ANEXO III

FICHA DE TRATAMIENTO DE DATOS

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

Artículo 28 del Reglamento (UE) 2016/679 (“RGPD”)

Entre

El **Responsable del Tratamiento**, identificado en el Contrato, representado por su representante legal debidamente facultado,

Y

El **Encargado del Tratamiento**, identificado en el Contrato, representado por su representante legal debidamente facultado,

En lo sucesivo, conjuntamente, las “**Partes**”, e individualmente, la “**Parte**”.

EXPONEN

I. Que las Partes han suscrito el Acuerdo Principal sobre el Tratamiento de Datos Personales (el “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. Que, conforme a lo establecido en el citado Acuerdo, el tratamiento de datos personales relativo a la prestación de determinados Servicios 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 participación de Subencargados;
III. Que la presente Ficha de Tratamiento de Datos especifica los detalles del Servicio conforme al Acuerdo. Completa e integra las disposiciones generales del Acuerdo, constituyendo una parte integrante y vinculante entre las Partes;
IV. Que, en caso de conflicto entre las disposiciones de la presente Ficha de Tratamiento de Datos y las del Acuerdo, prevalecerán las disposiciones de este último, salvo que en la Ficha se establezcan expresamente excepciones acordadas entre las Partes;
V. Que, en lo no previsto expresamente en estedocumento, serán de aplicación las disposiciones y definiciones contenidas en el Acuerdo y en el Contrato, que se entienden incorporadas por remisión.

En virtud de lo anterior, las Partes recogen en la tabla siguiente las especificaciones del tratamiento de Datos Personales relacionado con el Servicio, incluyendo información sobre finalidades, categorías de datos tratados, medidas de seguridad aplicadas y cualquier otro detalle relevante a efectos del Acuerdo.

	DESCRIPCION
SERVICIO	Plataforma Vidsigner
ENTIDAD PRESTADORA	**Validated ID SLU** 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.
BASE DEL TRATAMIENTO	El Encargado del Tratamiento podrá tratar los Datos

	Personales del Cliente en el contexto de la prestación del servicio, dentro de los límites estrictamente necesarios para la ejecución de los servicios previstos en el Contrato, en lo que respecta a: la recogida, el registro, la organización o estructuración, la consulta, el tratamiento, la selección, la extracción, la comparación, la utilización, la comunicación, la supresión o la destrucción.
FINALIDAD DEL TRATAMIENTO	Ejecución de los servicios de firma electrónica multicanal
MODALIDAD DE PRESTACIÓN DEL SERVICIO	Cloud SaaS (Shared/Private).
CATEGORIAS DE INTERESADOS	• Usuarios de la aplicación • Destinatarios de los procesos de firma
CATEGORIAS DE DATOS PERSONALES	Los Datos Personales tratados por el Encargado por cuenta del Responsable pertenecen a las siguientes categorías. **DATOS GENERALES:** • **De identificación del usuario y destinatarios**: nombre, apellidos, teléfono, email, NIF o equivalente, departamento, cargo, organización, biométricos del comportamiento conductual de la firma manuscrita recogida sobre un dispositivo tipo tablet. • **De contacto del usuario**: email, teléfono y otros. • **Del uso del servicio por el usuario y de registro de auditoría**: IP, URL, navegador, Sistema Operativo, fecha, y geolocalización de manera opcional. • **Los contenidos en los documentos enviados por la plataforma**. De libre elección por parte del Responsable del Tratamiento **CATEGORÍAS ESPECIALES DE DATOS**: • Datos de firma biométrica
LUGAR DE ALMACENAMIENTO DE LOS DATOS	Los datos se almacenan en los servidores del Encargado del Tratamiento y/o de los Subencargados situados dentro de la Unión Europea o del Espacio Económico Europeo (UE/EEE).
DURACIÓN DEL TRATAMIENTO	El tratamiento de los Datos Personales para la prestación de los Servicios tendrá la siguiente duración: Los documentos se conservarán durante 60 días a disposición del cliente contando con 30 días adicionales para su descarga Una vez transcurridos los períodos anteriormente mencionados, el Encargado del Tratamiento podrá conservar los Datos Personales en la medida en que ello constituya cumplimiento de obligaciones legales específicas o de órdenes emitidas por Autoridades competentes. Igualmente, se permite la conservación de los Datos Personales exclusivamente en la medida en que dichos datos sean necesarios para que el Encargado pueda

	acreditar, ejercer o defender sus propios derechos, durante un plazo máximo de 10 años.
MEDIDAS DE SEGURIDAD	Ref. **Annex III A - MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD**
SUB-ENCARGADOS	El Encargado del tratamiento utiliza otras empresas del Grupo Namirial y terceros seleccionados que ofrecen garantías de confidencialidad en el tratamiento de datos, para llevar a cabo las operaciones de tratamiento relacionadas con la prestación del Servicio. 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 sobre protección de datos personales, el Proveedor podrá utilizar mecanismos adecuados de transferencia de datos. Estas entidades son seleccionadas conforme a lo previsto en el Contrato, reciben instrucciones precisas sobre el tratamiento de los datos y realizan únicamente las actividades necesarias conforme a las directrices proporcionadas. Entre ellas Cláusulas Contractuales Tipo y decisión de adecuación de la comisión europea Privacy Framework, en el caso de Transferencias a Estados Unidos. La lista actualizada de estas entidades se incluye 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 en complemento de las previstas en el Contrato y constituyen un nivel adicional de protección para el tratamiento regulado por la Ficha de Tratamiento a la que se adjuntan. Estas medidas son aplicadas y aplicables al Proveedor del Servicio mencionado en el Contrato.

MEDIDAS TÉNICAS 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 o durante su transporte o almacenamiento en soportes de datos, y que sea posible verificar y determinar a qué entidades se han transmitido los datos personales: • • registro de accesos y operaciones relevantes; • prestación del servicio a través de conexiones cifradas como SFTP, HTTPS y plataformas de almacenamiento seguro en la nube; • uso de procedimientos de firma (según el nivel de firma elegido); detección de operaciones de recuperación y transmisión de datos; • transmisión en modo anónimo o seudonimizada; selección cuidadosa del personal y de los medios de transporte de documentos; procedimiento de entrega codificado. Se establecen otras medidas en las siguientes políticas internas: SCS-P01 Política del Grupo sobre Seguridad de la Información; SCS-P14 Política del Grupo sobre Privacidad y Protección de Datos Personales.
Medidas para garantizar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma oportuna en caso de un incidente físico o técnico	Se adoptan medidas técnicas y organizativas destinadas a garantizar la rápida restauración de la disponibilidad y el acceso a los datos personales en caso de incidente físico o técnico, incluyendo, en particular: • monitorización e informes de copias de seguridad; • restauración mediante herramientas automatizadas; • 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 lugar Seguro fuera de la sala de servidores. Se establecen otras medidas en las siguientes políticas internas: Plan de emergencia; SCS-P01 Política del Grupo sobre Seguridad de la Información; Instrucción de Trabajo sobre Seguridad Operativa.
Medidas para proteger los datos durante el almacenamiento	Medidas para garantizar la protección de los datos personales frente a la destrucción o pérdida accidental (como sistemas de alimentación ininterrumpida -SAI-, climatización, protección contra incendios, copias de seguridad de datos, almacenamiento seguro de soportes, protección antivirus, sistemas RAID, duplicación de discos,

	etc.): **Medidas Técnicas:** • Sistema de detección de incendios; • Extintor de incendios instalada en la sala de servidores; • Monitorización de temperatura y humedad en la sala de servidores; • Control de ventilación en la sala de servidoresSistema UPS (alimentación ininterrumpida) y generadores diésel de emergencia; • Sistema RAID/duplicidad de discos (disk mirroring);; • Videovigilancia continua en la sala de servidores; • Mensajes de alarma en caso de acceso no autorizado. **Medidas Organizativas:** • Servicio de copias de seguridad (backup); • Ausencia de tuberías en la sala de servidores; • Almacenamiento de soportes de respaldo en una ubicación segura fuera de la sala de servidores; • Particiones separadas para sistemas operativos y datos, cuando sea necesario. Se establecen otras medidas en las siguientes políticas internas: Plan de emergencia; SCS-P01 Política del Grupo sobre Seguridad de la Información; Instrucción de Trabajo sobre Seguridad Operativa.
Medidas para garantizar el registro de eventos (event logging)	Medidas organizativas adoptadas por el Encargado del Tratamiento: • proceso documentado para la detección y notificación de incidentes de seguridad/brechas de datos (véase la Política SCS-P04 de Gestión y Notificación de Incidentes del Grupo); • procedimiento formalizado para la gestión de incidentes de seguridad (véase la Política SCS-P04 de Gestión y Notificación de Incidentes del Grupo); • participación del Delegado de Protección de Datos (DPO) y del Responsable de Seguridad de la Información (CISO) en los incidentes de seguridad y brechas de datos; documentación de incidentes y brechas mediante el sistema de tickets (a través de la herramienta “Jira”; • proceso formal de seguimiento de los incidentes de seguridad y brechas de datos (véase la Política SCS-P04 de Gestión y Notificación de Incidentes del Grupo). Se establecen otras medidas en las siguientes políticas internas: Política de Seguridad de la Información del Grupo (SCS-P01); Política de Privacidad y Protección de Datos Personales del Grupo (SCS-P14); Instrucción operativa de seguridad; Instrucción de uso para usuarios de TI.
Medidas para garantizar la configuración del sistema, incluida la configuración predeterminada	El Encargado del tratamiento implementa las siguientes medidas para garantizar la integridad del sistema: uso de cortafuegos actualizados regularmente; uso de filtros de spam actualizados regularmente; uso de antivirus actualizado regularmente; sistema de detección de intrusiones (IDS) para los sistemas del Cliente; sistema de

	prevención de intrusiones (IPS) para los sistemas del Cliente.
Medidas internas de gestión y gobernanza de TI y ciberseguridad	El sistema cumple con la certificación ISO/IEC 27001 Y Esquema Nacional de Seguridad
Medidas para garantizar la limitación de la conservación de datos	Se realizan comprobaciones de seguridad OWASP Secure Mobile Development (véase, Política de Codificación Segura del Grupo SCS-P08). Análisis del perímetro de aplicaciones web
Medidas para garantizar la rendición de cuentas	Los empleados del Encargado reciben formación e información continua sobre protección de datos y están contractualmente obligados al secreto y la confidencialidad de los datos. Los terceros que puedan tener contacto con datos personales durante su trabajo para Validated, y/o entidades del Grupo Namirial están obligados a mantener el secreto y la confidencialidad de los datos mediante un acuerdo de confidencialidad (NDA, por sus siglas en inglés) antes del inicio de su actividad. Todas las empresas afiliadas al Encargado dentro de la UE han suscrito o suscribirán un acuerdo marco común sobre protección de datos y tratamiento por encargo como instrumento jurídico conforme al artículo 28 del RGPD, con el fin de garantizar un estándar uniforme de protección y seguridad de los datos en todo el grupo y regular los derechos y obligaciones relativos a cualquier tratamiento por cuenta de terceros
Medidas para permitir la portabilidad de los datos y garantizar su supresión	El Encargado 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 tienen autorización de acceso, y que los datos personales no puedan ser leídos, copiados, modificados ni eliminados sin autorización durante el tratamiento, uso y tras su almacenamiento.

ANNEXO III - B

SUBENCARGADOS

Este Anexo enumera los Subencargados aprobados a la fecha de firma de la correspondiente Ficha de Tratamiento de Datos, conforme al Acuerdo.

Las entidades enumeradas han sido seleccionadas en base 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 del tratamiento, respetando las instrucciones recibidas y adoptando medidas de seguridad adecuadas para la protección de los Datos Personales tratados.

La lista de Subencargados podrá actualizarse a lo largo del tiempo de conformidad con lo establecido en el Acuerdo.

NOMBRE DE LA EMPRESA	DIRECCIÓN	UBICACIÓN DEL TRATAMIENTO	ALCANCE DE LA ACTIVIDAD
MICROSOFT IRELAND OPERATIONS LIMITED	Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublín 18, Ireland	Holanda, Unión Europea	Uso de servidores para almacenamiento de la información alojada en la plataforma
Zendesk, Inc	1019 Market Street, San Francisco, CA 94103, United States	Irlanda, Unión Europea	Plataforma utilizada para los tickets de atención al RESPONSABLE, la información proporcionada para la gestión de incidencias y consultas
Atlassian Pty Ltd	341 George Street, Sydney, NSW 2000	Irlanda, Unión Europea.	Productos de software de seguimiento, colaboración, comunicación, gestión de servicios y desarrollo para equipos en organizaciones
Twilio Inc	101 Spear St, 1st floor San Francisco, CA 94105	Estados Unidos	Plataforma de comunicación y mensajería para empresas (servicios de SMS y mailing, entre otros).
Cloudflare, Inc	10 Townsend st, San Francisco (California) 94107 EE. UU	Unión Europea (España)	Red de Entrega de Contenido (CDN) protección del tráfico web.
Link Mobility Italia S.r.l	Via Paolo Da Cannobio 37 - 20122 - Milán (Mi)	Unión Europea (Italia)	Plataforma de comunicación y mensajería para empresas (servicios de SMS, RCS, WhatsApp, Telegram y correo electrónico), se comparte número de tlfno y mail y los que se incluyan en el cuerpo de la comunicación del propio mensaje o correo electrónico por parte del cliente

Vonage B.V.	Radarweg 29 A 12, Oficina 10.42, 1043NX Ámsterdam, Países Bajos	Unión Europea	Plataforma de comunicación y mensajería para empresas (servicios de SMS, RCS, WhatsApp, Telegram y correo electrónico,), se comparte número de tlfno y mail y los que se incluyan en el cuerpo de la comunicación del propio mensaje o correo electrónico por parte del cliente.
Mitto AG	Bahnhofstrasse 21, Zug CH-6300, Suiza	Unión Europea	Plataforma de comunicación y mensajería para empresas (servicios de SMS, RCS, WhatsApp, Telegram y correo electrónico), se comparte número de tlfno y mail y los que se incluyan en el cuerpo de la comunicación del propio mensaje o correo electrónico por parte del cliente.
Twilio Ireland Ltd	25-28 North Wall Quay, Dublino, Irlanda	Unión Europea y USA	Plataforma de comunicación y mensajería para empresas (servicios de SMS, RCS, WhatsApp, Telegram y correo electrónico,), se comparte número de tlfno y mail y los que se incluyan en el cuerpo de la comunicación del propio mensaje o correo electrónico por parte del cliente. La ubicación del tratamiento requerirá de transferencia internacional a USA cuando se realicen mensajes a destinatarios en esa ubicación.
Namirial SPA*	Via Caduti sul Lavoro, 4 – 60019 Senigallia (AN), Italia	EEE	Servicios en la nube / Proveedor de servicios / TI / Gestión de soporte de tickets / Monitorización de registros / Servicios SMS / Proveedor de correo electrónico / SOC (Centro de Operaciones de Seguridad) y MOC (Centro de Operaciones de Monitorización)

*La lista de los encargados del tratamiento adicionales utilizados por Namirial S.p.A. está disponible previa solicitud.