Encargado		*Responsable*	
Id.	*Soluciones Web Online, S.L.*	*Id.*	
NIF	*B04437729*	*NIF*	
Dirección	*Calle Hermanos Machado, 19, CP 04720 EL PARADOR, Almeria*	*Dirección*	
Actividades	*Hosting; Gestión de dominios; Desarrollo; Soporte técnico; SEO; VPN*		
Versión	*2022/11/30*		

1. Duración

1.1. La misma que el servicio que el cliente tenga contratado, según el caso, como hosting, gestión de dominios, desarrollo, soporte técnico, SEO, VPN… y del que este acuerdo forma parte como anexo.

2. Datos

x Identificativos
□ Patrimoniales
x Económicos
□ Académicos
□ Profesionales
□ Biométricos
□ Salud
□ Sexualidad
□ Ideología
□ Raza

3. Categorías

x Contactos
x Clientes
□ Empleados
□ Proveedores
□ Voluntarios
□ Visitantes
□ Usuarios
□ Suscriptores
□ Donantes
□ Beneficiarios
□ Accionistas
□ Representantes
□ Otros

4. Operaciones autorizadas

x Recogida
x Estructuración
x Almacenamiento
x Cesión
x Utilización
x Copia
x Cifrado
□ Seudonomización
□ Anonimización
□ Bloqueo
x Eliminación

5. Obligaciones del responsable del tratamiento

5.1. Asegurarse de que los datos que cede al procesador de datos han sido recogidos por medios leales y lícitos, según los principios rectores de la normativa de datos personales y se mantienen actualizados y veraces.

5.2. Entregar al procesador de datos los datos precisos para la prestación de los servicios contratados.

5.3. Realizar una evaluación del impacto en los datos personales de las operaciones de tratamiento a realizar por el procesador de datos, en los casos en que así proceda.

5.4. Realizar las consultas previas que corresponda.

5.5. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del procesador de datos.

5.6. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

5.7. Facilitar el derecho de información en el momento de recogida de los datos.

6. Obligaciones del procesador de datos

6.1. El procesador de datos asume todas las obligaciones establecidas en el Reglamento (UE) 2016/769 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento general de Protección de datos o GDPR), la Ley Orgánica de protección de datos de Carácter Personal y demás normativa que resulten aplicables, su normativa de desarrollo; así como las que deriven de las estipulaciones que se regulan en el presente acuerdo y, en particular, lo hará conforme a las siguientes.

6.2. ***Finalidad e instrucciones***

6.2.1. El procesador de datos única y exclusivamente tratará los datos facilitados por el responsable del tratamiento con la finalidad de prestarle los servicios que forman parte de la relación contractual principal que mantiene con el responsable del tratamiento.

6.2.2. La relación de nuevos servicios o la identificación de nuevos usos o finalidades de utilización de los datos exigirá un nuevo acuerdo de las partes y/o una actualización del presente acuerdo.

6.2.3. En ningún caso podrá utilizar datos para fines propios.

6.2.4. Si el procesador de datos considera que alguna de las instrucciones del responsable del tratamiento infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el procesador de datos le informará inmediatamente.

6.3. ***Registro de Actividad***

6.3.1. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

6.3.1.1. El nombre y los datos de contacto del procesador de datos o procesador de datos y de cada responsable del tratamiento por cuenta del cual actúe el procesador de datos y del representante del responsable del tratamiento o del procesador de datos y del delgado de protección de datos.

6.3.1.2. Las categorías de tratamientos efectuados por cuenta de cada responsable del tratamiento.

6.3.1.3. En su caso, las transferencias de datos personales a terceros países u organizaciones internacionales, incluidas las identificaciones de dichos terceros países u organizaciones internacionales y, en el caso de las transferencias indicadas en el artículo 40 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

6.3.1.4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

6.3.1.4.1. La seudonimización y el cifrado de datos personales.

6.3.1.4.2. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

6.3.1.4.3. Las directrices para restaurar la disponibilidad a los datos personales de forma rápida, en caso de incidente físico.

6.3.1.4.4. El procedimiento de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

6.4. ***Cesiones a Terceros***

6.4.1. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento; sea necesario para prestar el servicio o en los supuestos legalmente admisibles.

6.4.2. El procesador de datos puede comunicar los datos a otros procesadores de datos de datos del mismo responsable del tratamiento, de acuerdo con las instrucciones del responsable del tratamiento. En este caso, el responsable del tratamiento identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

6.4.3. Si el procesador de datos debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable del tratamiento de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

6.5. ***Subcontratación***

6.5.1. Se autoriza al procesador de datos a subcontratar los servicios auxiliares necesarios para sostener la estructura general del procesador de datos, por ejemplo: servicios de telecomunicaciones, mantenimiento de hardware u otros análogos. Todo ello, sin perjuicio de que el procesador de datos deberá suscribir los correspondientes acuerdos de procesador de datos de tratamiento con tales subcontratas.

6.5.2. En cambio, si para la prestación del servicio que se facilita al responsable del tratamiento, el procesador de datos precisa subcontratar medios o servicios directamente necesarios con los que son objeto del acuerdo principal, entonces deberán ser autorizados previamente por el responsable del tratamiento de manera expresa y por escrito, ya se trate de personas jurídicas o físicas (autónomos), que deberán quedar identificados por su nombre o razón social y NIF, así como el servicio concretamente subcontratado que prestan. Todo ello, previamente a su intervención en la prestación del servicio al responsable del tratamiento.

6.5.3. En cualquier caso, el subcontratista, que también tiene la condición de procesador de datos, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el procesador de datos y las instrucciones que dicte el responsable del tratamiento. Corresponde al procesador de datos inicial regular la nueva relación, de forma que el nuevo procesador de datos quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) 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 sub procesador de datos, el procesador de datos inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

6.6. ***Secreto***

6.6.1. El procesador de datos tiene la obligación de mantener el deber de secreto respecto a los datos personales a los que tenga acceso, incluso después de que finalice el objeto del presente encargo.

6.6.2. Solamente tratarán los datos de los ficheros aquellos empleados del procesador de datos de tratamiento que tengan entre sus funciones el cumplimiento de la prestación prevista en este acuerdo y no pudieran cumplir sus obligaciones sin tener acceso a los mismos. Dichas personas deberán observar la obligación legal de confidencialidad.

6.6.3. Además, el procesador de datos deberá:

6.6.3.1. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

6.6.3.2. Mantener a disposición del responsable del tratamiento la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

6.6.3.3. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

6.7. ***Asistencia al responsable del tratamiento en el ejercicio de Derechos por Terceros***

6.7.1. El procesador de datos deberá asistir al responsable del tratamiento en el ejercicio de los derechos de:

6.7.1.1. Acceso, rectificación, supresión y oposición.

6.7.1.2. Limitación del tratamiento.

6.7.1.3. Portabilidad de datos.

6.7.1.4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

6.8. ***Notificación de violaciones de la seguridad de los datos***

6.8.1. En los casos legales, el procesador de datos notificará al responsable del tratamiento, a través de correo electrónico, las violaciones de la seguridad de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia. Lo cual llevará a cabo sin dilación indebida y, en cualquier caso, antes del plazo máximo de 72 horas, desde que conociera la brecha.

6.8.2. De acuerdo con la Ley, no será necesaria la notificación cuando sea improbable que dicha violación de seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

6.8.3. En el caso de tener que notificarse, si se dispone de ella, se facilitará, como mínimo, la siguiente información:

6.8.3.1. Descripción de la naturaleza de la violación de los datos personales, inclusive, cuando sea posible, el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

6.8.3.2. El nombre y los datos de contacto del delegado de datos o de otro punto de contacto en el que pueda obtenerse más información.

6.8.3.3. Descripción de las posibles consecuencias de la vulneración de la seguridad de los datos personales.

6.8.3.4. Descripción de las medidas adoptadas para poner remedio a la violación de la seguridad de los datos, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

6.8.3.5. Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

6.9. ***Evaluaciones de impacto***

6.9.1. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

6.10. ***Control y Auditoría***

6.10.1. Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realice el responsable u otro auditor autorizado por él.

6.11. ***Medidas de Seguridad***

6.11.1. El procesador de datos queda obligado a implantar y observar, como mínimo, las medidas de seguridad siguientes:

6.11.1.1. Garantizar la confidencialidad y resiliencias permanentes de los sistemas y servicios de tratamiento.

6.11.1.2. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

6.11.1.3. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para la seguridad del tratamiento.

6.11.1.4. Seudonimizar y cifrar los datos personales, según los supuestos en que así proceda.

6.11.1.5. Las medidas de seguridad concretas adoptadas se describen en el Anexo II de Medidas de Seguridad.

6.11.1.6. Sin perjuicio de todo ello, el responsable del tratamiento podrá imponer otras medidas que puedan resultar de la evaluación de riesgos.

6.11.1.7. Sin perjuicio de todo ello, el encargado de tratamiento no puede dar una garantía absoluta y total sobre la inexistencia de violaciones de seguridad causadas por terceros.

6.12. ***Destino de los Datos al finalizar el servicio***

6.12.1. Al finalizar el servicio, el procesador de datos destruirá los datos que consten digital o analógicamente, salvo que el responsable del tratamiento disponga su conservación a través de las opciones de configuración de su panel de administración de cliente.

6.12.2. No obstante, incluso en el caso de destrucción, el procesador de datos podrá conservar una copia, con los datos debidamente bloqueados, por los plazos legales aplicables por los que no hayan prescrito cualesquiera responsabilidades derivadas de la prestación del servicio.

7. Información a los intervinientes del acuerdo

7.1.1. Responsable del tratamiento es cada parte interviniente cuyos datos obran en la cabecera.

7.1.2. La finalidad es dar cumplimiento a este acuerdo.

7.1.3. La legitimación es contractual.

7.1.4. No se cederán datos a terceros salvo amparo legal.

7.1.5. Derechos: a) acceso; b) rectificación; c) supresión; d) bloqueo; e) oposición; f) eliminación; g) desautomatización; h) portabilidad. Tales derechos los podrá ejercitar el titular de los datos mediante petición escrita adjuntando copia del Documento Nacional de Identidad, Pasaporte o documento equivalente (en el caso de actuar mediante representante, deberá acreditarse la autorización con que cuenta éste), expresando los datos afectados y el tipo de los derechos indicados que se ejercita, dirigida a las direcciones o medios de contacto del responsable del tratamiento que proceda según quién los ejercite y que figuran en la cabecera de este acuerdo.

7.1.6. Los datos se conservarán: a) por la duración de la relación contractual; b) por los plazos de prescripción de las obligaciones y responsabilidades legales.

7.1.7. Los interesados podrán interponer denuncia ante la AEPD en caso de considerar un uso indebido de sus datos.

Anexo I – Subcontratados

Proveedor	Servicio
Aspa Cloud, S.L.	Centro de datos
InterXion Holding NV	Proveedor europeo de servicios de centros de datos de colocación y operador neutral y en la nube
PCore Datacenter SL	Centro de datos
Infusion Software, Inc.	Plataforma de ventas y marketing por correo electrónico para empresas para administrar y optimizar el ciclo de vida del cliente
Hosting Concepts B.V.	Plataforma de gestión de dominios
Asesoría Antonio Pérez, S.L.	Asesoría laboral, fiscal y contable
Cloudflare, Inc.	Plataforma que gestiona la entrega de contenido, servicios de seguridad de Internet y servicios de servidores de nombres de dominio distribuidos, localizados entre el visitante y el proveedor de alojamiento, y que actúan como proxy inverso para sitios web
Ucelay Abogados, S.L.P.U.	Asesoramiento en protección de datos, contratos y derecho corporativo en general. DPD de Profesional Hosting

Anexo II -
Medidas de Seguridad

1. **En relación a los proveedores en la nube que utilizamos:**
    1. Son homologados legalmente de forma previa para asegurarnos de que cumplen con la normativa de privacidad.
    2. Verificamos que cumplen con los estándares de seguridad más exigentes según cada nivel de protección aplicable.
2. **Confidencialidad permanente de los sistemas y servicios de tratamiento.**
    1. Solamente el personal autorizado puede acceder a los datos personales tratados.
    2. El personal solamente puede acceder a los datos personales correspondientes a la naturaleza de las funciones desempeñadas.
    3. La comunicación de datos entre cliente y servidor se produce mediante protocolos HTPPS o certificados SSL.
    4. Protección con Contraseña de Directorios mediante factores de doble autenticación y autenticación mediante llaves físicas.
    5. Nos apoyamos en redes VPN para crear conexiones seguras entre nuestros ordenadores remotos.
3. **Resiliencia permanente de los sistemas y servicios de tratamiento.**
    1. Usamos sistemas de detección de intrusiones de red.
    2. Adoptamos medidas de hardening para minimizar vulnerabilidades en el servidor.
    3. Los sistemas que tratan la información están protegidos.
        1. Contra ataques DDOS.
        2. Por firewalls.
        3. Por bloqueadores de IP maliciosas.
    4. Sistemas antivirus, alertas y sandboxing que se activan ante casos de posible entrada de Malware:
        1. En caso de que un atacante infecte el sistema de un cliente, se detectará y aislará para que se extienda.
        2. En dicho caso, además, se enviarán los archivos infectados a cuarentena y se avisará al cliente para que los sustituya o revise al efecto de poder remover el código malicioso.
    5. Prevención:
        1. Sometemos nuestros procesos a auditorías de seguridad periódicas.
        2. Sujetamos nuestros sistemas a pruebas de hacking ético. Disponemos de nuestro propio equipo rojo de seguridad.
4. **Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.**
    1. Usamos tecnologías para facilitar una rápida y flexible restauración de los sistemas e informaciones respaldados.
    2. Utilizamos sistemas de redundancia de nuestra infraestructura (no de los contenidos alojados por nuestros clientes), para permitir una disponibilidad total del servicio prestado.
    3. Compromiso SLA para ofrecer una disponibilidad de servicio cercana al 99,99% en el último ejercicio económico (https://www.profesionalhosting.com/contratos/sla.html).
5. **Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para la seguridad del tratamiento.**

1. Llevamos a cabo las actualizaciones, correcciones de errores y parches de seguridad de los sistemas.

2. Ejecutamos análisis periódicos de la seguridad de los servidores.

3. Procesos de pruebas previas a la actualización.

4. Los scripts que se ofrecen para su instalación semi automatizada, adoptan medidas de seguridad por defecto manualmente reversibles. En el caso de Wordpress, por ejemplo:

    1. Seguridad del directorio wp-includes
    2. Seguridad del directorio wp-content/uploads
    3. Desactivada concatenación de scripts para el panel del administrador de WordPress
    4. Desactivada por defecto la función de pingbacks
    5. Protección contra Hotlink
    6. Desactivada edición de archivos en el panel de información de WordPress
    7. Protección de bots
    8. Bloqueado el acceso a archivos potencialmente confidenciales
    9. Bloqueado el acceso a .htaccess y .htpasswd
    10. Bloqueado análisis author
    11. Permisos exigidos para acceder a los archivos y directorios
    12. Claves de seguridad adicionales
    13. Permisos para la exploración de directorios
    14. Seguridad del archivo de configuración
    15. Desactivada la ejecución de PHP en directorios de la caché
    16. Prefijo de la tabla de la base de datos
    17. Bloquear el acceso a archivos confidenciales
    18. Nombre de usuario del administrador

6. Seudonimizar y cifrar los datos personales.

1. Las estadísticas y analíticas de los sistemas se recaban y tratan de forma anonimizada.

2. La información salvaguardada en nuestros dispositivos está cifrada con el máximo nivel de protección.