CONTRATO DE ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

1. Objeto del encargo de tratamiento: El presente documento constituye el contrato de encargado de tratamiento que formaliza la mercantil RAIOLA NETWORKS, S.L., con domicilio social en Avda. de Magoi, 66, SS, Dcha., C.P. 27002 Lugo (Lugo), con C.I.F.: B27453489, debidamente inscrita en el Registro Mercantil de Lugo al Tomo 460, Folio 183, Hoja LU-17.342 y con correo electrónico de contacto: info@raiolanetworks.com. (En adelante, RAIOLA NETWORKS, o el ENCARGADO DEL TRATAMIENTO) y el CLIENTE (en adelante, el CLIENTE, o el RESPONSABLE DEL TRATAMIENTO indistintamente), en tanto que contratante de los servicios de RAIOLA NETWORKS.

Para la prestación de los servicios contratados, puede darse la circunstancia de que determinados datos personales responsabilidad del RESPONSABLE DE TRATAMIENTO sean alojados en los servidores del ENCARGADO DE TRATAMIENTO.

Con la contratación de los servicios de RAIOLA NETWORKS, se habilita al ENCARGADO DEL TRATAMIENTO para el tratamiento por cuenta del RESPONSABLE DEL TRATAMIENTO de los datos personales que haya recabado, conforme a lo previsto en las presentes cláusulas y consistente únicamente en el almacenamiento que, en su caso realice, de los mismos en los Servidores de RAIOLA NETWORKS.

2. Identificación de la información afectada: La prestación de los servicios objeto de este contrato, no implica que, como regla general, RAIOLA NETWORKS acceda a los datos de carácter personal de los ficheros que el RESPONSABLE DE TRATAMIENTO aloje en sus servidores, puesto que dicho acceso no es necesario para la prestación del servicio por parte de RAIOLA NETWORKS.

No obstante lo anterior, a los efectos previstos en el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), en el desarrollo de las funciones propias del servicio contratado, RAIOLA NETWORKS realiza, según el concepto legal, tratamientos de datos de carácter personal del cliente, en la medida en que el servicio prestado implica el almacenamiento de los datos en los servidores de su titularidad.

A tal efecto, RAIOLA NETWORKS, en su condición de ENCARGADO DE TRATAMIENTO, manifiesta que únicamente tratará los datos en la medida en que estos se alojan en sus servidores, al ceder al RESPONSABLE DE TRATAMIENTO un espacio virtual en el que éste volcará y administrará en exclusiva dichos datos. Tales tareas se llevarán a cabo conforme a lo establecido en el presente documento, que contiene las instrucciones que han de seguirse en dicho tratamiento.

En caso de que el RESPONSABLE DE TRATAMIENTO estimase oportuno impartir instrucciones distintas de las referidas en el presente documento, las comunicará de forma expresa a RAIOLA NETWORKS, quien, en caso de que impliquen alteración de las condiciones del servicio pactadas, podrá resolver el contrato.

Cualquier otro tratamiento de datos que deba realizar RAIOLA NETWORKS distinto del mencionado, deberá ser solicitado por escrito por el cliente y aceptado por RAIOLA NETWORKS. En ese momento, se fijarán las instrucciones que RAIOLA NETWORKS deba cumplir, según el cliente, para llevar a cabo esos otros tratamientos de datos adicionales.

3. Obligaciones y derechos del RESPONSABLE: El RESPONSABLE garantiza que los datos facilitados al ENCARGADO se han obtenido lícitamente y que son adecuados, pertinentes y limitados a los fines del tratamiento.

El RESPONSABLE pondrá a disposición del ENCARGADO cuanta información sea necesaria para ejecutar las prestaciones objeto del encargo.

El RESPONSABLE advierte al ENCARGADO que, si determina por su cuenta los fines y los medios del tratamiento, será considerado responsable del tratamiento y estará sujeto a cumplir las disposiciones de la normativa vigente aplicables como tal.

4. Obligaciones y derechos del ENCARGADO: El ENCARGADO se obliga a respetar todas las obligaciones que pudieran corresponderle como encargado del tratamiento conforme lo dispuesto en la normativa vigente y cualquier otra disposición o regulación que le fuera igualmente aplicable.

El ENCARGADO no destinará, aplicará o utilizará los datos a los que tenga acceso para un fin distinto al encargo o que suponga el incumplimiento de este contrato.

El ENCARGADO pondrá a disposición del RESPONSABLE la información necesaria para demostrar el cumplimiento del contrato, permitiendo las inspecciones y auditorías necesarias para evaluar el tratamiento.

5. Personal autorizado para realizar el tratamiento: El ENCARGADO garantiza que el personal autorizado para realizar el tratamiento se ha comprometido de forma expresa y por escrito a respetar la confidencialidad de los datos.

El ENCARGADO tomará medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones del RESPONSABLE o esté obligada a ello en virtud de la legislación vigente.

El ENCARGADO garantiza que el personal autorizado para realizar el tratamiento ha recibido la formación necesaria para asegurar que no se pondrá en riesgo la protección de datos personales.

6. Medidas de seguridad: El ENCARGADO manifiesta estar al corriente en lo que

concierne a las obligaciones derivadas de la normativa de protección de datos, especialmente en lo que se refiere a la implantación de las medidas de seguridad para las diferentes categorías de datos y de tratamiento establecidas en el artículo 32 del RGPD, cuando resulte de aplicación.

El ENCARGADO garantiza que se implementarán de forma adecuada dichas medidas de seguridad y cooperará con el RESPONSABLE para avalar su cumplimiento.

El RESPONSABLE realizará un análisis de los posibles riesgos derivados del tratamiento para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos de los interesados y, si determinara que existen riesgos, trasladará al ENCARGADO un informe con la evaluación de impacto para que proceda a la implementación de medidas adecuadas para evitarlos o mitigarlos.

El ENCARGADO, por su parte, deberá analizar los posibles riesgos y otras circunstancias que puedan incidir en la seguridad que le sean atribuibles, debiendo informar, si los hubiere, al RESPONSABLE para evaluar su impacto.

De todas formas, el ENCARGADO garantiza que se implementarán las siguientes medidas de protección de datos, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento:

- Seudonimización y cifrado de datos personales.

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

- Restaurar la disponibilidad y el acceso a datos de forma rápida en caso de incidente físico o técnico.

- Procedimientos de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

En concreto, el ENCARGADO dispone de las siguientes medidas de seguridad:

El servicio cuenta con las medidas de seguridad impuestas en los centros de datos (Data Center) consistentes en:

Acceso: El área interna y externa de los centros de datos está monitorizada con vídeo y sensores de movimiento y dispone de personal de vigilancia, todo ello 24 horas al día, todos los días del año.

El perímetro de los centros está cercado con alambradas de alambre de púas.

El personal de los centros de datos cuenta con una insignia de identificación RFID, usada para permitir su acceso a través de las puertas de seguridad. El acceso a los centros de datos tiene un nivel mayor de protección: solo el personal autorizado podrá acceder.

Cada sala del centro de datos cuenta con sistema de detección y extinción de fuego,

así como puertas contra incendios y los centros de datos cumplen la regla APSAD R4 de instalación de extintores.

Red de comunicaciones: Red de fibra óptica propia y Red de datos redundante: varios enlaces para evitar el riesgo de no disponibilidad de los servicios.

Hardware: Personal técnico presente 24 horas, todos los días del año, en los centros de datos para asegurar que los servidores están mantenidos de forma constante

Servidores con fuentes de alimentación y tarjetas de red redundadas.

Alimentación eléctrica: Los centros de datos están alimentados por dos fuentes de alimentación eléctrica separadas y están equipados con sistemas de alimentación ininterrumpida. Existen generadores eléctricos que cuentan con una autonomía de 48 horas para contrarrestar cualquier fallo de la red de suministro eléctrico.

Además, se establecen las siguientes medidas de seguridad en función del tipo de servicio de que se trate:

Servidores compartidos o hosting web:

Sistema de almacenamiento replicado para evitar pérdida de datos ante fallos de hardware. Copias de seguridad de datos con periodicidad diaria (retención de las 14 últimas).

Sistema para evitar el degradado del servicio a raíz de usuarios haciendo uso excesivo de sus recursos contratados. Monitorización en tiempo real de la infraestructura para la detección proactiva de posibles degradaciones de servicio.

Protección contra todos los tipos de ataques distribuidos de denegación de servicio (DDoS).

Actualizaciones software de la infraestructura aplicadas sin necesidad de ventana de corte de servicio.

Filtrado de comunicaciones entrantes y salientes mediante cortafuegos.

Acceso a gestión datos de usuario mediante autenticación con usuario y contraseña. Cuentas de usuario aisladas, asegurado que un usuario solo tendrá acceso a sus datos y recursos contratados.

Mitigación automatizada de ataques de fuerza bruta contra aplicaciones y servicios.

Posibilidad de habilitar comunicaciones cifradas en aplicaciones vía protocolo HTTPS.

Filtrado de comunicaciones entrantes y salientes mediante cortafuegos.

Actualizaciones software de la infraestructura automatizadas.

Análisis de malware en tiempo real de todos los archivos transferidos por los usuarios.

Cortafuegos de aplicaciones para mitigar ataques conocidos contra la infraestructura.

Servidores Privados Virtuales (VPS):

Sistema de almacenamiento replicado para evitar pérdida de datos ante fallos de hardware.

Copias de seguridad de datos con periodicidad diaria (retención 3 últimas).

Protección contra todos los tipos de ataques distribuidos de denegación de servicio (DDoS).

Monitorización en tiempo real de la infraestructura de virtualización para la detección proactiva de posibles degradaciones de servicio.

Confidencialidad: Acceso a servidor virtual de usuario mediante autenticación con usuario y contraseña.

Acceso a servidor virtual de usuario mediante sistema criptográfico de clave pública.

Servidores dedicados:

Sistema de almacenamiento replicado para evitar pérdida de datos ante fallos de hardware.

Copias de seguridad de datos conforme al servicio contratado por el cliente.

Protección contra todos los tipos de ataques distribuidos de denegación de servicio (DDoS).

Filtrado de comunicaciones entrantes y salientes mediante cortafuegos.

Acceso a gestión del servidor mediante autenticación con usuario y contraseña.

Acceso a gestión del servidor mediante autenticación con sistema criptográfico de clave pública.

7. Violación de la seguridad: Las violaciones de seguridad que tenga conocimiento el ENCARGADO deberán notificarse, sin dilación indebida y en un máximo de 24 horas, al RESPONSABLE para su conocimiento y aplicación de medidas para remediar y mitigar los efectos ocasionados. No será necesaria la notificación cuando sea improbable que comporte un riesgo para los derechos y las libertades de las personas físicas.

La notificación de una violación de seguridad deberá contener, como mínimo, la siguiente información:

- Descripción de la naturaleza de la violación.
- Categorías y el número aproximado de interesados afectados.
- Categorías y el número aproximado de registros de datos afectados.
- Posibles consecuencias.
- Medidas adoptadas o propuestas para remediar o mitigar los efectos.
- Datos de contacto donde pueda obtenerse más información (DPO, responsable de seguridad, etc.).

Cuando la violación de seguridad se haya producido bajo la responsabilidad del ENCARGADO, el RESPONSABLE podrá obligarle a notificarla a la Autoridad de control y, si fuera necesario, a comunicarla a los interesados afectados.

8. Comunicación de los datos a terceros: El ENCARGADO no podrá comunicar los datos a otros destinatarios, salvo que hubiera obtenido una autorización previa y por escrito del RESPONSABLE; la cual, de existir, se anexará al presente contrato.

La transmisión de datos a Autoridades públicas en el ejercicio de sus funciones públicas no son consideradas comunicaciones de datos, por lo que no se precisará de la autorización del RESPONSABLE si dichas transmisiones son necesarias para alcanzar la finalidad del encargo.

9. Transferencias internacionales de datos: El ENCARGADO no podrá realizar transferencias de datos a terceros países u organizaciones internacionales no establecidos en la UE, salvo que hubiera obtenido una autorización previa y por escrito del RESPONSABLE; la cual, de existir, se anexará al presente contrato.

10. Subcontratación del tratamiento de datos: El ENCARGADO no podrá subcontratar a un tercero la realización de ningún tratamiento de datos que le hubiera encomendado el RESPONSABLE, salvo que hubiera obtenido de éste una autorización previa y por escrito para ello; la cual, de existir, se anexará al presente contrato.

A tal efecto, el RESPONSABLE DEL TRATAMIENTO autoriza de forma expresa la subcontratación de los servicios de hosting con la mercantil OVH HISPANO, S.L.U., con CIF B-83834747 e inscrita en el Registro Mercantil de Madrid, al Tomo 19514, Libro 0, Folio 77, Sección 8, Hoja M-342678. El domicilio social está en Madrid, C/ Princesa nº 22, 2º Dcha., 28008 Madrid.

Para subcontratar con otras empresas, el ENCARGADO debe comunicarlo por escrito al RESPONSABLE, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de 15 días naturales.

El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el ENCARGADO DEL TRATAMIENTO y las instrucciones que dicte el responsable. Corresponde al ENCARGADO regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad, etc.) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el ENCARGADO seguirá siendo plenamente

responsable ante el RESPONSABLE en lo referente al cumplimiento de las obligaciones.

11. Derechos de los interesados: El ENCARGADO creará, siempre que sea posible y teniendo en cuenta la naturaleza del tratamiento, las condiciones técnicas y organizativas necesarias para asistir al RESPONSABLE en su obligación de responder las solicitudes de los derechos del interesado.

En el caso de que el ENCARGADO reciba una solicitud para el ejercicio de dichos derechos, deberá comunicarlo al RESPONSABLE de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente con otras informaciones que puedan ser relevantes para resolver la solicitud.

Cuando los datos sean tratados exclusivamente con los sistemas del ENCARGADO, deberá resolver, por cuenta del RESPONSABLE, y dentro del plazo establecido, las solicitudes recibidas para el ejercicio de los derechos del interesado en relación con los datos objeto del encargo, sin menoscabo de comunicarlo al RESPONSABLE de acuerdo con lo establecido en el párrafo anterior; a saber, los derechos de acceso, rectificación, supresión y portabilidad de datos y los de limitación u oposición al tratamiento, y si fuera el caso, a no ser objeto de decisiones individualizadas automatizadas.

12. Responsabilidad: Conforme a lo establecido en el artículo 82 del RGPD, el ENCARGADO se hace responsable frente al RESPONSABLE por los daños y perjuicios causados a interesados o terceros incluidas las sanciones administrativas, que se deriven de reclamaciones judiciales o extrajudiciales o de procedimientos sancionadores de la Autoridad de control, que sean consecuencia de la inobservancia de las instrucciones asumidas en el presente contrato.

13. Confidencialidad: EL ENCARGADO se compromete a guardar la máxima reserva y secreto sobre la información clasificada como confidencial. Se considerará información confidencial cualquier dato al que EL ENCARGADO acceda en virtud del presente contrato y/o en el acuerdo general que regula los servicios a prestar por parte de EL ENCARGADO a EL RESPONSABLE, en especial la información y datos propios de EL RESPONSABLE a los que haya accedido o acceda durante la ejecución del mismo. No tendrán el carácter de confidencial todas aquellas informaciones y datos que fueran de dominio público o que estuvieran en posesión de EL ENCARGADO con anterioridad a iniciar la prestación de sus servicios y hubieran sido obtenidas por medios lícitos.

La referida obligación de confidencialidad tendrá carácter indefinido, manteniéndose en vigor con posterioridad a la finalización del contrato de prestación de servicios del que el presente trae causa.

14. Fin de la prestación de servicio: Una vez finalice la prestación de servicios objeto

de este contrato, el ENCARGADO certificará, a elección del RESPONSABLE, la supresión o devolución de todos los datos personales y las copias existentes.

No procederá la supresión de datos cuando se requiera su conservación por una obligación legal, en cuyo caso el ENCARGADO procederá a la custodia de los mismos bloqueando los datos y limitando su tratamiento en tanto que pudieran derivarse responsabilidades de su relación con el RESPONSABLE.

El ENCARGADO mantendrá el deber de secreto y confidencialidad de los datos incluso después de finalizar la relación objeto de este contrato.

Y para que conste a los efectos oportunos, en prueba de conformidad de las partes, firman el presente contrato, por duplicado ejemplar y a un solo efecto, en , a de de 20

EL RESPONSABLE DE TRATAMIENTO:

EL ENCARGADO DE TRATAMIENTO

_____

EMPRESA:
Representante legal:

_____

RAIOLA NETWORKS, S.L.
Fdo.: Martín Gómez Hermida