.
FINALIDAD DEL TRATAMIENTO	Celebración del Contrato y prestación de los servicios objeto del Contrato.
MODALIDAD DE PRESTACIÓN	*Cloud* SaaS (*Shared/Private*)
CATEGORÍAS DE INTERESADOS	• Clientes finales; • Usuarios del Servicio.
CATEGORÍAS DE DATOS PERSONALES TRATADOS	Los Datos Personales tratados por el Encargado del Tratamiento por cuenta del Responsable del Tratamiento pertenecen a las siguientes categorías. **DATOS COMUNES:** • **Datos personales (nombre, apellidos, correo electrónico, fecha de nacimiento, lugar de nacimiento, nacionalidad, sexo, código fiscal, domicilio/residencia);** • **Datos de contacto (correo electrónico, número de teléfono);** • **Datos de registro (dirección IP);** • **Otros datos posibles: datos contenidos en las comunicaciones certificadas.** **CATEGORÍAS ESPECIALES DE DATOS PERSONALES:** • **Otros datos posibles: datos especiales contenidos en las comunicaciones certificadas.**
UBICACIÓN DE ALMACENAMIENTO DE LOS DATOS	Los datos se almacenan en los servidores del Encargado del Tratamiento y/o de los subencargados del tratamiento situados dentro de la Unión Europea/EEE.
DURACIÓN DEL TRATAMIENTO DE DATOS PERSONALES	El tratamiento de Datos Personales para la prestación de los Servicios tendrá la siguiente duración: toda la duración del Contrato con el Responsable del Tratamiento; toda la duración del Acuerdo con el Responsable del Tratamiento si, por cualquier motivo, fuera superior a la duración del Contrato. Tras la expiración de los plazos antes mencionados, se permitirá al Encargado del Tratamiento conservar adicionalmente los Datos Personales en la medida en que ello constituya el cumplimiento de obligaciones legales específicas u órdenes de las Autoridades competentes.

	La conservación de los Datos Personales también se permite exclusivamente en la medida en que dichos Datos Personales sean necesarios para que el Encargado del Tratamiento pueda demostrar, ejercer o defender su propio derecho, por un período máximo de 10 años.
MEDIDAS DE SEGURIDAD	Ref. **Anexo III A - MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS**
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 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 los 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 facilitadas. La lista actualizada de estas entidades se facilita en el Anexo III B del presente documento.

ANEXO III - A

MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS

Las medidas de seguridad descritas en el presente Anexo se aplican con carácter 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. Son aplicables a la Entidad Prestadora del Servicio a que se refiere el Contrato, que podrá coincidir o no con el Encargado del Tratamiento.

1. MEDIDAS DE SEGURIDAD TÉCNICAS

TIPO DE MEDIDA	DESCRIPCIÓN
Medidas para garantizar de forma permanente la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento	El proceso de verificación de la integridad de los paquetes de información y documentos dentro del servicio incluye: • Auditorías internas periódicas para comprobar y verificar que el estado del Sistema de Gestión de Seguridad de la Información sea adecuado y conforme a la ley; • Los empleados están formados para comprender los flujos de comunicación y, sin autenticación previa, no tendrán acceso a los datos tratados; • Los flujos de comunicación están protegidos mediante el uso de redes privadas virtuales (VPN). De este modo, las conexiones establecidas con las VPN protegerán la información intercambiada, ya que la información se cifrará entre ambos extremos del túnel; • Para cada servicio ofrecido, se redactan procedimientos para determinar el alcance y la frecuencia de las copias de seguridad cifradas (AES256) de los datos tratados, especificando la duración de la conservación. En estos casos, se establecerá el número de copias necesarias y la duración de la conservación.
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	En caso de una Violación de la Seguridad de los Datos Personales, Uanataca dispone de un proceso de gestión de incidentes informáticos que funciona de la siguiente manera: • Un equipo responsable, basándose en un análisis exhaustivo de incidentes informáticos anteriores, desarrollará un plan de acción compuesto por medidas preventivas para limitar la repetición de dichos episodios; • Al detectar un incidente físico o técnico, este se clasificará y dividirá en las categorías adecuadas necesarias para determinar la gravedad y la prioridad del tratamiento que deba aplicarse; • Posteriormente, mediante el proceso de notificación de incidentes, se pondrán de relieve las acciones inmediatas que deban adoptarse para garantizar la capacidad de restablecer con prontitud la disponibilidad y el acceso a los datos personales afectados; • Uanataca prevé asimismo la elaboración de un registro de incidentes informáticos, en el que es necesario disponer de la mayor cantidad posible de información sobre el incidente, a saber: • Fecha y hora del incidente; • Tipo y gravedad del incidente; Recursos afectados; Posibles orígenes; Estado del incidente; Acciones adoptadas para resolver el problema;

	Quién realizó las acciones anteriores; Fecha y hora de resolución y cierre del incidente. Por último, para la resolución del incidente informático, se redacta un documento explicativo del procedimiento que debe aplicarse en caso de Violación de la Seguridad de los Datos Personales, teniendo en cuenta los distintos escenarios posibles.
Medidas para proteger los datos durante su almacenamiento	Uanataca supervisará la evolución de las herramientas y mecanismos existentes para controlar el malware (antimalware, antiphishing, antispam, análisis de web y correo electrónico) con el fin de mejorar la protección de los activos de información. **La supervisión permitirá:** • Realizar análisis automáticos y periódicos para detectar cualquier tipo de malware; • Realizar comprobaciones automáticas de los archivos adjuntos de correo electrónico y de las descargas desde la web, ya que pueden contener códigos maliciosos; • Bloquear el acceso a determinadas aplicaciones o sitios web en función de la política de privacidad, creando así «listas negras» de prevención; • Permitir el acceso a determinadas aplicaciones o sitios web en función de la política de privacidad, creando así «listas blancas»; • Analizar y detectar posibles páginas web que puedan contener amenazas que pudieran comprometer los datos tratados.
Medidas para garantizar el registro de eventos	**Para los empleados y colaboradores de Uanataca se prevé una fase de registro en la que se crearán cuentas específicas con el dominio uanataca.com.** • Estas medidas de registro se aplican también a las cuentas con acceso directo a las VPN de Uanataca para el trabajo remoto. • Uanataca se ha dotado de software (Kibana + ElasticSearch) para la gestión de eventos relacionados con la seguridad y la supervisión de usuarios. Este software está configurado en modo local (On-premise), directamente en los servidores de Uanataca. • Este sistema de gestión prevé que los sujetos considerados puedan acceder a sus cuentas introduciendo una contraseña, que debe cumplir determinados requisitos para ser suficientemente difícil de adivinar o descifrar. • Uanataca prevé asimismo el desarrollo de procedimientos para garantizar la custodia de los archivos centralizados, permitiendo el acceso a ellos únicamente mediante autenticación de doble factor, consistente en la introducción de una contraseña y un PIN. Además, teniendo en cuenta que los dispositivos de acceso pueden pertenecer a Uanataca o al empleado o colaborador, se distinguen varios tipos de acceso: Acceso de trabajador simple, que tendrá acceso a la información contenida en los archivos, correos electrónicos y wikis para llevar a cabo su actividad laboral, incluso de forma

	remota; Acceso de administración, mediante VPN, con autenticación de doble factor (contraseña más clave privada RSA), para quienes ocupen funciones administrativas de nivel superior; Por último, el acceso especial. Este tipo de acceso, que debe autorizarse previamente, se concederá para la realización de actividades específicas y de duración limitada.
Medidas para garantizar la configuración del sistema, incluida la configuración predeterminada	Los proyectos de desarrollo se gestionarán mediante REDMINE, una herramienta integrada de gestión de tickets, código fuente y documentación (wiki). Se trata de un software de gestión de proyectos y seguimiento de errores de código abierto y basado en web, descargado y configurado directamente en los servidores internos de Uanataca. El código fuente de las aplicaciones se mantendrá actualizado mediante repositorios de gestión de datos (GIT). La autenticación para acceder a los repositorios se realizará mediante la introducción de un nombre de usuario y una contraseña (en poder de cada usuario del tratamiento de datos) a través de canales de comunicación cifrados. Cada proyecto, tanto en REDMINE como en GIT, tendrá diferentes funciones de acceso, tales como: administrador, propietario del producto (Product Owner), desarrollador. Los cambios e iteraciones del código se realizarán en ramas independientes dentro del mismo gestor de código fuente.
Medidas de gestión y gobernanza interna en materia de TI y ciberseguridad	Uanataca dispone de un Comité Técnico de Seguridad que desempeñará las siguientes funciones: Elaboración de normas de seguridad, de conformidad con las directrices establecidas; Elaboración de procedimientos de seguridad, para la implementación de los controles derivados de las normas anteriores y de conformidad con el Comité de Seguridad; Desarrollo y elaboración de procedimientos derivados de los planes operativos de continuidad del negocio. El sistema cumple con la certificación ISO/IEC 27001.
Medidas para garantizar la limitación de la conservación de datos	La custodia de la información y los datos se clasifica en función de la conservación y supresión de la información en poder de Uanataca. Para cumplir con este requisito, se elaborarán documentos para cada país, teniendo en cuenta los distintos regímenes legales que deban respetarse, con el fin de determinar los siguientes plazos: Plazo de conservación: se refiere al período mínimo durante el cual Uanataca debe conservar la información facilitada por los usuarios; Plazo máximo de supresión: se refiere al período máximo tras el cual Uanataca debe suprimir la información antes mencionada. Este período se inicia en el momento en que expira el plazo de conservación.
Medidas para garantizar la responsabilidad proactiva	Para garantizar la seguridad de los datos tratados, Uanataca designará a un Responsable de Seguridad encargado de las siguientes funciones:

	Elaboración del análisis de riesgos. Centralizar todas las acciones del Sistema de Gestión de Seguridad de la Información (SGSI) de Uanataca. Comunicar la Política de Seguridad a todo el personal y a las partes interesadas. Impartir formación en el SGSI y clasificar la información conforme a los criterios de clasificación definidos en la normativa correspondiente. Coordinar y supervisar las acciones llevadas a cabo por los Responsables de Riesgo. Notificar a todo el personal que se incorpore a Uanataca sus obligaciones en materia de cumplimiento de la Política de Seguridad y su marco normativo. Verificar el cumplimiento de la Política de Seguridad en la gestión de todos los contratos con terceros que se encuentren dentro del ámbito del SGSI. Organizar, planificar y realizar auditorías periódicas del SGSI. Uanataca también designará a Responsables de Riesgo, que tendrán las siguientes funciones: Serán responsables de dirigir y controlar las acciones de mejora para minimizar los riesgos; Controlarán las acciones de minimización de riesgos para garantizar en todo momento su trazabilidad; Se coordinarán con el Responsable de Seguridad para informar sobre sus avances respecto al SGSI.
Medidas para permitir la portabilidad de los datos y garantizar su supresión	Uanataca garantiza la supresión de los datos tratados cuando dejen de cumplirse los requisitos legales y contractuales. A continuación se indican algunas de las causas que permitirán la supresión de la información: Fin de la condición de legitimación del tratamiento, asociado al fin de la relación contractual que permite la conservación de dicha información. Expiración del plazo legal para la conservación de la información y los datos tratados. Ejercicio de derechos por parte de los interesados. Los interesados podrán solicitar legítimamente la supresión de su información personal en poder de Uanataca. Para esta actividad, se tendrá en cuenta la legislación del país de origen del interesado. Para abordar estos supuestos, Uanataca ha desarrollado un procedimiento capaz de garantizar la supresión de los datos mediante dos métodos diferentes: La información puede destruirse por completo, en el caso de formato papel, mediante el uso de destructoras de papel o mediante servicios específicos de destrucción de información en papel.

	La información digital se suprimirá de los archivos informáticos. Asimismo, se suprimirán las copias de seguridad que contengan copias de dicha información, de modo que no puedan reutilizarse.

2. MEDIDAS DE SEGURIDAD ORGANIZATIVAS

TIPO DE MEDIDA	DESCRIPCIÓN
Procedimientos para probar, verificar y evaluar periódicamente la eficacia de las medidas técnicas y organizativas destinadas a garantizar la seguridad del tratamiento	Uanataca garantiza la autenticidad e integridad del contenido cumpliendo la normativa aplicable en materia de firma electrónica y adhiriéndose a las normas internacionales. • Uanataca utiliza cifrado TLS para el protocolo HTTPS en sus sistemas de comunicación, aplicando conjuntos de cifrado limitados en los que solo se permiten los protocolos considerados suficientemente seguros para el acceso AES256 (TLS 1.2 o superior). • Todos los algoritmos utilizados por Uanataca para la creación y validación de firmas digitales y electrónicas cumplen con el «conjunto criptográfico» ETSI TS 119 312. • Las actividades se llevan a cabo dentro de los controles de la certificación ISO/IEC 27001.

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 lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679.

Operan bajo la autoridad del Encargado del Tratamiento, siguiendo las instrucciones recibidas y adoptando las medidas de seguridad adecuadas para la protección de los Datos Personales tratados.

La lista de subencargados del tratamiento podrá actualizarse con el 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

TABLA B

SUBENCARGADOS DEL TRATAMIENTO TERCEROS

NOMBRE DE LA EMPRESA	DIRECCIÓN	UBICACIÓN DEL TRATAMIENTO	ÁMBITO DE ACTIVIDAD
Uanataca S.A.U.	Avenida Meridiana 350, piso 3, 08027 Barcelona (España)	EEE/EE. UU.	Gestión de la infraestructura tecnológica que soporta el Servicio
Atlassian B.V.	Ámsterdam, Singel 236,	EEE	Gestión de tickets de

	1016 AB Ámsterdam, Países Bajos		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
Yarix S.r.l.	Montebelluna (TV), Vicolo Boccacavalla n.º 12, 31044	EEE	SOC (Centro de Operaciones de Seguridad) y MOC (Centro de Operaciones de Supervisión)